Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Inteligência de Ameaças Cibernéticas para Melhoria na Detecção e Resposta a Incidentes

Gustavo Antonio Souza de Barros

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Orientador
Prof. Dr. João José Costa Gondim

Brasília
2024

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Inteligência de Ameaças Cibernéticas para Melhoria na Detecção e Resposta a Incidentes

Gustavo Antonio Souza de Barros

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Prof. Dr. João José Costa Gondim (Orientador)
CIC/UnB

Prof. Dr. Robson de Oliveira Albuquerque
Universidade de Brasília

Prof. Dr. Marcelo Antonio Marotta
Universidade de Brasília

Prof. Dr. Joao Luiz Azevedo De Carvalho
Coordenador do Curso de Engenharia da Computação

Brasília, 17 de abril de 2024

Dedicatória

Dedico este trabalho à minha amada família, cujo amor incondicional esteve presente comigo durante toda a minha vida. E aos meus amigos, pelos momentos compartilhados de aprendizado, risadas e apoio mútuo.

Agradecimentos

Agradeço ao meu estimado orientador João José Costa Gondim, cuja orientação experiente e apoio foram fundamentais em todas as etapas deste projeto. Sua dedicação e ensinamentos foram essenciais para a conclusão deste projeto.

Gostaria de estender meus agradecimentos a Cristoffer Leite e os demais autores da pesquisa em que esse trabalho foi baseado, seu estudo serviu como inspiração e guia para esta monografia.

Além disso, desejo expressar minha gratidão à Universidade de Brasília pelo ambiente de aprendizado propício e recursos oferecidos ao longo desta jornada.

A Deus, por estar comigo nos momentos mais difíceis dessa trajetória.

Por fim, um sincero obrigado a todos os amigos, familiares e colegas que ofereceram apoio moral e encorajamento durante todo o processo.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

A detecção de ataques cibernéticos é uma tarefa complexa, pois exige a análise de extensos volumes de dados. Mesmo com esse desafio, a defesa contra ciberataques ainda requer uma quantidade significativa de intervenção manual. Nesse cenário, buscar a automatização de partes do processo é essencial. A Inteligência de Ameaças Cibernéticas consiste na coleta, processamento e análise de dados sobre ataques, sendo o tráfego de rede uma importante fonte de informações. Este trabalho apresenta uma abordagem automatizada para integrar essa inteligência na detecção de ameaças e resposta a incidentes, por meio da análise de Técnicas, Táticas e Procedimentos documentados em relatórios de inteligência, sua correlação com incidentes de rede e a geração de padrões de ataque. O software desenvolvido constrói padrões a partir de ataques previamente observados e avalia a correspondência desses padrões com registros de rede, procurando identificar possíveis atacantes e as técnicas empregadas. O método implementado fornece ao operador informações contextualizadas sobre ameaças cibernéticas relacionadas a incidentes observados, facilitando a tomada de decisões por parte da equipe de segurança.

Palavras-chave: inteligência de ameaças cibernéticas, cibersegurança, automatização, detecção, resposta a incidentes

Abstract

Detecting cyberattacks is a complex task, as it requires the analysis of a large volume of data. Despite this challenge, defense against cyberattacks still demands a significant amount of manual effort. In this cenario, automating parts of the process becomes essential. Cyber Threat Intelligence consists of collecting, processing, and analyzing data related to attacks, with network traffic serving as a key source of information. This work presents an automated approach to integrate this intelligence into threat detection and incident response by analyzing Tactics, Techniques, and Procedures documented in intelligence reports, correlating them with network incidents, and generating attack patterns. The developed software builds patterns based on previously observed attacks and assesses the match of these patterns with the network logs, aiming to identify potential attackers and the techniques employed. The implemented method provides the operator with contextualized information on cyber threats related to observed incidents, facilitating decision-making by the security team.

Keywords: cyber threat intelligence, cybersecurity, automatization, detection, incident response

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

API Interface de Programação de Aplicação.

APTs Ameaças Persistente Avançada.

CLI Interface de Linha de Comando.

CSIRTs Times de Segurança e Resposta a Incidentes.

CTI Inteligência de Ameaças Cibernéticas.

DML Detecção de Nível de Maturidade.

IoCs Indicadores de Comprometimento.

IoT Internet das Coisas.

IPO Orquestrador de Padrões de Inteligência.

JSON Notação de Objetos JavaScript.

NIDS Sistema de Detecção de Intrusões de Rede.

SDOs Objetos de Domínio Stix.

STIX Structured Threat Information Expression.

TIP Plataforma de Inteligência de Ameaças.

TTPs Técnicas, Táticas e Procedimentos.

Capítulo 1

Introdução

Em um mundo cada vez mais marcado pela digitalização, o volume de dados sensíveis circulando em rede aumenta de forma exponencial. Muitas das informações mais valiosas não são mais armazenadas fisicamente, mas em nossos computadores ou na nuvem [2]. Entretanto, esse cenário apresenta um novo desafio, com a crescente dependência de diferentes tecnologias, a gama de ameaças também evolui de maneira alarmante [3]. Além disso, à medida que a complexidade dos sistemas aumenta, sua segurança tende a diminuir, tornando-os mais vulneráveis a ataques.

Em todo o globo, organizações enfrentam a necessidade emergencial de desenvolver formas de prevenir e mitigar essas novas ameaças. Essa demanda vai além de ferramentas tecnológicas avançadas, exigindo também uma abordagem estratégica baseada na coleta e análise de informações. Diante disso, o *Cyber Threat Intelligence* (CTI), ou Inteligência de Ameaças Cibernéticas é um componente essencial para a defesa cibernética. A CTI pode ser compreendida como qualquer informação valiosa que ajude a identificar, avaliar, monitorar e responder a ameaças digitais, e sua análise permite informar os usuários sobre possíveis ameaças ao seus sistemas [4].

Qualquer dispositivo conectado à Internet está vulnerável a ser vetor de invasão ou alvo, e cada um deles gera enormes volumes de registros de conectividade [5]. Essa quantidade de dados dificulta a análise pelos operadores de segurança, o que acaba desacelerando os processos de defesa. Os cibercriminosos, nesse contexto, possuem a vantagem de iniciar os ataques, enquanto as equipes de segurança se encontram em uma posição reativa [6]. Esse desequilíbrio expõe a necessidade de otimizar os processos de segurança, procurando diminuir o esforço manual por parte dos Times de Segurança e Resposta a Incidentes (CSIRTs) e automatizar parte dessa operação.

Este trabalho utiliza a metodologia apresentada em Cristoffer et al. [1] para integrar a CTI nos processos de segurança e permitir uma abordagem mais ativa de defesa, no contexto de tráfego de rede. O objetivo é implementar um *software* que seja capaz de

gerar inteligência acionável, de forma que a detecção e resposta a incidentes sejam mais eficazes. Dando suporte a essa abordagem, foi desenvolvido um *software*, denominado de Orquestrador de Padrões de Inteligência (IPO), que identifica possíveis atacantes comparando as técnicas empregadas em incidentes detectados em rede com aquelas de ataques observados anteriormente. De modo geral, o programa utiliza uma base de dados de CTI para gerar padrões de ataques a partir de relatórios de inteligência, relacionando as técnicas dos atacantes com alertas de rede. O sistema avalia os registros de rede monitorados e verifica sua correspondência com os padrões registrados, permitindo que operadores identifiquem rapidamente as técnicas empregadas e a similaridade com ataques previamente documentados.

1.1 *Outline* da monografia

Esta monografia é organizada em seis capítulos. O Capítulo 1 apresenta a introdução ao tema. O Capítulo 2 discute o referencial teórico necessário para o entendimento do trabalho. O Capítulo 3 expõe a metodologia proposta. O Capítulo 4 detalha a implementação da solução desenvolvida. O Capítulo 5 apresenta os resultados obtidos. O Capítulo 6 discute os resultados e suas implicações, propondo possíveis direções para pesquisas futuras.

Capítulo 2

Referencial Teórico

Este capítulo apresenta a revisão teórica do trabalho, organizada em cinco seções. A Seção 2.1 introduz os termos e conceitos fundamentais para o entendimento do projeto. A Seção 2.2 discute o atual cenário de ameaças e o uso convencional da Inteligência de Ameaças Cibernéticas na cibersegurança. A Seção 2.3 apresenta a metodologia em que o presente estudo foi baseado e a Seção 2.4 aborda os trabalhos relacionados. Por fim, o capítulo é sintetizado na Seção 2.5.

2.1 Definições e Conceitos Relacionados

2.1.1 Da Inteligência à Inteligência de Ameaças

O conceito de inteligência tem diversas interpretações, que variam conforme o contexto onde é inserido. De forma geral, podemos definir inteligência como informações que podem ser utilizadas para alterar resultados [7]. Em um contexto profissional, Dalziel [8] define inteligência como dados que foram coletados, processados e analisados, para produzir informações que precisam ser relevantes, acionáveis e valiosas. Desse modo, a inteligência passa a ter um papel prático na resolução de problemas. A Figura 2.1 ilustra de forma visual esse conceito, demonstrando a relação entre dados, informações e inteligência.

O processo de transformação de dados em *insights* úteis encontra uma aplicação crucial em segurança da informação, especialmente na inteligência de ameaças. A inteligência de ameaças refere-se à capacidade de transformar dados brutos sobre potenciais perigos em informações estratégicas e acionáveis. Este campo envolve a coleta, agregação, processamento, análise e interpretação de informações relacionadas a possíveis ataques e vulnerabilidades, fornecendo contexto necessário para tornar eficaz a tomada de decisões de defesa [10].

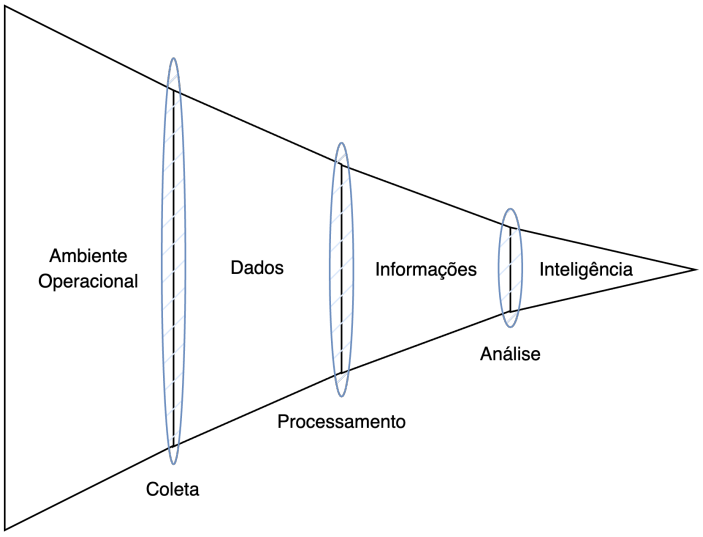

Figura 2.1: Fluxo de produção de inteligência. (Fonte: adaptado de [9]).

2.1.2 Inteligência de Ameaças Cibernéticas (CTI)

A inteligência de ameaças, quando aplicada no campo de segurança cibernética, é chamada de Inteligência de Ameaças Cibernéticas (CTI). Segundo Gartner [11], a CTI refere-se ao conhecimento fundamentado em evidências, como contexto, mecanismos, indicadores, implicações e recomendações práticas, sobre ameaças ou perigos existentes ou emergentes que possam afetar ativos, sendo possivelmente utilizados para informar decisões relativas à resposta a essa ameaça ou perigo. Exemplos práticos de evidências são Indicadores de Comprometimento (IoCs), métodos de ataque e ferramentas utilizadas. Esses dados de CTI são frequentemente compilados em relatórios de inteligência que descrevem as ameaças identificadas.

Ao contrário de abordagens convencionais de defesa, o CTI foca na antecipação e mitigação de riscos ao oferecer informações contextualizadas sobre potenciais ataques e vulnerabilidades. Portanto, um dos principais objetivos de quem usa essa inteligência é transformar as informações em inteligência acionável, capaz de auxiliar as decisões estratégicas e operacionais [12]. Dessa maneira, a CTI pode ajudar organizações a se tornarem mais proativas, identificando vulnerabilidades e atividades suspeitas antes dos atacantes a explorarem [13]. A aplicação correta desse recurso é fundamental para organizações que desejam aprimorar suas defesas, pois permite adaptar estratégias de acordo com ameaças emergentes.

O compartilhamento de informações é um aspecto central da CTI, pois permite que as partes interessadas desenvolvam rapidamente contramedidas [14]. Ferramentas e padrões como o STIX [15] facilitam o compartilhamento das informações e promovem uma

colaboração eficaz entre as organizações. Esse conhecimento permite que as organizações sejam eficientes na gestão de risco, implementando medidas preventivas, como correções de vulnerabilidades encontradas, detecção de ataques em seus primeiros estágios e respostas rápidas a incidentes. Além disso, o estudo das metodologias de ataque possibilita que sejam desenvolvidos novos mecanismos de defesa.

2.1.3 Observáveis e Indicadores de Comprometimento (IoCs)

Observáveis são artefatos de rede, como endereços IP, *hashes*, nomes de domínio, nomes de arquivos ou endereços de email, que são essenciais para identificar incidentes de segurança [16]. Esses observáveis, quando vinculados a um ataque conhecido, são denominados Indicadores de Comprometimento (IoCs). Os IoCs são fundamentais para a CTI, pois constituem artefatos forenses que permitem a análise e mitigação de ataques.

Depois de sua coleta, esses IoCs podem ser inseridos em vários mecanismos de defesa, como sistemas de detecção de intrusões e listas de bloqueio [17], sendo fundamentais para prevenir ameaças e responder rapidamente a incidentes. Embora os IoCs sejam valiosos na resposta a incidentes, eles constituem uma pequena porção do quebra-cabeça. Para evitar detecção, criminosos são capazes de se adaptar e substituir essas estruturas rapidamente. Por essa razão, para construir uma defesa mais robusta, é recomendado o uso integrado desses indicadores com outros, como Técnicas, Táticas e Procedimentos (TTPs).

2.1.4 Técnicas, Táticas e Procedimentos (TTPs)

As chamadas Técnicas, Táticas e Procedimentos descrevem o comportamento dos atores de ataque [10]. Dentro do campo da cibersegurança, o estudo mais aprofundado das TTPs é um passo fundamental para antecipar as ações de cibercriminosos. As táticas são os objetivos que os atacantes buscam alcançar, como invadir uma rede ou escapar dos mecanismo de detecção. As técnicas descrevem como é realizado o processo para atingir esses objetivos, ou seja, os métodos empregados, o que inclui ações como ataques de *phishing* e a exploração de vulnerabilidades. Os procedimentos detalham a aplicação da técnica, especificando as ferramentas, comandos e o contexto de onde estes foram utilizados.

Para a Inteligência de Ameaças Cibernéticas, o estudo das TTPs é elemento chave, pois provê aos analistas uma visão aprofundada do modo de operação dos atores do ataque. Enquanto os IoCs podem ser rapidamente alterados pelos atacantes, as TTPs possuem um teor comportamental mais estável, o que dificulta sua modificação e permite o desenvolvimento de defesas mais robustas. Ao compreender as TTPs, as equipes de segurança

conseguem construir modelos de defesa capazes de reconhecer padrões comportamentais dos atacantes, aumentando a eficácia na detecção e na resposta a incidentes.

2.1.5 Plataforma de Inteligência de Ameaças (TIP)

As Plataformas de Inteligência de Ameaças são soluções que centralizam em uma única aplicação o processo de coleta, pré-processamento, enriquecimento, correlação, análise e compartilhamento de eventos de ameaças e dados associados [18]. Essas plataformas são importantes na hora de transformar os dados brutos de CTI em uma inteligência prática, amparando o processo de análise e fortalecendo a segurança das organizações. Uma funcionalidade comum nas TIPs é a capacidade de coletar relatórios de inteligência da internet de forma automática através de conectores, agindo como uma base de dados de CTI. Para lidar com as grandes quantidades de dados, são usados formatos e *frameworks* que padronizam a CTI, como o STIX [15] e a matriz MITRE ATT&CK [19].

Muitas organizações descobriram que a troca de CTI é uma necessidade para sobreviver a futuros ataques [14]. A construção de uma defesa sólida contra ameaças cibernéticas exige a integração de diversas fontes de informação. Dessa forma, as TIPs são uma peça essencial para os especialistas de inteligência. De acordo com a Agência da União Europeia para a Segurança de Redes e Informação (ENISA), há 80 iniciativas e organizações, além de mais de 50 CSIRTs nacionais e 80 governamentais, envolvidos no compartilhamento de Inteligência de Ameaças Cibernéticas (CTI) na União Europeia (UE) e na Zona Econômica Europeia (EEA)[20].

2.1.6 MITRE ATT&CK

O MITRE ATT&CK é uma base de conhecimento global que categoriza as Técnicas, Táticas e Procedimentos usados por cibercriminosos [19]. Esse *framework* organiza as TTPs observadas em incidentes reais em uma matriz estruturada, dividida de acordo com as diferentes fases do ciclo de vida dos ataques. A Figura 2.2, para facilitar o entendimento da estrutura da matriz, ilustra três etapas comuns de um ataque (Acesso Inicial, Execução e Impacto), juntamente com algumas das técnicas associadas a cada uma delas.

Para cada técnica, o MITRE ATT&CK detalha informações sobre formas de detecção, táticas relacionadas, procedimentos empregados e estratégias de mitigação. Essa organização facilita a compreensão dos métodos e comportamentos dos adversários por parte da equipe de segurança, permitindo ajustes na estratégia de defesa com base no conhecimento obtido. Além disso, cada TTP é associada a um identificador único, o que facilita o gerenciamento e o rastreamento das informações.

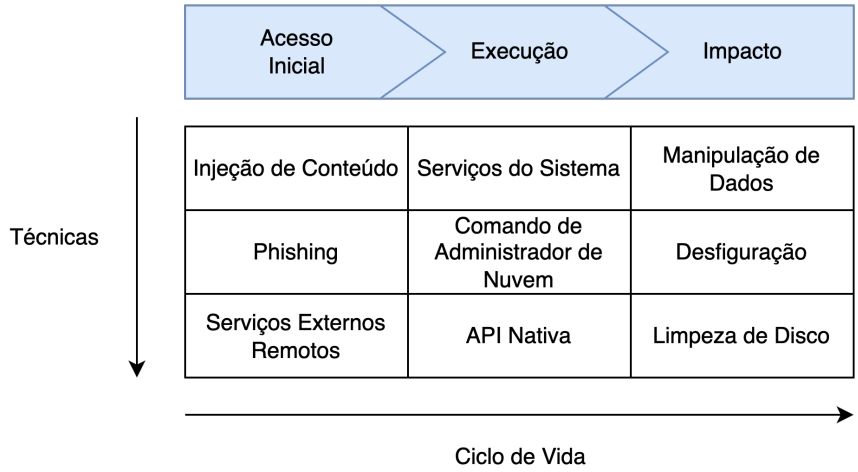

Figura 2.2: Fragmento simplificado da Matriz MITRE ATT&CK Enterprise (Fonte: [19]).

Diante das constantes mudanças no cenário de cibersegurança, o ATT&CK é continuamente atualizado para lidar com ameaças emergentes. Também é muito versátil, abrangendo uma ampla gama de sistemas operacionais e ambientes de trabalho, como redes empresarias, industriais e mobile. Esses fatores tornam a matriz adaptável a diferentes necessidades de segurança.

2.1.7 Structured Threat Information Expression (STIX)

O STIX é uma linguagem desenvolvida com o objetivo de especificar, capturar, caracterizar e comunicar informações padronizadas sobre ameaças cibernéticas [3]. Amplamente adotado por organizações de cibersegurança, o STIX permite uma comunicação estruturada de indicadores de ameaças, incidentes, técnicas, vulnerabilidades, e outros tipos de entidades. A linguagem proporciona uma visão geral de uma ameaça, compactando informações em *bundles*, que contêm várias entidades chamadas Objetos de Domínio Stix (SDOs). Esses objetos descrevem os diferentes tipos de dados de CTI de maneira organizada.

Essa padronização garante uma consistência de dados, mesmo entre diferentes ferramentas e plataformas. Essa interoperabilidade é essencial para criar um ambiente colaborativo na área de cibersegurança. O uso do STIX facilita o compartilhamento de dados de CTI, fato crucial para uma área onde o acesso a informações e agilidade são aspectos determinantes para obter bons resultados. Também permite o desenvolvimento e integração de soluções automatizadas, logo que otimiza o gerenciamento de dados, permitindo uma defesa mais robusta.

2.1.8 Sistema de Detecção de Intrusões de Rede (NIDS)

O Sistema de Detecção de Intrusões de Rede (NIDS) é um tipo de ferramenta baseada em mineração de dados para a detecção de intrusões em redes [21]. O sistema monitora o tráfego de rede e realiza a identificação de atividades suspeitas. Esse processo ocorre através da inspeção de pacotes em tempo real, comparando o conteúdo em rede com assinaturas conhecidas de ataques, definidas em regras. Esses sistemas estão sujeitos a gerarem falsos positivos, por isso exigem manutenção regular das assinaturas e das regras de detecção.

Os NIDS representam um componente essencial na proteção das redes, fornecendo uma camada extra de segurança. Na detecção de um possível ataque, o sistema pode realizar diversas ações programadas pelos administradores de rede. Entre essas ações estão a geração de um alerta, bloqueio de tráfego suspeito e registro de eventos. Um recurso amplamente utilizado nesses sistemas é a configuração de listas de bloqueio automáticas para IoCs, a fim de mitigar ataques observados anteriormente. Alguns NIDS também possuem integração com outros mecanismos de segurança, tornando assim a defesa mais robusta.

2.2 Estado da Arte

2.2.1 Panorama Atual de Ameaças

Com a crescente complexidade nos sistemas e alta integração tecnológica na sociedade, novos desafios foram introduzidos na área de cibersegurança. As organizações têm investido mais em serviços de nuvem e expandido sua presença no meio digital, e com isso, surgem novos fatores de riscos. Segurança de nuvem, junto com as vulnerabilidades inerentes do *Internet of Things* (IoT), tornam necessária uma compreensão mais aprofundada do cenário de ameaças [22].

Segundo dados do *Identity Theft Resource Center*, em 2023 houve 2.365 ciberataques, que afetaram mais de 300 milhões de vítimas [23]. Com o aumento da quantidade de ataques, a complexidade dessas operações criminosas também cresce, resultando no surgimento de ameaças cada vez mais sofisticadas [24].

Uma ameaça em destaque são as chamadas *Advanced Persistent Threats* (APTs), caracterizadas por ataques sofisticados de grupo de hackers. As APTs agem de modo a ficarem hospedadas de forma persistente no alvo para roubar informações cruciais e permanecer indetectável por um longo período de tempo [25]. Outra ameaça comum são os *ransomwares*, que são *malwares* desenvolvidos para impedir acesso ou criptografar dados até que um valor de resgate seja pago. Além disso, existem vulnerabilidades de software

conhecidas como *zero-day*, que são falhas de segurança no sistema ainda não documentadas, e cuja existência é conhecida apenas pelos adversários. Devido a essa característica, elas frequentemente permanecem indefinidas por um período considerável, dificultando sua identificação.

2.2.2 Arquitetura Tradicional de Cibersegurança

O avanço da educação em segurança cibernética tem contribuído para que as organizações fortaleçam seus mecanismos de defesa. No entanto, parte dessas instituições ainda utiliza modelos clássicos de defesa. Na Figura 2.3, é sintetizado o fluxo normalmente implementado nessas arquiteturas tradicionais. Essa estrutura atribui ênfase à coleta de IoCs, utilizando ferramentas de segurança para identificar e bloquear ataques com base nesses indicadores, geralmente de forma genérica e automática.

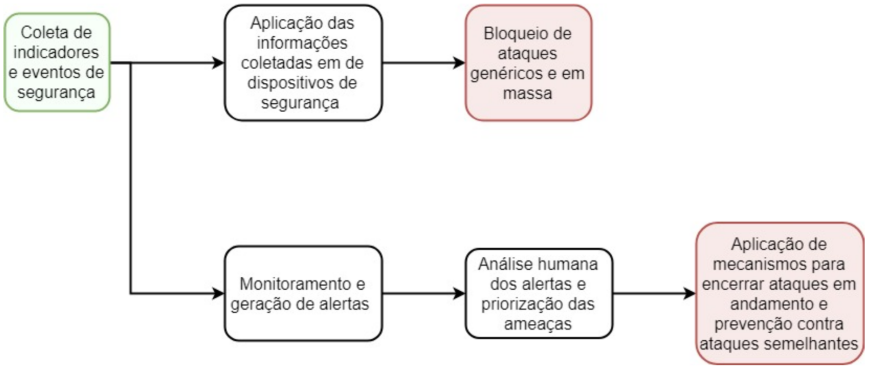

Figura 2.3: Fluxo do modelo tradicional de segurança cibernética (Fonte: [24]).

Uma porção significativa dos Times de Segurança e Resposta a Incidentes (CSIRTs) ainda trabalham apenas com IoCs [26], o que pode deixar brechas na segurança de uma organização. A mitigação de ataques mais sofisticados requer a monitorização contínua do tráfego de rede, a análise de alertas de segurança e a correlação de eventos para a identificação de ameaças. Entretanto, essa atividade demanda um grande esforço manual do operador, que precisa verificar um vasto volume de registros de rede, consultar alertas os alertas emitidos e tentar identificar possíveis ameaças. Como consequência, percebe-se que essa metodologia de defesa possui uma instância mais reativa [24], focada em resposta a incidentes, e tem como ponto fraco não ser eficaz o suficiente para identificar ataques mais complexos durante sua execução.

2.3 Base Metodológica

O presente trabalho foi inspirado na solução em Cristoffer et al. [1], que busca preencher lacunas no que diz respeito ao uso da CTI nos mecanismo de segurança, principalmente no que se refere à acionabilidade na resposta a incidentes. O problema abordado pela pesquisa base está relacionado ao grande esforço analítico por parte das equipes de segurança para verificação dos incidentes de rede. É possível observar no fluxo de uma implementação simples com NIDS, conforme ilustrado na Figura 2.4, observa-se que, que além da análise dos eventos da rede, frequentemente compostos por longos registros de conectividade, também é necessário relacionar esses dados com informações de inteligência. Esse processo de análise e correlação impõe uma carga significativa sobre o analista de segurança, comprometendo a eficiência do método devido à sua complexidade e ao alto volume de dados envolvidos.

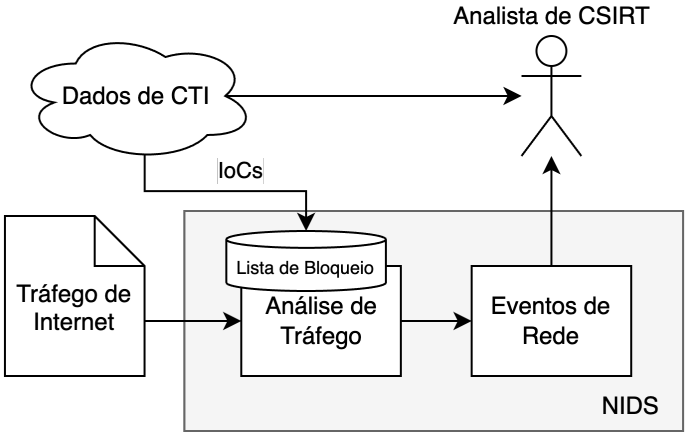

Figura 2.4: Implementação simples de arquitetura tradicional com NIDS (Fonte: adaptado de [1]).

A automatização de processos e a geração de CTI acionável são recursos que têm a capacidade de aumentar a eficácia dos Times de Segurança e Resposta a Incidentes (CSIRTs). Essas medidas facilitam a análise das informações, o que torna o fluxo de defesa mais rápido na proteção contra ciberataques, agilizando as tomadas de decisão por parte dos times de segurança. Essa necessidade é uma demanda forte no mercado, que anseia por soluções que sejam capazes de detectar e responder possíveis ameaças rapidamente, um dos principais desafios da área de cibersegurança.

O Orquestrador de Padrões de Inteligência (IPO), ferramenta proposta em Cristoffer et al. [1], tem como objetivo gerar inteligência acionável para as equipes de segurança de forma mais otimizada. O *software* busca identificar atacantes e as técnicas empregadas

por eles em registros de rede, usando conhecimento obtido de ataques observados anteriores, que são armazenados em padrões descrevendo o comportamento do atacante. Esses padrões são construídos a partir de relatórios de inteligência de CTI e tem como base as TTPs dos atacantes, representando o comportamento típico do adversário. Através da correspondência entre os padrões armazenados e os registros de conectividade, é possível identificar o nível de similaridade desse ataque com os previamente documentados, ajudando a tomada de decisão das Times de Segurança e Resposta a Incidentes. A pesquisa base tem como foco ameaças de *malware*, tentando identificar diferentes famílias nos registros de rede.

2.4 Trabalhos Correlatos

Apesar de um interesse cada vez maior na CTI, ela ainda é uma adição recente nos modelos de segurança e sua integração possui espaço para aprimoramento. O objetivo desta seção é contextualizar o trabalho atual de acordo com as soluções propostas anteriormente, verificando lacunas que ainda não haviam sido preenchidas.

Estudos nessa área dispõem de características comuns: Extração de TTPs e Automatização da Análise de CTI. Porém, buscando ampliar o uso da CTI, é interessante avaliar também a Acionabilidade na Resposta de Incidentes. A Tabela 2.1 compara os diferentes estudos. Embora seja notável que houve avanços na implementação prática da CTI na cibersegurança, ainda falta explorar este recurso no processo de resposta a incidentes. A proposta do presente trabalho procura gerar inteligência acionável a partir da identificação de possíveis atacantes e técnicas empregadas a partir de registros de rede.

Referência	**Automatização na Análise de CTI**	**Mapeamento de TTPs**	**Acionabilidade na Resposta a Incidentes**
Alam et al [27]	✓	✓	
Husari et al [28]	✓	✓	
Rani et al [29]	✓	✓	
Zhu et al [30]	✓		
Hybrid Analysis [31]		✓	✓
Esta proposta	✓	✓	✓

Tabela 2.1: Comparação de diferentes estudos acerca da integração de CTI.

2.5 Síntese do Capítulo

Este capítulo apresentou os diversos conceitos fundamentais para compreender a área de Inteligência de Ameaças Cibernéticas, fornecendo uma base sólida para seu entendimento. Também abordou o atual cenário de cibersegurança, detalhando as principais ameaças e apresentando uma visão geral do funcionamento de uma das arquiteturas clássicas de defesa.

O grande foco em IoCs e a análise praticamente manual por parte dos Times de Segurança e Resposta a Incidentes (CSIRTs) representam um gargalo significativo na cibersegurança. A metodologia proposta em Cristoffer et al. [1], base para o presente estudo, tenta minimizar esse problema através de um novo mecanismo de detecção de ameaças e resposta a incidentes a partir de padrões comportamentais dos atacantes. Existe um grande potencial no uso de Técnicas, Táticas e Procedimentos dos atacantes para melhorar a eficácia das operações de seguranças e tornar a defesa mais robusta. Dessa forma, o método propõe identificar possíveis atacantes através das técnicas empregadas em rede e padrões observados anteriormente.

Capítulo 3

Metodologia

Esse capítulo é organizado em sete seções: A Seção 3.1 apresenta a metodologia proposta como solução, descrevendo o funcionamento geral do software desenvolvido e seus objetivos. A Seção 3.2 consiste da arquitetura geral do software, apresentando como as diferentes partes do programa trabalham entre si. A Seção 3.3 detalha os módulos presentes no sistema e como eles realizam suas funções. A Seção 3.4 sumariza as contribuições do presente estudo em relação à metodologia base. A Seção 3.5 apresenta a infraestrutura utilizada e como foi configurado o ambiente de testes. Na Seção 3.6 são abordados os casos de teste. Por fim, a Seção 3.7 sintetiza os comentários finais do capítulo.

3.1 Metodologia Proposta

A solução desenvolvida, baseada na metodologia proposta por Cristoffer et al [1], busca aumentar a eficiência do processo de segurança cibernética por meio da geração de inteligência acionável a partir de CTI. A ferramenta implementada, com o uso de TTPs, fornece ao operador informações contextualizadas sobre possíveis ameaças usando registros de rede, procurando aumentar a eficácia da análise de tráfego, o que permite mais acionabilidade e respostas rápidas.

O *software*, chamado de *Intelligence Pattern Orchestrator* (IPO), processa, filtra e ranqueia a CTI, criando padrões que descrevem as características de uma ameaça, utilizando esses padrões para identificar potenciais ameaças em rede. Através do IPO, são enriquecidas as informações sobre eventos suspeitos de rede. O objetivo é prover ao analista informação contextual sobre esses incidentes, associando eles com padrões vistos em ataques anteriores e assim diminuindo a carga analítica manual. O programa dispõe de duas funcionalidades principais: Construção de Padrão e Correspondência de Padrões. Além de uma função auxiliar de Mapeamento de Assinaturas.

A construção de um padrão inicia-se com a seleção de um relatório de inteligência presente em uma base de dados de CTI. Em seguida, o IPO realiza a coleta de informações adicionais sobre a ameaça de interesse a partir de outros relatórios correlacionados. Usando o conhecimento obtido, as técnicas empregadas pelos atacantes são utilizadas como base para a criação de um padrão, que é armazenado no sistema e pode ser usado para identificar o atacante em futuras incidências.

O tráfego de rede é uma importante fonte de informações de CTI. Através dele, e com o auxílio de ferramentas como um NIDS, é possível monitorar possíveis ameaças e até mesmo detectar as técnicas que estão sendo utilizadas para realizar essa intrusão. Usando os padrões construídos, o software é capaz de verificar registros de redes para identificar os atacantes e as técnicas que estão sendo empregadas. Esse nível de correspondência é dado por um valor de porcentagem, que se refere a similaridade das TTPs do padrão e dos detectados nos registros de rede. Essa informação é vital para que os Times de Segurança e Resposta a Incidentes consigam ser mais eficientes.

3.2 Arquitetura do Software

O Orquestrador de Padrões de Inteligência é constituído de quatro módulos principais: Coleta de Informação, Filtro e Ranqueamento, Construção de Padrão e Correspondência de Padrões. Os módulos desenvolvidos trabalham de maneira conjunta para realizar as funcionalidades do programa, como demonstrado no fluxo da Figura 3.1.

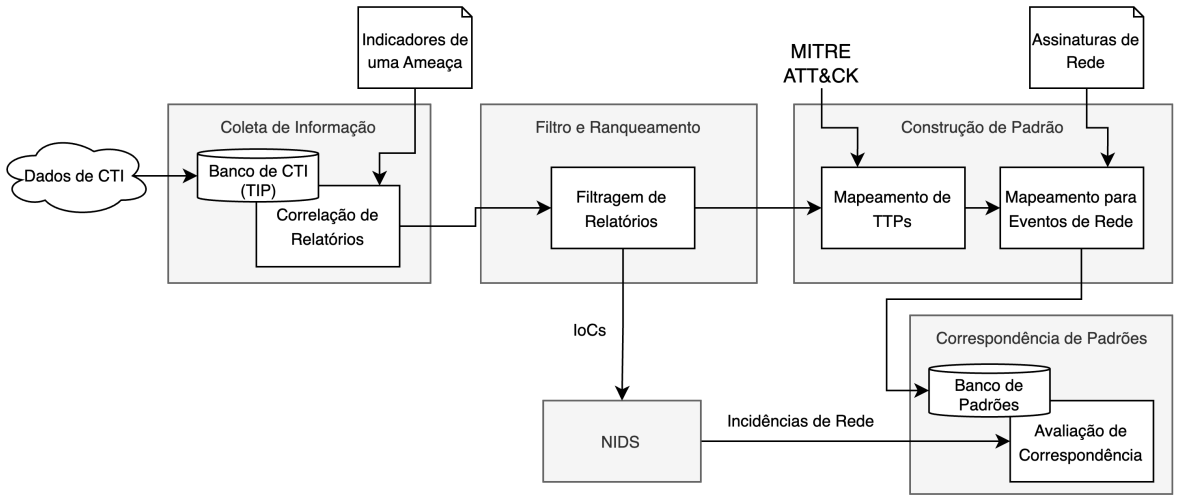

Figura 3.1: Fluxo de dados do IPO (Fonte: adaptado de [1]).

Quando se trata de construir um novo padrão, três módulos atuam de modo sequencial: Coleta de Informação, Filtro e Ranqueamento e Construção de Padrão. A primeira etapa

compreende a Coleta de Informação, na qual indicadores de uma determinada ameaça são utilizados para identificar dados correlacionados de CTI em outras fontes, buscando enriquecer a compreensão sobre as características da ameaça. Em seguida, a CTI será filtrada com base no seu nível de informação, no componente denominado de Filtro e Ranqueamento. Na fase chamada de Construção de Padrão, com o uso das Técnicas, Táticas e Procedimentos do atacante, e seu mapeamento com a matriz MITRE ATT&CK, são elaborados padrões para reconhecer essas ameaças através de seu comportamento e eventos de rede relacionados. Por fim, esses padrões são armazenadas em um banco de dados.

Os padrões armazenados são usados para avaliar atividades suspeitas na rede através do módulo de Correspondência de Padrões. A identificação acontece por meio da análise dos *logs* do NIDS, configurado para gerar alertas únicos, os quais são utilizados para identificar TTPs. Esses padrões fornecem contexto sobre atividades suspeitas em rede e facilitam a análise por parte da equipe de segurança, assim como resposta rápida a incidente através do conhecimento informado.

Para a execução do IPO, é crucial que alguns requisitos sejam cumpridos: uma base de dados populada em uma TIP e a integração com um NIDS. Os dois são fundamentais para que os módulos do orquestrador funcionem corretamente. O fluxo de uma implementação completa do IPO em um esquema de segurança, integrado com a NIDS e a TIP, é ilustrado na Figura 3.2.

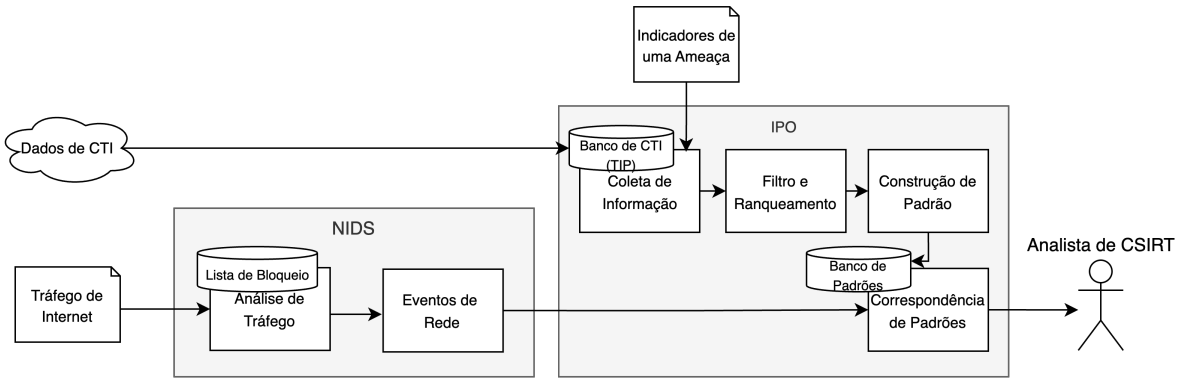

Figura 3.2: Fluxo de segurança com uso de NIDS e IPO (Fonte: adaptado de [1]).

Além dos módulos principais, foi desenvolvida uma função auxiliar, denominada de Mapeamento de Assinaturas. Essa função é capaz de processar um pacote de regras de NIDS que contenha referências ATT&CK, criando um arquivo de mapeamento de alertas de rede para TTPs.

3.3 Módulos

3.3.1 Coleta de Informação

O módulo de Coleta de Informação visa consolidar o conhecimento relativo a uma ameaça de entrada, agregando dados de diversas fontes de CTI. Para alcançar esse objetivo, esse módulo reúne relatórios de inteligência disponíveis em múltiplas fontes na internet, identificando aqueles que estão correlacionados com a ameaça em questão. O enriquecimento dos dados permite a construção de padrões detalhados, que capturam de forma mais abrangente o comportamento do atacante.A Figura 3.3 apresenta um panorama geral do módulo, demonstrando como esse componente recebe um relatório de inteligência contendo os indicadores de uma ameaça, e usa dados de CTI para criar uma lista de relatórios correlacionados.

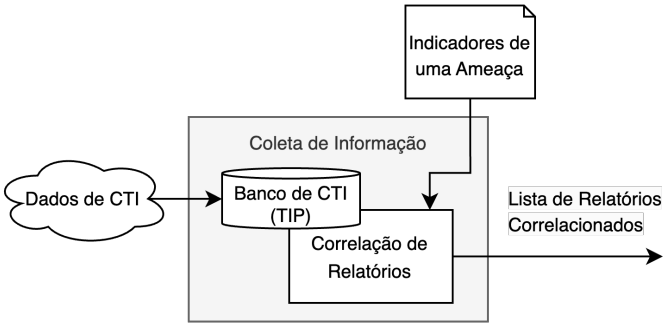

Figura 3.3: Fluxo do módulo de Coleta de Informação do IPO.

Base de Dados

A integração de uma TIP populada com múltiplas fontes de CTI ao IPO é essencial para reunir informações sobre ameaças. A plataforma age como um repositório central que facilita o acesso a grandes volumes de informações sobre ameaças, armazenando relatórios de segurança que detalham ameaças conhecidas e suas características. Uma base de dados bem estruturada fornece ao orquestrador acesso a um conjunto abrangente e atualizado de dados, o que facilita a análise e correlação de informações por parte do *software*.

Correlação de Relatórios

Com base em um relatório inicial sobre uma ameaça, o orquestrador busca na TIP outros relatórios que contenham alguma informação correlacionada. Essa correlação é baseada em diversos fatores, como similaridades nos indicadores, contexto de ataque ou atores responsáveis.

À medida que relatórios correlacionados são identificados, eles são adicionados em uma lista. Esse processo é iterativo: a cada novo relatório adicionado, o IPO verifica a TIP em busca de mais relatórios relacionados, repetindo o processo até que nenhuma nova correlação seja encontrada. O resultado obtido é uma lista de relatórios relacionados a uma mesma ameaça.

3.3.2 Filtragem e Ranqueamento

Os relatórios de CTI são constituídos de uma variedade de informações diferentes sobre a ameaça. Para construir padrões coerentes, é necessário definir quais dessas informações são úteis e relevantes para esse processo. Com isso, esse módulo tem a função de filtrar relatórios que não possuem informações comportamentais do atacante, ao mesmo tempo que envia IoCs para bloqueio automático na NIDS. A Figura 3.4 detalha o fluxo do funcionamento geral do módulo.

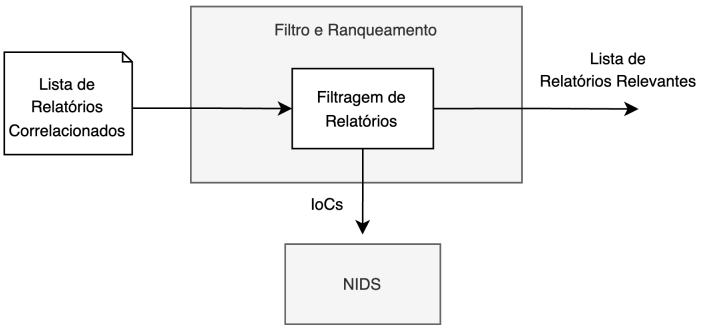

Figura 3.4: Fluxo do módulo de Filtragem e Ranqueamento do IPO.

Ranqueamento: CTI de alto nível e CTI de baixo nível

A CTI abrange diferentes tipos de informação, algumas podem ser de cunho operacional, como IoCs, ou de cunho comportamental, como padrões de ataque. Utilizando o modelo de Detecção de Nível de Maturidade (DML) [26], representado na Figura 3.5, as informações de CTI podem ser divididas em alto e baixo nível. Essa separação é fundamental, pois a CTI de alto nível fornece informações sobre o comportamento do atacante, o que é crucial para a criação de padrões e análise profunda das ameaças. A de baixo nível se encontra entre o DML-0 até o DML-2, e se refere principalmente aos IoCs, envolvendo dados operacionais. A de alto nível consiste do DML-3 para cima, consistindo de informações como TTPs, estratégia, objetivos e identidade do atacante.

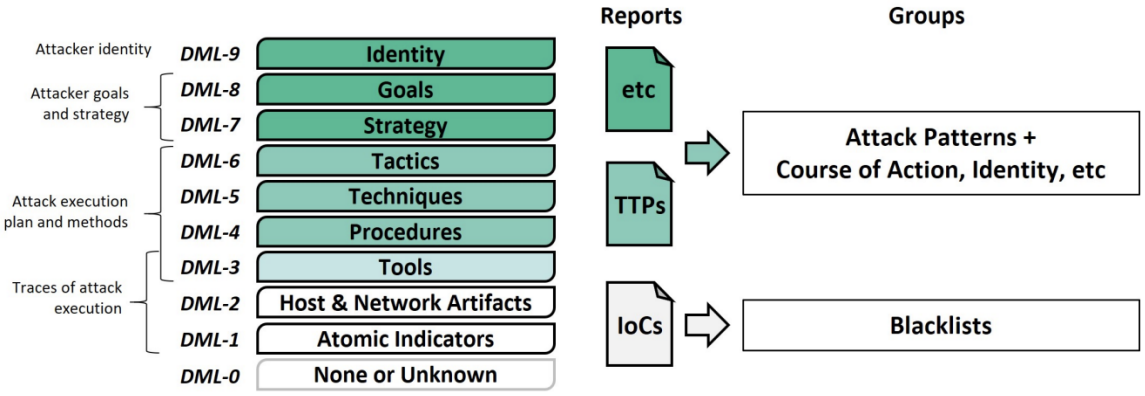

Figura 3.5: Modelo de Detecção de Nível de Maturidade (DML) (Fonte: [26]).

Filtragem dos Relatórios

Entre os relatórios da lista recebida, é necessário determinar em quais deles há conteúdo relevante para a construção de padrão. O nível geral de um relatório é definido pelo sua CTI de maior nível. Portanto, um relatório é considerado relevante se nele consta ao menos uma informação de alto nível. Os relatórios de baixo nível são descartados e seus IoCs encaminhados para a lista de bloqueio da NIDS. Considerando que R_i seja uma lista de relatórios, e *Threshold* seja DML-3 devido à nossa definição de CTI de alto nível, podemos expressar a lista de relatórios relevantes pela equação (3.1).

$$\text{Relatórios Relevantes} = \{R_i \mid DML_{max}(R_i) \geq Threshold\} \tag{3.1}$$

3.3.3 Construção de Padrão

No módulo de Construção de Padrão, através das TTPs da ameaça, são construídos padrões que representam o comportamento de um atacante em rede. Através de uma lista de relatórios e das assinaturas configuradas na NIDS, é gerado um arquivo que fica armazenado no sistema representando o padrão criado. Esses arquivos guardam eventos de rede que representam o comportamento do atacante, expresso com base nas técnicas empregadas e os alertas de rede relacionados. O fluxo desse módulo e a integração dos seus diferentes processos é ilustrado pela Figura 3.6.

Mapeamento das TTPs para MITRE ATT&CK

Na detecção de ameaças por meio de análise de rede, nem todas as informações incluídas na classe de CTI de alto nível são imediatamente úteis. Nesse contexto, as TTPs

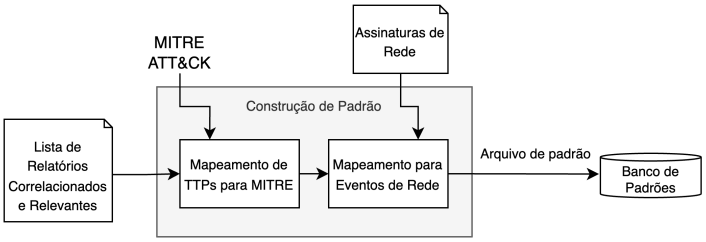

Figura 3.6: Fluxo do módulo de Construção de Padrão do IPO.

desempenham um papel crucial, pois algumas delas podem ser identificadas diretamente em eventos de rede. O processo desenvolvido extraí os TTPs dos relatórios de inteligência e organiza as informações em duas listas separadas: uma contendo as TTPs encontradas nos relatórios e outra reunindo o restante dos elementos de CTI de alto nível. Embora essas informações adicionais não sejam diretamente acionáveis para a detecção, elas oferecem um contexto valioso para os analistas, auxiliando na interpretação e priorização das ameaças. Nos relatórios de inteligência, as informações sobre uma determinada TTP costumam acompanhar uma referência com o identificador do MITRE ATT&CK. Usando essas referências, é gerada uma lista dos TTPs expressos em função do ATT&CK.

Mapeamento das TTPs para Eventos de Rede

Para garantir que os padrões de ataque sejam gerados corretamente e as ameaças detectadas em rede, é necessário que o NIDS esteja preparado para receber regras personalizadas que identifiquem as TTPs do adversário. Ao estudar a matriz do MITRE ATT&CK, é possível identificar quais TTPs podem ser detectados através de eventos de rede. Esses eventos podem ser acompanhados por alertas, que tem uma assinatura única. A partir disso, é possível criar assinaturas no NIDS que alertem sobre a presença dessas TTPs. Essa configuração personalizada assegura que os eventos do tipo alerta de rede estejam associados a padrões de ataques conhecidos. Essa configuração na NIDS permite que o IPO e os analistas identifiquem a técnica empregada usando a matriz ATT&CK.

O processo implementado, usando as regras do NIDS com assinaturas personalizadas, e os TTPs, vinculados com identificadores do ATT&CK, realiza o mapeamento das técnicas para eventos de rede associados, gerando uma lista descrevendo o comportamento do adversário em função desses eventos. Desse modo, é possível criar um arquivo descrevendo o padrão de ataque observado. No IPO, o padrão é um objeto estruturado por certos atributos: nome, descrição, eventos, gravidade, categoria e janela de tempo.

- **Nome**: Identificador para o novo padrão criado.

- **Descrição**: Breve descrição sobre a ameaça definida, podendo incluir informações da CTI contextual extraída.
- **Eventos**: Lista dos eventos de rede que definem o comportamento suspeito. Esses eventos são representados pelas assinaturas das regras do NIDS.
- **Gravidade**: Severidade do ataque.
- **Categoria**: Escopo do padrão. O valor padrão é "Segurança".
- **Janela de Tempo**: Duração do ciclo de vida esperado desse ataque.

Essa etapa é um ponto de interação do operador e o Orquestrador de Padrões de Inteligência, pois no momento da criação do padrão, é necessário o preenchimento dos atributos, exceto o de eventos que é gerado automaticamente pelo orquestrador como descrito anteriormente. Dessa forma, um padrão é criado e fica armazenado no sistema, potencialmente em um banco de dados.

3.3.4 Correspondência de Padrões

Esse módulo é utilizado pelos operadores de segurança para verificar os *logs* de rede em busca de atividades suspeitas. Dessa forma, ao analisar os eventos de rede, são identificados os alertas de rede e as técnicas relacionadas, fornecendo um contexto valioso sobre as atividades suspeitas detectadas. Além disso, também avalia a similaridade desse ataque com os padrões registrados no sistema. Essas informações permitem que os operadores de segurança interpretem os eventos de rede em termos de possíveis ameaças, possibilitando uma resposta rápida e eficaz. A Figura 3.7 apresenta o fluxo geral do módulo.

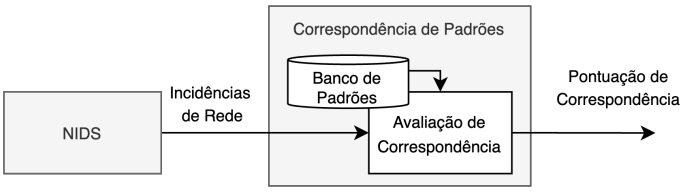

Figura 3.7: Fluxo do módulo de Construção de Correspondência de Padrões do IPO.

Avaliação de Correspondência

No IPO, é criada uma pontuação baseada no nível de correspondência entre as TTPs identificadas nos eventos de rede e os TTPs do padrão. Embora a pontuação de correspondência pudesse ser calculada pela quantidade de eventos de rede que coincidem com os

registrados no padrão, esse método pode ser impreciso, já que uma única TTP pode gerar múltiplos tipos diferentes de eventos de rede. Dessa forma, a pontuação é determinada pela quantidade de TTPs presentes tanto nos registros de rede quanto do padrão, sendo calculada pela porcentagem de interseção entre esses dois conjuntos. A (3.2) demonstra a fórmula utilizada.

- TTP_{registro}: Conjunto de TTPs detectadas nos registros de rede analisados.
- $TTP_{\text{padrão}}$: Conjunto de TTPs definidas no padrão.

$$\text{Pontuação de Correspondência} = \frac{|TTP_{\text{registro}} \cap TTP_{\text{padrão}}|}{|TTP_{\text{padrão}}|} \times 100 \tag{3.2}$$

Os *logs* analisados são comparados com todos os padrões cadastrados, sendo atribuída uma pontuação que indica o grau de correspondência com cada padrão. Além disso, o analista também é informado sobre qualquer TTP detectada. Dessa forma, com a ameaça mais contextualizada, o operador pode ser mais eficaz na resposta a incidentes.

3.3.5 Mapeamento de Assinaturas

Projetada para dar suporte aos CSIRTs, tem como objetivo facilitar o mapeamento de assinaturas do NIDS para TTPs, que é essencial para um uso fluído do orquestrador. Ao invés de ser necessário escrever cada regra personalizada específica para a matriz MITRE ATT&CK, essa funcionalidade permite que o operador carregue um arquivo de pacotes de regras. O IPO então automaticamente irá percorrer essas regras procurando referências MITRE. Gerando um arquivo de mapeamento de ATT&CK para assinaturas do NIDS. Esse processo pode ser visto na Figura 3.8.

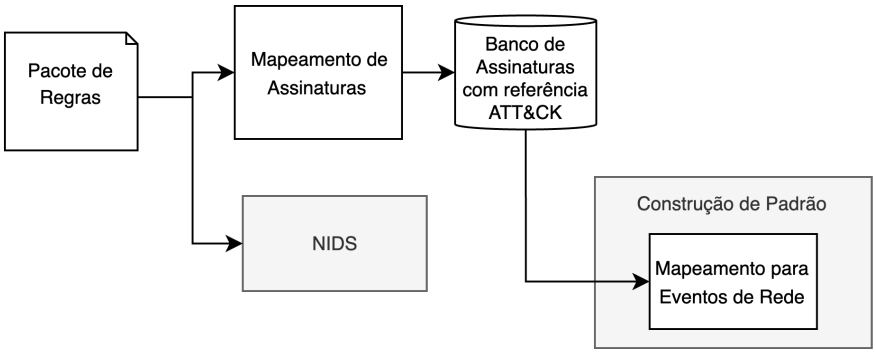

Figura 3.8: Fluxo de dados da função Mapeamento de Assinaturas..

O arquivo de mapeamento funciona como um banco de dados do tipo *key-value*, onde as assinaturas do NIDS atuam como chaves, e os identificadores do MITRE ATT&CK

funcionam como os valores correspondentes. Esse formato permite que os processos de mapeamento do IPO sejam otimizados, logo que realizar a associação entre TTP e assinatura se torna mais eficiente. Além disso, com essa funcionalidade, o operador pode adicionar ou modificar as regras do NIDS e configurar o IPO de maneira ágil, além de ter a possibilidade de utilizar pacotes públicos de assinaturas, como os fornecidos pelo *Emerging Threats*.

3.4 Contribuições deste trabalho em relação à Cristoffer et al. [1]

A pesquisa desenvolvida em Cristoffer et al. [1] serviu como base para o *software* desenvolvido no presente trabalho. Visando tornar mais eficiente a detecção e resposta em incidentes na área de cibersegurança, foi implementado o Orquestrador de Padrões de Inteligência. A arquitetura proposta mantém a estrutura de quatro módulos descritos no trabalho base, adotando um modelo arquitetural semelhante. Contudo, diferenças significativas foram introduzidas na implementação e na abordagem de avaliação dos resultados.

No estudo original, eventos de rede são usados para calcular a porcentagem de correspondência. No entanto, no presente estudo são utilizadas diretamente as TTPs. Essa abordagem foi adotada após a identificação de casos em que múltiplos eventos de rede apontavam para a mesma TTP, resultando em uma pontuação final equivocada. Logo, houve a necessidade de avaliar de forma diferente. Usando o arquivo de mapeamento, os eventos de rede são convertidos em TTPs, comparando diretamente as TTPs do padrão e do registros de rede. Além disso, no artigo original, de acordo com a pontuação de correspondência, havia um nível de confiança atrelado, essa funcionalidade adicional não foi implementada neste trabalho.

Outra diferença significativa é nas ameaças usadas como caso de teste no IPO. Enquanto no trabalho original ele foi projetado e testado com famílias de malware, o do presente estudo foi produzido para realizar esse processo para ameaças em geral, sem distinção de tipo. Qualquer tipo de ameaça, desde que esteja em relatórios de inteligência da TIP, pode ser utilizada para criar um novo padrão.

A fim de incrementar mais o contexto da informação de saída na verificação de *logs*, a saída não conta só com a pontuação de correspondência, mas também todas as TTPs encontrados naqueles registros. Essa informação provê um contexto adicional importante para o analista de CSIRT, detectando potenciais ataques sem depender dos padrões registrados.

Na solução desenvolvida para este trabalho, o atributo regex foi retirado da arquitetura dos padrões. O trabalho anterior usou como identificador para as assinaturas do NIDS

strings, que descreviam de forma breve o alerta. No trabalho descrito neste estudo, esses são campos numéricos e únicos. Logo, o processamento dessa informação, principalmente quanto se trata do mapeamento, foi diferente. Não houve necessidade de um campo de regex, e por isso ele foi removido.

Houve a inserção de um novo módulo auxiliar, o mapeamento de assinaturas, que apesar de não participar ativamente do fluxo de segurança, se prova importante na hora de otimizar os processos do sistema. Com ele, a partir de um pacote de regras de NIDS inicial, é gerado um arquivo de mapeamento de MITRE ATT&CK para assinaturas de rede, que funciona com um banco de dados chave-valor. A existência desse arquivo possibilita um mapeamento mais rápido das informações, e também permite maior flexibilidade do sistema. Outro ponto positivo é que esse arquivo garante uma consistência nos mapeamentos, uma vez que as associações entre assinaturas de rede e identificadores do MITRE ATT&CK são centralizadas e armazenadas. Além disso, permite ajustes rápidos e eficientes, permitindo a atualização de regras de forma ágil, conforme ajustes são necessários.

3.5 *Setup* Experimental

A infraestrutura utilizada para os testes foi uma máquina do modelo MacBook Air com chip Apple M2, 8gb de memória unificada e 256gb de armazenamento. Houve virtualização com Docker, que foi configurado para ter acesso total aos recursos da máquina.

A partir de relatórios de inteligência de CTI da TIP, provenientes das fontes MITRE [32], MISP [33] e AlienVault [34], foram construídos com o uso do IPO padrões para cada caso de teste. Para avaliar o desempenho dos padrões, foi criado um ambiente de testes que simula os registros de redes de um sistema em ataque, permitindo verificar a eficiência da funcionalidade de correspondência de padrões. Através de um *script*, foram gerados *logs* artificiais da ferramenta Suricata, imitando o tráfego de rede associado a uma ameaça selecionada. Os dados de inteligência usados para gerar esses registros foram obtidos do Hybrid Analysis [31]. Esses dados foram processados pelo *script*, que extraiu suas TTPs e referências ATT&CK, mapeando essas informações para as assinaturas configuradas do NIDS para gerar um arquivo de *log* no formato definido. Um exemplo simplificado de como funciona o formato dos eventos de rede desse *log* é mostrado abaixo:

```
{
    "timestamp": "2024-09-11T05:53:01.125448",
    "event_type": "alert",
    "src_ip": "192.168.1.1",
    "src_port": 52227,
    "dest_ip": "192.168.1.2",
```

```
    "dest_port": 33282,
    "proto": "TCP",
    "alert": {
        "action": "blocked",
        "signature_id": "2019650",
        "signature": "Alert for technique T1036",
        "severity": 1
    }
}
```


Uma avaliação precisa do programa desenvolvido exige a seleção de relatórios de CTI que não tenham sido previamente utilizados para compor o banco de dados do TIP. Essa estratégia é essencial para evitar vieses na análise do desempenho do software, garantindo que os padrões não estejam familiarizados com os dados. Do contrário, haveria o risco de obter uma taxa de sucesso artificialmente elevada. Essa abordagem assegura que a validação dos padrões de detecção seja realizada de forma justa, refletindo a eficácia do programa em um cenário realista. O formato de *log* reflete o comportamento esperado em um cenário real de detecção de ameaças, com eventos de rede detalhando dados do pacote, seguido do alerta com assinatura correspondente à técnica ATT&CK detectada.

3.6 Casos de Teste

Para avaliar o sistema desenvolvido, foram selecionados quatro casos de teste baseados em grupos de ataque, dessa forma representando uma ampla variedade de metodologias utilizadas. Foram selecionados ataques do grupo hacker Lazarus [35], que tem mais de 10 anos de atividade. Blackcat [36], um ransomware ativo desde 2021. Kimsuky [37], um APT norte-coreano. E, por fim, Apt 28 [38], do grupo de espionagem russo Fancy Bear. A escolha inclui grupos com histórico significativo de atividades, como Lazarus e APT 28, bem como ameaças mais recentes, como Blackcat e Kimsuky. Isso permite cobrir diferentes tipos ataques cibernéticos, como *ransomwares* e APTs.

3.6.1 Lazarus

O Lazarus é um grupo hacker que atua desde 2010. É alegado que tem forte vinculo com a Coreia do Norte [35]. São atribuídos a eles vários ataques bem sucedidos, como o roubo de 12 milhões do Banco del Austro do Equador [39], o de 81 milhões de dólares do Banco de Bangladesh [40], e outro de 60 milhões de dólares do Far Eastern International Bank, do Taiwan [41]. Também é reportado como responsabilidade deles um dos mais famosos

casos de *ransomware*, o WannaCry, que infectou mais de 300 mil computadores no mundo todo.

3.6.2 Blackcat

O Blackcat é um *ransomware* recente, também conhecido como ALPHV, e é um grupo de origem russa [36]. O seu malware é programado em RUST e ataca empresas de vários setores diferentes. Opera em um modelo de Ransomware como Serviço (RaaS), no qual os criadores do malware permitem que outros grupos o utilizem, em troca de uma porcentagem do dinheiro de resgate.

3.6.3 APT28

O APT28 é um notório grupo de espionagem russo, também conhecido como Fancy Bear, com evidências sugerindo uma relação com a agência de inteligência deste país. Seus alvos incluem governos do leste europeu como a Geórgia e Ucrânia, mas também já realizou ataques à organizações internacionais, como a NATO e algumas agências americanas.

3.6.4 Kimsuky

O Kimsuky é um APT que é geralmente associado com o território norte coreano. Seus alvos na maior parte das vezes são organizações sul coreanas, porém, sua gama de vítimas tem se expandido, com ataques conhecidos ao Estados Unidos, Rússia e nações europeias. O grupo tem demonstrado alta atividade em 2024.

3.7 Síntese do Capítulo

Este capítulo apresentou a metodologia aplicada no *software* desenvolvido, visando atacar o problema de ineficiência presente em arquiteturas de cibersegurança com o uso CTI para detectar e responder incidentes de maneira acionável. Isso é feito a partir da metodologia proposta em Cristoffer et al [1], através de uma nova implementação do Orquestrador de Padrões de Inteligência (IPO). Essa solução é dividida em quatro módulos que atuam de forma conjunta para realizar duas funcionalidades: Construção de Padrão e Correspondência de Padrões. Os padrões são produzidos a partir de informações de CTI correlacionadas de diferentes relatórios de inteligência, que são filtradas e utilizadas para criar padrões que descrevem as técnicas dos adversários em rede através de TTPs. Esses padrões descrevem ameaças observadas anteriormente, o que permite detectar novas

instâncias dessas ameaças em eventos de rede, gerando assim inteligência acionável para detecção e resposta a incidentes.

Foram discutidas as contribuições em relação ao trabalho base, destacando as diferenças de abordagem e implementação feitas durante o desenvolvimento da pesquisa. Também são descritas as configurações dos experimentos, com o detalhamento do ambiente de testes, e explicando a utilização de um *script* que gera *logs* do Suricata a partir de exemplos de ameaças reais. Os casos de teste são apresentados, consistindo de grupos *hackers* conhecidos por ataques de *ransonware* e APTs.

Capítulo 4

Implementação

Neste capítulo, é discutido o desenvolvimento do software e as decisões de implementação. Na Seção 4.1, são discutidas as integrações necessárias para o funcionamento do IPO, detalhando como o sistema se conecta com o NIDS e a TIP. É abordada na Seção 4.2 a definição da interface do sistema e das funcionalidades necessárias. É descrita na Seção na 4.3 as ferramentas de desenvolvimento utilizadas. Na Seção 4.4, são explorados detalhes de implementação dos módulos. E, para fechar o capítulo, é realizada sua síntese na seção 4.5.

4.1 Integrações

Dois componentes de segurança adicionais são essenciais para a implantação do IPO: NIDS e TIP. Nessa seção é descrito como foram feitas essas integrações e as ferramentas escolhidas.

4.1.1 OpenCTI

O OpenCTI foi a Plataforma de Inteligência de Ameaças (TIP) escolhida para ser integrada com o IPO na execução desse projeto. É uma plataforma *open-source* reconhecida pela sua flexibilidade e capacidade de integração. Ademais, é eficiente em seus processos e lida bem com grandes volumes de informações. Ferramentas de correlação, contextualização e grafos estão incluídas na plataforma, facilitando o manejo dos dados. Na plataforma, é possível injetar dados de diversas fontes de CTI. No ambiente em questão, a base de dados foi populada a partir das seguintes fontes de CTI: MISP, AlienVault e MITRE.

Cada entidade no OpenCTI recebe um identificador único, permitindo uma gestão eficiente dos relatórios de inteligência por parte do orquestrador. Também tem como ponto positivo a sua API em GraphQL, permitindo chamadas personalizáveis e evitando

que o operador de segurança tenha que interagir diretamente com a plataforma para acessar a base de dados. Além disso, Possui compatibilidade com o *framework* MITRE ATT&CK, mantendo referências a matriz em vários objetos de CTI. Estas características foram um fator importante para sua seleção no projeto.

4.1.2 Suricata e *Emerging Threats*

O ambiente desenvolvido conta com a presença do Sistema de Detecção de Intrusões de Rede (NIDS) denominado Suricata. É uma ferramenta reconhecida pelo mercado e amplamente utilizada. Além de uma boa capacidade de inspeção de pacotes de rede, é bem flexível e possui uma série de funcionalidades. Pode ser configurada com regras personalizadas e que são compatíveis com outros NIDS, facilitando sua adaptação e escalabilidade. Essas fatores fazem com que o Suricata seja uma opção eficaz e robusta para a prevenção de intrusões.

O pacote de regras *EF Open Ruleset* provido pela *Emerging Threats* (EF), possui inúmeras assinaturas feitas por uma equipe de especialistas de segurança. Nessas regras, já estão incluídas referências para a matriz MITRE ATT&CK e identificadores de assinatura únicos. Tendo isso em vista, esse pacote foi usado para configurar o Suricata no ambiente de testes.

4.2 Fluxo de Usuário

Antes da implementação do Orquestrador de Padrões de Inteligência, a criação de um diagrama de casos de uso permitiu visualizar como os diferentes módulos se comportariam na perspectiva do usuário. A partir do diagrama, que pode ser visualizado na Figura 4.1, foram projetadas três funcionalidades: registrar novo padrão, mapear assinaturas, e verificar *logs*.

Para iniciar o programa, basta apenas executar seu *script* de arranque. A tela inicial dá acesso a todas as funcionalidades, como é possível notar na Figura 4.2. A interação do usuário com o software é feita por CLI, usando o terminal para navegação e impressão das informações.

A funcionalidade de registro de um novo padrão exige que o usuário forneça um nome para o padrão a ser criado, além de especificar o identificador de um relatório proveniente do OpenCTI, selecionando a ameaça na qual o padrão será fundamentado. Com essas informações, o Orquestrador de Padrões de Inteligência é capaz de acessar os dados detalhados da ameaça base, realizando as etapas necessárias para a construção do padrão. O padrão gerado é então armazenado em um arquivo no formato JSON, facilitando sua integração e uso posterior.

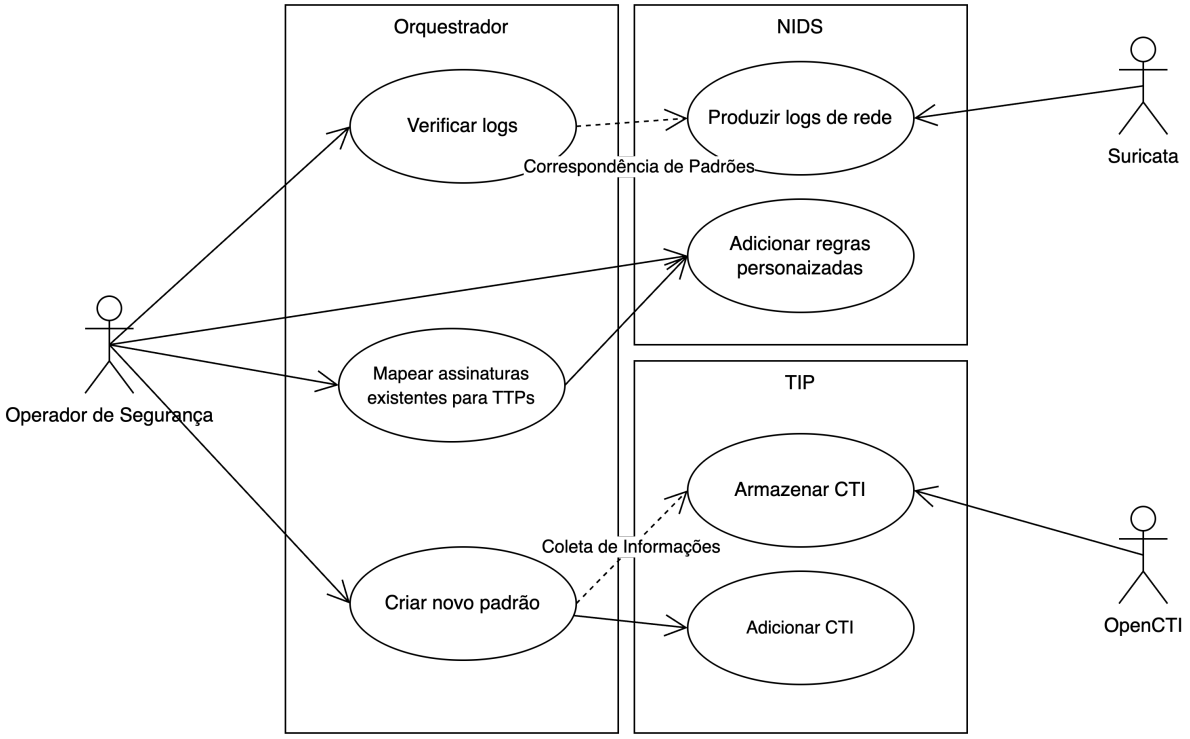

Figura 4.1: Diagrama de casos de uso de um modelo de segurança implementado com IPO.

```
1. Registrar novo padrão
2. Mapear Assinaturas
3. Verificar registros de rede
Pressione qualquer outra tecla para encerrar o programa
Escolha uma opção:
```

Figura 4.2: Tela inicial do IPO.

Na função de mapear de assinaturas, o usuário deve fornecer o pacote de regras utilizado na NIDS, no formato .rules. O algoritmo, por sua vez, examina as regras em busca dos identificadores únicos das assinaturas e das referências relacionadas ao MITRE ATT&CK, associando as técnicas específicas utilizadas para gerar os alertas de rede. Após essa análise, o Orquestrador de Padrões de Inteligência armazena o mapeamento resultante em um arquivo .json, que funciona como um banco de dados do tipo chave-valor, possibilitando consultas rápidas e a integração eficiente dos dados.

A funcionalidade denominada "Verificar Logs", permite a avaliação dos padrões registrados no banco de dados em relação aos *logs* de rede fornecidos pelo usuário. O algoritmo gera uma pontuação de correspondência para cada padrão, indicando o grau de similaridade com os dados inseridos, e também imprime as técnicas do MITRE ATT&CK

detectadas no registro.

4.3 Ferramentas de Desenvolvimento

Para escrita do código, foi utilizada a linguagem de programação Python na sua versão 3.11.5, com gerenciamento via pip para instalação de dependências. A IDE principal foi o Visual Studio Code 1.91.0. O controle de versão foi feito através do Git 2.42.0, com integração com o Github, a fim de facilitar o gerenciamento do código. Foi utilizado também o Docker 4.25.0 para a virtualização, permitindo a criação de um ambientes isolados para testes e execução do sistema e de suas dependências. Além disso, foi utilizado a versão do OpenCTI 5.11.12 Community Edition.

A escolha por Python como linguagem principal foi motivada por sua flexibilidade, aliada à vasta gama de bibliotecas disponíveis. A linguagem oferece integrações com diversos *frameworks* e TIPs, como o OpenCTI e ATT&CK. Além disso, a linguagem possui diferentes recursos para facilitar o manejo de dados, o que facilitou o desenvolvimento dos algoritmos necessários.

Com a utilização do docker no projeto foi possível criar um ambiente isolado e reprodutível, com todas as dependências e configurações necessárias, sem que fosse necessário preocupar-se com incompatibilidades entre versões de bibliotecas ou sistemas operacionais.

4.4 Detalhes de Implementação

Os chamados Objetos de Domínio Stix (SDOs) são uma forma de padronizar CTI, categorizando essas informações em entidades pré-definidas, como indicadores, ferramentas, vulnerabilidades, e outras. Essas entidades são usadas para formar relacionamentos que contextualizam um ataque, como exemplifica a Figura 4.3.

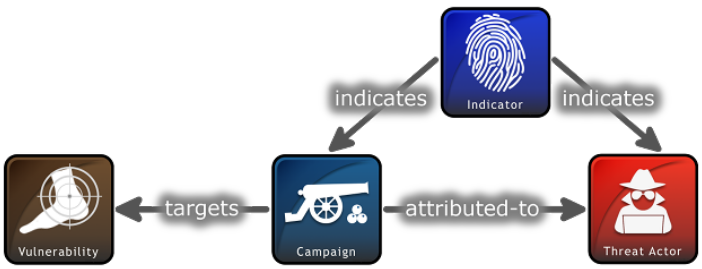

Figura 4.3: Exemplo de relacionamento STIX (Fonte: [15]).

Um relatório de segurança, é, na realidade, um agrupamento de SDOs. São importantes na implementação pois os dados de CTI no OpenCTI são expressos por esse tipo de objeto. Além disso, nessa padronização, cada entidade possui um identificador único. Esses identificadores são utilizados para selecionar um relatório de entrada para a construção de um padrão e para manipulação dos dados da TIP. Dessa forma, não é preciso armazenar os objetos completos em cada processo, basta guardar a referência por meio dos identificadores.

4.4.1 Coleta de Informação

Há várias abordagens possíveis para fazer a correlação de relatórios usando o OpenCTI. Uma delas é usar a funcionalidade já embutida na plataforma. O contraponto é que dessa forma perde-se controle do que está sendo usado para fazer essa correlação. Então, para realizar esse processo de forma mais refinada e evitar a formação de padrões de baixa qualidade, foram priorizados SDOs do tipo Indicador. Os indicadores têm natureza investigativa e servem para especificar condições particulares que podem indicar a presença de uma determinada TTP, juntamente com informações contextuais relevantes [42]. A correlação é feita através da busca desses indicadores em outros relatórios, através da API do OpenCTI.

4.4.2 Filtro e Ranqueamento

No formato STIX, os SDOs são compostos por dezoito diferentes tipos de entidades [15]. Para ranquear as informações de CTI da TIP, é atribuído a cada tipo de entidade um nível da escala DML. Relatórios contendo apenas objetos de nível DML-3 ou inferior, ou seja, que só possuem CTI de baixo nível, são considerados irrelevantes e descartados do processo. Entretanto, seus IoCs são enviados para o Suricata. Para realizar esse processo, são feitas chamadas à API do OpenCTI, buscando todas as entidades relacionadas a um determinado relatório. Com isso, é possível aplicar o filtro com base no ranqueamento estabelecido para cada relatório avaliado.

4.4.3 Construção de Padrão

Entre a CTI de alto nível, se destacam as TTPs, pois são chave na construção de um padrão. As TTPs correspondem aos SDOs de tipo *Attack Pattern* (padrão de ataque). Além disso, o resto dos objetos constituem o que foi denominado de CTI contextual, que compreende as informações de alto nível encontradas, mas que não são padrões de ataque. Com essa separação da CTI em duas listas, TTPs e CTI contextual, obtemos na primeira

em a informação comportamental necessária para construir o padrão, e na segunda um contexto útil na hora de auxiliar os operadores na resposta a incidentes.

Para associar os padrões de ataque com a matriz MITRE ATT&CK, utilizam-se as referências registradas nas entidades do OpenCTI, na qual os objetos de padrão de ataque geralmente incluem o identificador ATT&CK relacionado. Usando as assinaturas da NIDS, realiza-se a transformação das TTPs em eventos de rede, definindo assim o atributo eventos, primordial na estrutura do padrão. O padrão gerado ao final desse processo é expresso em um arquivo em formato JSON e pode potencialmente ficar armazenado em um banco de dados.

4.4.4 Correspondência de Padrão

Com o uso do pacote de regras da *Emerging Threats*, uma mesma TTP pode estar associada a múltiplos eventos de rede. Na implementação realizada, os eventos de rede que correspondem ao padrão são convertidos novamente em TTPs e avaliados com base nisso, removendo-se as técnicas duplicadas. O algoritmo percorre o registro em busca de eventos do tipo alerta. Para cada alerta, são extraídas as assinaturas identificadoras, as quais são utilizadas para localizar as TTPs detectadas naquele registro. Desse modo, é possível calcular a similaridade das técnicas encontradas e as técnicas de cada padrão.

4.4.5 Mapeamento de Assinaturas

Essa função auxiliar permite a criação de um arquivo que funciona como banco de dados *key-value*, onde a chave é uma assinatura do Suricata, e valor o identificador mitre da TTP relacionada. O Suricata foi configurado para usar o pacote de regras *EF Open Ruleset*. Então, para mapear as TTPs para assinaturas do NIDS, foi desenvolvida uma função que percorre as regras do pacote e busca suas respectivas referências no MITRE ATT&CK. Como resultado, é gerado um arquivo de mapeamento a partir dessas regras. Dessa forma, o orquestrador pode realizar mapeamentos rápidos entre TTPs e assinaturas, ou vice-versa, sempre que necessário.

4.5 Síntese do Capítulo

Este capítulo sintetizou os elementos que compõem a estrutura de segurança, destacando a integração do OpenCTI como banco de dados (TIP) e do Suricata como NIDS, além de explorar a interação do usuário com o sistema e seus casos de uso. Também foram abordados aspectos técnicos da implementação, como as ferramentas de desenvolvimento

utilizadas, e o conceito de Objetos de Domínio STIX (SDOs), fundamentais para o entendimento dos módulos. Também foram discutidas as escolhas realizadas durante a implementação, incluindo o uso do pacote de regras do Emerging Threats.

Capítulo 5

Resultados

Esse capítulo apresenta os resultados obtidos na execução do *software* desenvolvido. A Seção 5.1 apresenta os resultados para o caso de teste do Lazarus, a Seção 5.2 para o BlackCat, a Seção 5.3 para o APT28 e a Seção 5.4 para o Kimsuky. A seção 5.5 discute os resultados obtidos. A Seção 5.6 consiste de estatísticas do projeto. Adicionalmente, a Seção 5.7 discorre sobre os experimentos que foram realizados durante a implementação do software. Por fim, o capítulo é resumido na Seção 5.8.

5.1 Lazarus

Como é possível observar na Figura 5.1, embora tenha ocorrido uma grande correlação entre os registros de rede do Lazarus e seu padrão, com 55% de correspondência, o orquestrador indicou que a ameaça mais provável era o Kimsuky, com 66% de correspondência.

```
4. Pattern matching
Log file to be analized:
lazarus

Matching score with the registered patterns: (0 to 100)
kimsuky - 66.67
lazarus - 55.56
apt28 - 30.00
blackcat - 33.33

(6) signatures with identified TTPs:
Signature 2035027: Mitre Technique ID T1036, Mitre Tactic ID TA0005
Signature 2008327: Mitre Technique ID T1027, Mitre Tactic ID TA0005
Signature 2025709: Mitre Technique ID T1570, Mitre Tactic ID TA0008
Signature 2046045: Mitre Technique ID T1005, Mitre Tactic ID TA0009
Signature 2016476: Mitre Technique ID T1071, Mitre Tactic ID TA0011
Signature 2016476: Mitre Technique ID T1071, Mitre Tactic ID TA0011
```

Figura 5.1: Pontuação de correspondência com um *log* de Lazarus.

5.2 Blackcat

Usando os registros de rede do Blackcat como entrada, as pontuações são as demonstradas na Figura 5.2. Nesse teste, o padrão do Blackcat obteve a mesma pontuação de correspondência que o Kimsuky, com 33%. Apesar da pontuação de correspondência significativa, ela ainda é insuficiente para uma detecção conclusiva.

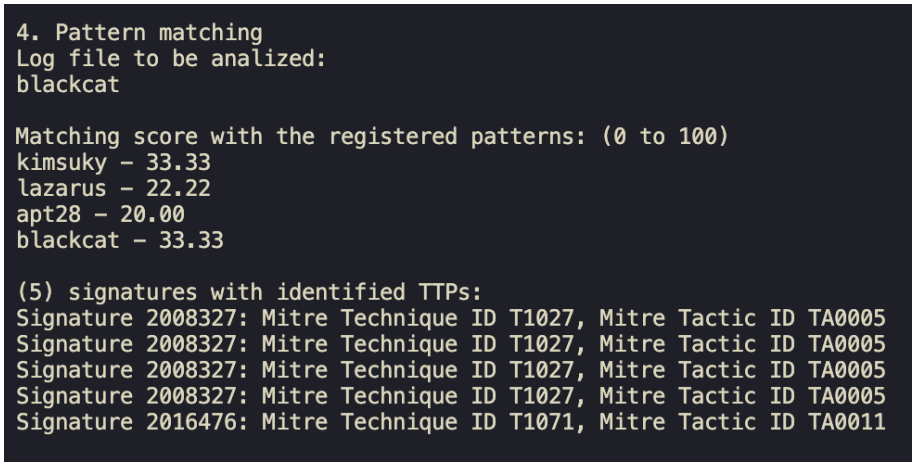

Figura 5.2: Pontuação de correspondência com um *log* de Blackcat.

5.3 APT28

Como pode ser observado na Figura 5.3, é perceptível que o sistema encontrou correspondências baixas com os padrões registrados. O padrão do APT28 obteve apenas 30% de pontuação de correspondência, valor próximo ao do Kimsuky e Blackcat, que atingiram ambos 33%.

5.4 Kimsuky

Os resultados para o Kimsuky, que podem ser vistos na Figura 5.4, revelaram uma correspondência de 83% com seu padrão. Além disso, os TTPs do Lazarus foram altamente correspondidos, com 67% de pontuação.

5.5 Análise dos Resultados

A Tabela 5.1 sintetiza os resultados obtidos, com as pontuações de correspondência (PC) de cada caso de teste em relação aos padrões desenvolvidos para as diferentes ameaças.

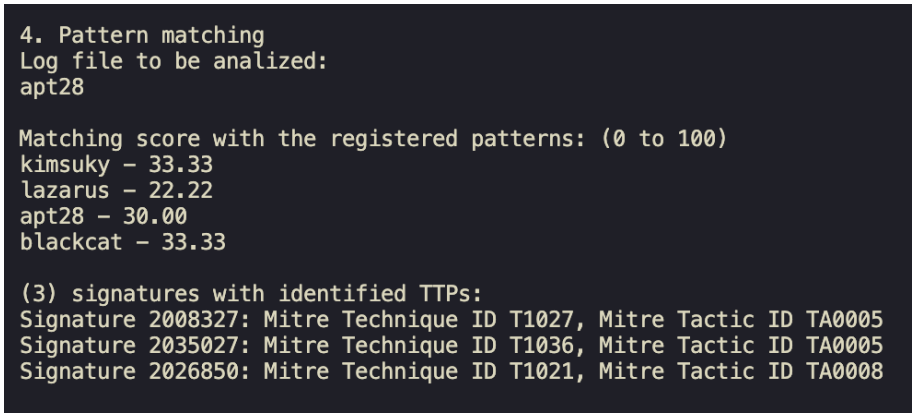

Figura 5.3: Pontuação de correspondência com um *log* de APT 28.

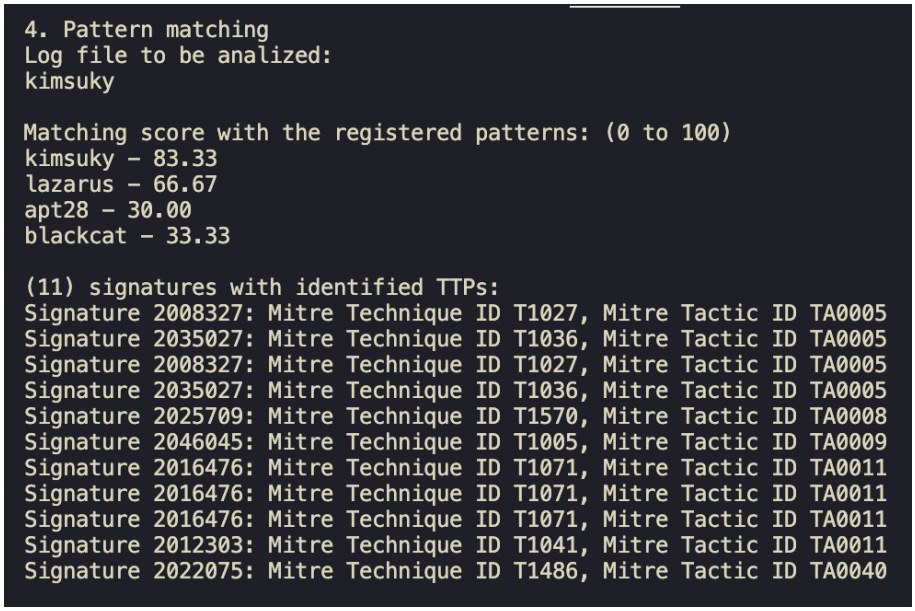

Figura 5.4: Pontuação de correspondência com um *log* de Kimsuky.

No caso de teste do Lazarus, observou-se uma grande correspondência com seu padrão relacionado, apresentando 56% de pontuação. No entanto, a ameaça mais provável foi identificada como Kimsuky, com 66% de correspondência. Isso potencialmente se deve pela grande variabilidade de metodologias já utilizadas por esse grupo em diferentes campanhas, o que dificulta a obtenção de uma correspondência alta quando resumido a um único ataque. Durante sua longa história, o Lazarus executou uma ampla gama de ataques, empregando técnicas variadas em cada campanha, incluindo ataques de APTs, similar ao Kimsuky. Esse fator pode ter influenciado nos resultados obtidos nesse teste.

O caso BlackCat apresentou baixa correspondência com todos os padrões, inclusive o seu próprio, com 33% de pontuação. Esse resultado é esperado em relação aos outros

Padrão	PC(Log Lazarus)	PC(Log Blackcat)	PC(Log Apt28)	PC(Log Kimsuky)
Lazarus	56%	22%	22%	67%
Blackcat	33%	33%	33%	33%
APT28	30%	20%	30%	30%
Kimsuky	66%	33%	33%	83%

Tabela 5.1: Tabela com as Pontuações de Correspondência obtidas para cada padrão testado.

padrões, logo que o BlackCat é o único grupo especializado somente em ransomware, o que o torna distinto dos demais. É possível notar que os grupos que já realizaram ataques persistentes têm uma pontuação de correspondência menor quando comparados ao registros de redes de um ataque ransomware. Isso sugere que essas pontuações são influenciadas por semelhanças no estilo de ataque. Além disso, quando um padrão tem poucos TTPs vinculados, sua pontuação se infla ou decai rapidamente, como é o caso do BlackCat, o que pode ter contribuído para a baixa pontuação obtida.

A análise do log *log* APT28 revelou pontuações de correspondência baixas para todos os padrões, com apenas 33% de pontuação de correspondência em relação ao padrão criado para essa ameaça, o que é equivalente à pontuação obtida pelo Kimsuky nesse caso de teste. Assim como no Lazarus, é possível que a baixa pontuação de correspondência se deva à variação de metodologias, uma vez que o APT28 é outro grupo com um histórico longo de atividades.

Para o registro de rede de uma ameaça do grupo Kimsuky, foi observada uma alta correspondência com o padrão construído, com 83% de pontuação. Um fator que impacta os resultados é a qualidade dos relatórios da TIP. É possível que com uma disponibilidade maior de relatórios recentes sobre essa ameaça, teria sido criado um padrão melhor para o Kimsuky, refletindo no alta pontuação de correspondência obtida. Além disso, foi observada uma correspondência significativa com o Lazarus, assim como no primeiro caso de teste, o que demonstra que os dois padrões compartilham elementos em comum.

5.6 Estatísticas

A Tabela 5.2 resume as principais estatísticas do projeto, apresentando números relacionados à construção de cada padrão utilizado como caso de teste. Estão inclusos dados como o tempo de execução total, o número de relatórios correlacionados e relevantes, além da quantidade de Técnicas, Táticas e Procedimentos encontradas e mapeadas. Essas métricas são essenciais para avaliar o desempenho nas diferentes fases de processamento do Orquestrador de Padrões de Inteligência.

	Lazarus	**Blackcat**	**APT28**	**Kimsuky**
Relatórios Correlacionados	7	4	6	3
Relatórios Relevantes	7	4	6	3
TTPs Encontrados	39	22	45	26
TTPs Mapeados	9	3	10	6
Tempo de Execução (s)	151,99	57,20	125,42	31,82

Tabela 5.2: Estatísticas para cada caso de teste.

Observa-se que o número de relatórios correlacionados para Lazarus e APT28 foi superior aos dos outros dois grupos, o que pode ser atribuído ao longo período de relevância dessas organizações criminosas. Em todos os casos de teste, nenhum relatório foi considerado irrelevante, o que demonstra a alta qualidade das informações armazenadas e das fontes de CTI conectadas à TIP.

Percebe-se também que a quantidade de TTPs que podem ser mapeadas para eventos de rede é baixa, o que resulta em uma perda significativa de informação, pois nem todas são detectáveis por dados de rede. Esse cenário levanta a questão de como seria possível ampliar esse escopo.

Uma relação direta é observada entre o número de relatórios correlacionados e o tempo de execução, sendo esse o processo com mais demanda de tempo. Esse comportamento reflete a complexidade e o esforço computacional necessários para identificar padrões e conexões entre os dados.

5.6.1 Dataset

O banco de dados da TIP (OpenCTI) foi alimentado com dados provinentes de *feeds* do MISP, AlienVault e MITRE Datasets. Essas informações são transmitidas por meio de mensagens em conectores, e a volumetria dos dados recebidos pode ser observada na Tabela 5.3.

Conector	**Quantidade de Mensagens (milhares)**
Misp Feed	3.740,2
AlienVault	112,23
MITRE Datasets	93,3

Tabela 5.3: Mensagens trocadas entre TIP e diferentes fontes de CTI.

É possível observar que a maior parte desses dados provém dos feeds do MISP, sendo essa a principal fonte de dados da TIP. De maneira geral, foram adicionados à base de dados:

- 279.280 entidades
- 238.320 relações
- 1.110 relatórios
- 268.930 observáveis

Embora o MISP seja responsável pela maior quantidade de dados, um estudo dos dados do sistema revelou que a maior parte dos relatórios tem origem no AlienVault, sendo esta a fonte de 91% dos relatórios do sistema. No total, foram inseridos 21 gigabytes de dados de CTI na TIP.

5.7 Experimentos

A maior parte da experimentação foi realizada no módulo de Coleta de Informação, mais especificamente na correlação de relatórios. Encontrar um equilíbrio em que a coleta não seja tão restrita mas que também não fuja do escopo da ameaça é uma tarefa desafiadora. Houve uma tentativa de incluir no processo de correlação mais atributos contextuais, como padrões de ataque, *malware* utilizado e grupo associado. Porém, ao adicionar esses atributos, observou-se um grande incremento no número de relatórios relacionados, o que aumentava o tempo de execução e trazia resultados de menos qualidade, pois nem todo relatório novo tinha uma relação realmente coerente com a ameaça de entrada.

5.8 Síntese do Capítulo

Este capítulo apresenta resultados obtidos no estudo, incluindo os dados brutos e algumas ponderações sobre cada um deles, como a sobreposição de técnicas em mais de uma ameaça, a diversidade de metodologia de ataques, e a influência da quantidade de CTI na TIP. São abordadas estatísticas que resumem vários aspectos do projeto, como dados sobre cada padrão construído, incluindo tempo de execução, relatórios correlacionados e TTPs mapeados, observando-se uma forte correlação entre a quantidade de relatórios correlacionados e tempo de execução. Além disso, apresenta dados sobre o *Dataset* presente na TIP, que foi o banco de dados do Orquestrador de Padrões de Inteligência. O capítulo é encerrado abordando experimentos realizados para tentar tornar a solução mais eficiente, detalhando os resultados encontrados.

Capítulo 6

Conclusão

Os testes realizados com os quatro diferentes grupos de ataque: Lazarus, Blackcat, APT28 e Kimsuky, evidenciaram os desafios no desenvolvimento de sistemas de detecção baseados em padrões de CTI. O sistema apresentou capacidade de identificar TTPs entre os registros de rede, porém os resultados relacionados à correspondência de padrões ficaram aquém do esperado. Entretanto, alguns casos de teste demonstraram o potencial da solução.

É evidente que, pela pouca quantidade de TTPs mapeáveis para rede, ocorre uma sobreposição significativa sobre elas, principalmente em estilos de ataques similares, o que pode gerar resultados imprecisos. Como os grupos Lazarus e Kimsuky possuem metodologias de ataques similares, suas pontuações de correspondência apresentam valores próximos quando avaliados com padrões relacionados. No caso de teste do Lazarus, essa semelhança gera uma análise que aponta o Kimsuky como suspeito principal. Esse resultado sugere que há pouca informação disponível em rede para fazer diferenciações mais precisas sobre diferentes atacantes.

A análise do comportamento dos grupos que realizaram ataques persistentes, comparados aos registros de rede de ataques do tipo ransomware (BlackCat), revela aspectos significativos na detecção e categorização de ameaças. A pontuação de correspondência mais baixa para os grupos de ataques de persistência pode ser atribuída à natureza distinta de suas táticas e técnicas. Ataques de persistência frequentemente se concentram na manutenção de acesso a sistemas-alvo ao longo do tempo, utilizando métodos que priorizam furtividade e controle prolongado, enquanto ataques de ransomware, como os associados ao BlackCat, são tipicamente mais diretos, focados em criptografar dados para extorquir vítimas. Essa análise sugere que o IPO pode contribuir para a identificação do tipo de ameaça em questão.

Analisando o caso de teste do APT28, o padrão construído possui baixa pontuação de correspondência para todos os testes realizados. Acredita-se que o uso de diferentes

metodologias pelo grupo ao longo do tempo comprometeu a correspondência do padrão com seus ataques mais recentes. Lidar com essa variabilidade é algo necessário para construir padrões coerentes.

A detecção do Kimsuky, por sua vez, demonstra a viabilidade da construção de padrões para a identificação de ameaças. Esse resultado positivo provavelmente foi influenciado pela grande quantidade de CTI que tem sido disponibilizada recentemente sobre essa ameaça. Esses dados, por serem atualizados e de maior qualidade, contribuíram para a construção de um padrão de correspondência robusto, mesmo com uma quantidade não tão grande de relatórios. A TIP populada com fontes confiáveis permite que o processo de coleta de informação funcione de forma coerente, criando padrões mais completos para as ameaças.

O Orquestrador de Padrões de Inteligência foi inicialmente projetado para construir padrões e estabelecer correspondências com diferentes famílias de *malware*. Aplicar essa metodologia em um gama mais abrangente de ameaças, como feito no presente estudo, pode ter comprometido os resultados, gerando padrões menos coerentes. Um manejo mais cuidadoso das informações durante o processo de criação dos padrões é essencial para lidar com os diferentes tipos de ameaças.

Diante das evidências apresentadas, é possível concluir que o IPO desenvolvido neste projeto não foi capaz de garantir que a correspondência de padrões ocorresse de forma consistente, não atingindo o objetivo de facilitar o processo de resposta a incidentes com o uso de inteligência acionável. No entanto, a identificação das técnicas de ataque empregadas em eventos de rede e os resultados obtidos em certos casos de teste demonstraram o potencial da metodologia de realizar esse processo. Ajustes no software implementado e mudanças pontuais na metodologia, especialmente em relação aos diferentes tipos de ameaças, podem permitir que o Orquestrador de Padrões de Inteligência alcance o objetivo para o qual foi projetado.

6.1 Melhorias e Trabalhos Futuros

O projeto está todo em uma interface de linha de comando (CLI). A implementação de uma interface gráfica tornaria o programa mais amigável e facilitaria a visualização das informações. Também seria possível adicionar funcionalidades interessantes, como destacar as TTPs encontradas e visualização dos relatórios de CTI. Como a integração com o OpenCTI ainda não está completa, não é possível usar o projeto de forma totalmente isolada. É necessário abrir a TIP para inserir dados da ameaça ou pegar o identificador da ameaça de interesse.

O código apresenta espaço para otimização, o uso de TTPs ao invés de eventos nos padrões aumentaria a velocidade de certos procedimentos, e também facilitaria a adaptação a novas regras registradas. O módulo de filtragem e ranqueamento poderia ser revisado, tornando esse processo mais direto e eficiente. O mapeamento das assinaturas também poderia ser mais organizado.

A separação das ameaças em campanhas poderia trazer padrões mais coerentes. Considerando que grupos mudam suas metodologias com o passar do tempo. Além disso, a exploração de métodos mais avançados de correlação de padrões, como o uso de técnicas de aprendizado de máquina nas TTPs, pode aumentar significativamente a precisão do sistema.

A aplicação do software em um ambiente totalmente real, o uso do orquestrador em uma simulação controlada seria interessante para ver o desempenho da solução e a efetividade da metodologia proposta.

Uma questão interessante não respondida de forma sólida foi como o programa lida com os diferentes tipos de ameaças, e, caso haja distinção de resultados, explorar formas de adaptá-lo para lidar de maneira mais eficiente com essas divergências. Além disso, o orquestrador nesse momento é limitado a eventos de rede, levantando a questão de como expandir esse escopo para aprimorar a detecção de atacantes.

Outro ponto relevante é o processo de correlação de relatórios, particularmente na definição de quais entidades contextuais são mais adequadas para esse fim. Um manejo mais refinado das informações de CTI pode contribuir para a construção de padrões mais consistentes e eficazes.

Referências

[1] Leite, Cristoffer, Jerry den Hartog, Daniel Ricardo dos Santos e Elisa Costante: *Actionable cyber threat intelligence for automated incident response*. Em Reiser, Hans P. e Marcel Kyas (editores): *Secure IT Systems*, páginas 368–385, Cham, 2022. Springer International Publishing, ISBN 978-3-031-22295-5. viii, 1, 10, 12, 13, 14, 15, 22, 25

[2] Pokorny, Zane: *The Threat Intelligence Handbook: Moving toward a security intelligence program*. Annapolis, CyberEdge Group, 2019. 1

[3] Barnum, Sean: *Standardizing cyber threat intelligence information with the structured threat information expression (stix)*. Mitre Corporation, 11:1–22, 2012. 1, 7

[4] Chadwick, David W, Wenjun Fan, Gianpiero Costantino, Rogerio de Lemos, Francesco Di Cerbo, Ian Herwono, Mirko Manea, Paolo Mori, Ali Sajjad e Xiao Si Wang: *A cloud-edge based data security architecture for sharing and analysing cyber threat information*. Future Generation Computer Systems, 102:710–722, 2020, ISSN 0167-739X. `https://www.sciencedirect.com/science/article/pii/S0167739X19300895`. 1

[5] Pincovscy, João Alberto: *Metodologia para inteligência de ameaças cibernéticas com integração de sensores*. Dissertação (mestrado em engenharia elétrica), Universidade de Brasília, Brasília, 2022. 1

[6] Tounsi, Wiem: *What is Cyber Threat Intelligence and How is it Evolving?*, páginas 1–49. abril 2019, ISBN 9781786304483. 1

[7] Chismon, D. e M. Ruks: *Threat intelligence: Collecting, analysing, evaluating*. Relatório Técnico, "MWR InfoSecurity Ltd", 2015. 3

[8] Dalziel, H.: *How to Define and Build an Effective Cyber Threat Intelligence Capability*. Elsevier Science & Technology Books, 2014. 3

[9] US Joint Chiefs of Staff: *Joint Publication 2-0 Joint Intelligence*. Jt Publ, October 2013. 4

[10] National Institute of Standards and Technology (NIST): *Guide to cyber threat information sharing*. Special publication 800-150, National Institute of Standards and Technology, 2016. `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf`. 3, 5

[11] Gartner: *Definition: Threat intelligence*. https://www.gartner.com/doc/2487216/definition-threat-intelligence, 2013. 4

[12] Abu, Md Sahrom, Siti Rahayu Selamat, Aswami Ariffin e Robiah Yusof: *Cyber threat intelligence–issue and challenges*. Indonesian Journal of Electrical Engineering and Computer Science, 10(1):371–379, 2018. 4

[13] Webb, Jeb, Sean Maynard, Atif Ahmad, Graeme Shanks *et al.*: *Information security risk management: An intelligence-driven approach*. Australasian Journal of Information Systems, 18(3), 2014. 4

[14] Wagner, Thomas D., Khaled Mahbub, Esther Palomar e Ali E. Abdallah: *Cyber threat intelligence sharing: Survey and research directions*. Computers & Security, 87:101589, 2019, ISSN 0167-4048. `https://www.sciencedirect.com/science/article/pii/S016740481830467X`. 4, 6

[15] Open, OASIS: *Stix: Introduction*. `https://oasis-open.github.io/cti-documentation/stix/intro`, 2023. Accessed: 2024-09-15. 4, 6, 30, 31

[16] Connolly, Julie, Mark Davidson, Matt Richard e Clem Skorupka: *The mitre corporation on the trusted automated exchange of indicator information (taxii™)*. Relatório Técnico, The MITRE Corporation, August 2012. Accessed: 2024-09-08. 5

[17] Liao, Xiaojing, Kan Yuan, XiaoFeng Wang, Zhou Li, Luyi Xing e Raheem Beyah: *Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence*, página 755–766. Association for Computing Machinery, New York, NY, USA, 2016, ISBN 9781450341394. `https://doi.org/10.1145/2976749.2978315`. 5

[18] Guarascio, Massimo, Nunziato Cassavia, Francesco Sergio Pisani e Giuseppe Manco: *Boosting cyber-threat intelligence via collaborative intrusion detection*. Future Generation Computer Systems, 135:30–43, 2022, ISSN 0167-739X. `https://www.sciencedirect.com/science/article/pii/S0167739X22001571`. 6

[19] MITRE Corporation: *Mitre att&ck framework*, 2024. `https://attack.mitre.org`, Acesso em 6 setembro 2024. 6, 7

[20] Deloitte, B, J De Muynck e S Portesi: *Cyber security information sharing: An overview of regulatory and non-regulatory approaches*, 2015. 6

[21] Raghunath, Bane Raman e Shivsharan Nitin Mahadeo: *Network intrusion detection system (nids)*. Em *2008 First International Conference on Emerging Trends in Engineering and Technology*, páginas 1272–1277, 2008. 8

[22] Rawat, S.: *Navigating the cybersecurity landscape: Current trends and emerging threats*. Journal of Advanced Research in Library and Information Science, 10(3):13–19, 2023. 8

[23] *Itrc annual data breach report*. Relatório Técnico, Identity Theft Resource Center (ITRC), 2023. 8

[24] Silva, Alessandra de Melo e: *Metodologia integrativa para produção de inteligência de ameaças cibernéticas utilizando plataformas de código aberto*. Dissertação (mestrado profissional em engenharia elétrica), Universidade de Brasília, Brasília, 2020. 8, 9

[25] Alshamrani, Adel, Sowmya Myneni, Ankur Chowdhary e Dijiang Huang: *A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities*. IEEE Communications Surveys & Tutorials, PP:1–1, janeiro 2019. 8

[26] Bromander, Siri, Audun Jøsang e Martin Eian: *Semantic cyberthreat modelling*. Em *Semantic Technologies for Intelligence, Defense, and Security*, 2016. `https://api.semanticscholar.org/CorpusID:7525979`. 9, 17, 18

[27] Alam, Md Tanvirul, Dipkamal Bhusal, Youngja Park e Nidhi Rastogi: *Looking beyond iocs: Automatically extracting attack patterns from external cti*, 2023. `https://arxiv.org/abs/2211.01753`. 11

[28] Husari, G., E. Al-Shaer, M. Ahmed, B. Chu e X. Niu: *Ttpdrill: Automatic and accurate extraction of threat actions from unstructured text of cti sources*. Em *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017. [Online]. Available: `https://www.academia.edu/36127275/TTPDrill_Automatic_and_Accurate_Extraction_of_Threat_Actions_from_Unstructured_Text_of_CTI_Sources`. 11

[29] Rani, Nanda, Bikash Saha, Vikas Maurya e Sandeep Kumar Shukla: *Ttpxhunter: Actionable threat intelligence extraction as ttps from finished cyber threat reports*, 2024. `https://arxiv.org/abs/2403.03267`. 11

[30] Zhu, Z. e T. Dumitras: *Chainsmith: Automatically learning the semantics of malicious campaigns by mining threat intelligence reports*. Em *2018 IEEE European Symposium on Security and Privacy (Euro S & P)*, páginas 458–472. IEEE, April 2018. 11

[31] *Hybrid Analysis*. `https://www.hybrid-analysis.com/`. Accessed: 2024-09-11. 11, 23

[32] MITRE: *Mitre att&ck framework*. `https://attack.mitre.org`. Accessed: 2024-09-10. 23

[33] Project, MISP: *Misp threat intelligence feeds*. `https://www.misp-project.org/feeds/`. Accessed: 2024-09-10. 23

[34] AlienVault: *Open threat exchange (otx)*. `https://otx.alienvault.com/`. Accessed: 2024-09-10. 23

[35] Radware: *The lazarus group (apt38): North korean threat actor*, 2024. `https://www.radware.com/cyberpedia/ddos-attacks/the-lazarus-group-apt38-north-korean-threat-actor/`, Accessed: 2024-09-10. 24

[36] BlackBerry: *Blackcat: Ransomware protection*, 2024. https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/blackcat, Accessed: 2024-09-10. 24, 25

[37] Cybersecurity and Infrastructure Security Agency (CISA): *Aa20-301a: North korean advanced persistent threat activity, kimsuky*, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a, Accessed: 2024-09-10. 24

[38] CrowdStrike: *Who is fancy bear?*, 2024. https://www.crowdstrike.com/en-us/blog/who-is-fancy-bear/, Accessed: 2024-09-10. 24

[39] Symantec: *Swift attackers' malware linked to more financial attacks*. https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks. Accessed: 2024-09-08. 24

[40] *Two bytes to $951m*. https://baesystemsai.blogspot.co.uk. Accessed: 2024-09-08. 24

[41] Ashok, India: *Lazarus: North korean hackers suspected to have stolen millions in taiwan bank cyberheist*. International Business Times UK, 2017. https://www.ibtimes.co.uk/lazarus-north-korean-hackers-suspected-have-stolen-millions-taiwan-bank-cyberheis Accessed: 2024-09-08. 24

[42] STIX Project: *Ttps vs indicators*. https://stixproject.github.io/documentation/concepts/ttp-vs-indicator/#:~:text=TTPs%20describe%20what%20and%20how,those%20actions%20might%20look%20like, 2023. Accessed: 2024-09-15. 31