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

Gustavo Antonio Souza de Barros[1], **João José Costa Gondim**[2]

[1]Bacharelado em Engenharia de Computação
Universidade de Brasília (UnB) – Brasília, DF – Brazil

[2]Departamento de Engenharia Elétrica
Universidade de Brasília (UnB) – Brasília, DF – Brazil

gustavoasb@gmail.com, gondim@unb.br

Abstract. *Detecting cyberattacks is a complex task, as it requires the analysis of a large volume of data. In this scenario, automating parts of the process is essential. Cyber Threat Intelligence consists of collecting, processing, and analyzing data related to attacks, where network traffic acts as a key source of information. The developed software constructs attack patterns based on past incidents and evaluates the match between these patterns and network logs, aiming to identify potential attackers and the techniques employed. The tests were conducted using artificial logs that simulate an attack, and the results indicate that the approach has potential, although refinements are needed for effective application in real-world scenarios.*

Resumo. *A detecção de ciberataques é uma tarefa complexa, pois exige a análise de grandes volumes de dados. Nesse cenário, a automação de partes do processo é essencial. A Inteligência de Ameaças Cibernéticas consiste na coleta, processamento e análise de dados relacionados a ataques, com o tráfego de rede sendo uma fonte chave de informações. O software desenvolvido constrói padrões de ataque a partir de incidentes prévios e avalia a correspondência desses padrões com registros de rede, visando identificar possíveis ameaças e as técnicas empregadas. Os testes, conduzidos com registros artificiais que simulam um ataque, indicam que a abordagem tem potencial, embora ainda demande refinamentos para aplicação em cenários reais.*

1. Introdução

Em um mundo cada vez mais digitalizado, grande parte das informações valiosas já não são mais armazenadas em formato físico, mas em sistemas computacionais ou na nuvem [Pokorny 2019]. Esse cenário traz um novo desafio: o aumento da dependência tecnológica vem acompanhado de uma rápida diversificação das ameaças cibernéticas [Barnum 2012]. Nesse contexto, a Inteligência de Ameaças Cibernéticas (CTI, do inglês *Cyber Threat Intelligence*) é um componente essencial para a segurança digital. Ela pode ser compreendida como qualquer informação valiosa que auxilie a identificar, avaliar, monitorar e responder a ameaças digitais, e sua análise permite informar aos usuários sobre possíveis ameaças aos seus sistemas [Chadwick et al. 2020].

Todo dispositivo conectado à Internet constitui um potencial vetor de ataque ou alvo, e cada um gera uma quantidade significativa de registros de tráfego de rede

[Pincovscy 2022]. Esse volume massivo de dados dificulta a análise pelos operadores de segurança, comprometendo a agilidade dos processos defensivos. Sob essas circunstâncias, os cibercriminosos detêm a vantagem de iniciar os ataques, enquanto as equipes de segurança se encontram em uma posição reativa [Tounsi 2019]. Esse desequilíbrio evidencia a necessidade de otimização dos processos de segurança, reduzindo a dependência de análises manuais por meio de automações.

Este trabalho baseia-se na metodologia apresentada por [Leite et al. 2022] para integrar CTI aos processos de segurança, visando uma postura proativa no monitoramento de tráfego de rede. Para dar suporte a essa abordagem, foi desenvolvido o software denominado Orquestrador de Padrões de Inteligência (IPO, do inglês *Intelligence Pattern Orchestrator*), que automatiza a identificação de possíveis atacantes ao comparar incidentes observados em rede com registros de ataques cibernéticos previamente documentados. O sistema utiliza uma base de dados de CTI para gerar padrões comportamentais de ataque a partir de relatórios de inteligência, correlacionando técnicas adversárias com alertas de rede. Dessa forma, o software analisa os registros de rede monitorados e verifica sua correspondência com padrões conhecidos, permitindo que operadores identifiquem rapidamente as técnicas empregadas e a similaridade com ameaças catalogadas.

Diferentemente de abordagens baseadas em Processamento de Linguagem Natural para análise de relatórios, como o NO-DOUBT [Perry et al. 2019], o IPO realiza correlação com resposta ágil em registros de rede, fornecendo contexto operacional imediatamente acionável durante investigações, uma capacidade ainda pouco explorada em ferramentas acadêmicas.

2. Desenvolvimento

O Orquestrador de Padrões de Inteligência é uma ferramenta desenvolvida para coletar, filtrar e estruturar dados sobre ameaças cibernéticas, gerando padrões que representem comportamentos maliciosos. Esses padrões possibilitam identificar potenciais ameaças no tráfego de rede, fornecendo contexto valioso aos analistas para agilizar a investigação e reduzir a carga analítica manual. O IPO conta com duas funcionalidades principais: Construção de Padrão e Verificação de Registro de Rede.

2.1. Arquitetura do Software

O IPO estrutura-se em quatro módulos principais: Coleta de Informações, Filtro e Ranqueamento, Construção de Padrão e Correspondência de Padrões. O software exige uma base de dados devidamente populada em uma Plataforma de Inteligência de Ameaças (TIP)[1] para seu funcionamento básico. Para análise de tráfego em redes reais e detecção efetiva de ameaças, torna-se necessária a integração com um Sistema de Detecção de Intrusões em Rede (NIDS)[2], que fornece os registros de tráfego para processamento. A arquitetura do software é detalhada na Figura 1.

[1]Plataforma de Inteligência de Ameaças (TIP, do inglês *Threat Intelligence Plataform*). Ferramenta que agrega CTI de múltiplas fontes e auxilia o gerenciamento dos dados.

[2]Sistema de Detecção de Intrusões em Rede (NIDS, do inglês *Network Intrusion Detection System*). Ferramenta capaz de monitorar o tráfego de rede.

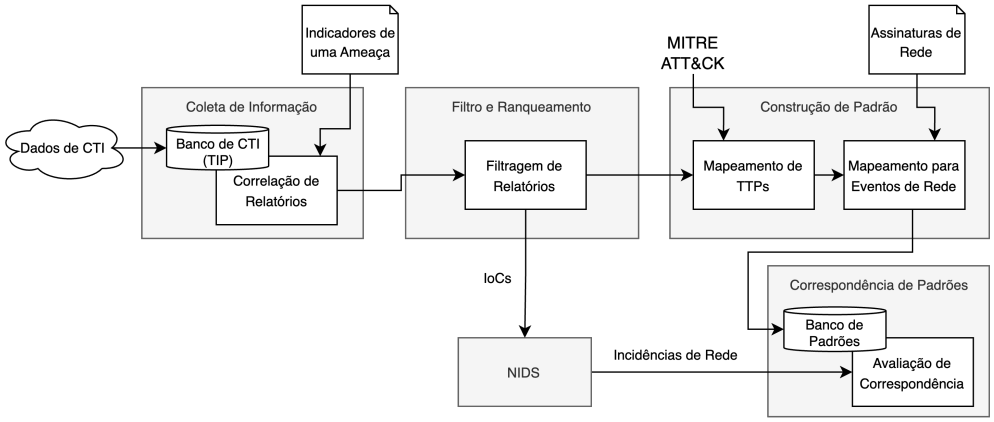

Figura 1. Arquitetura e Fluxo de Dados do IPO.

2.2. Funcionalidades

2.2.1. Construção de Padrão

A construção de padrões é uma funcionalidade central do Orquestrador de Padrões de Inteligência. Seu objetivo é armazenar informações comportamentais sobre uma ameaça em estruturas chamadas de padrões. O processo é iniciado com a seleção de um relatório de inteligência presente na base de dados de CTI (TIP). Em seguida, o orquestrador coleta informações adicionais sobre a ameaça a partir de outros relatórios correlacionados. As técnicas empregadas pelo atacante são utilizadas como base para gerar um padrão, que é salvo em um banco de dados e pode ser usado para identificar o atacante em futuras incidências. O processo envolve três módulos que atuam sequencialmente:

1. **Coleta de Informações:** Indicadores da ameaça são utilizados para identificar dados correlacionados em outras fontes de inteligência, enriquecendo a compreensão sobre as características do adversário.
2. **Filtro e Ranqueamento:** A CTI obtida é filtrada com base no seu nível de informação, priorizando dados relevantes para a construção de padrões.
3. **Construção de Padrão:** As Táticas, Técnicas e Procedimentos (TTPs)[3] do atacante são mapeadas com a matriz MITRE ATT&CK[4], gerando padrões que descrevem o comportamento da ameaça. Esses padrões são armazenados em um banco de dados.

2.2.2. Verificação de Registro de Rede

O tráfego de rede monitorado por um NIDS serve como fonte de informação para o IPO. O software analisa esses registros, comparando-os com os padrões armazenados em seu banco de dados para determinar o grau de correspondência. Durante esse processo, também são automaticamente identificadas as técnicas de ataque empregadas, ampliando a compreensão das atividades suspeitas.

[3]Táticas, Técnicas e Procedimentos (TTPs, do inglês *Tactics, Techniques and Procedures*). Forma organizada de descrever o comportamento do adversário em ataques (objetivos, métodos e ações específicas).

[4]Matriz que categoriza as Técnicas, Táticas e Procedimentos usados por cibercriminosos, agindo como uma base de conhecimento sobre o comportamento de adversários e respostas a incidentes.

A verificação é conduzida pelo módulo Correspondência de Padrões, que analisa os *logs*[5] do NIDS para identificar técnicas adversárias através de alertas configurados previamente. A ferramenta calcula uma pontuação de correspondência com base nas TTPs identificadas nos *logs* e nos padrões, fornecendo aos analistas um contexto detalhado sobre as ameaças detectadas.

2.3. Módulos

Os módulos do orquestrador operam de maneira integrada para executar as funcionalidades propostas. Cada módulo foi desenvolvido de forma autônoma pelos autores, com código-base e lógica customizados para seu respectivo funcionamento.

2.3.1. Coleta de Informações

O módulo de Coleta de Informação consolida dados de uma ameaça analisando relatórios de inteligência disponíveis publicamente ou em plataformas especializadas. O sistema identifica correlações entre documentos com base em Indicadores de Comprometimento (IoCs, do inglês *Indicators of Compromise*), como endereços IP maliciosos, *hashes* de arquivos ou domínios suspeitos, estabelecendo as bases para a construção de padrões comportamentais detalhados que caracterizam a ameaça.

O processo tem início com a seleção de um relatório base na TIP. O algoritmo então realiza buscas automatizadas por relatórios correlacionados, expandindo iterativamente o escopo da investigação. A cada novo relatório incorporado, o sistema reavalia a TIP em busca de correlações adicionais, até que nenhuma nova seja encontrada. O resultado é uma lista de relatórios de inteligência sobre a ameaça em questão.

2.3.2. Filtragem e Ranqueamento

Este módulo é responsável por extrair informações comportamentais do atacante a partir de relatórios de inteligência, enquanto coleta os Indicadores de Comprometimento para bloqueio automático no NIDS. A CTI abrange diferentes tipos de informações, que podem ser de cunho operacional (como IoCs) ou comportamental (como TTPs). As informações comportamentais descrevem o *modus operandi* do atacante (técnicas, estratégias e objetivos), sendo essenciais para construção de padrões e análise aprofundada de ameaças.

O formato STIX[6] [OASIS 2025] é utilizado para categorizar as informações dos relatórios, enquanto o modelo DML (Definido no Anexo C) determina a relevância dos dados. Informações classificadas como DML-3 ou superior são consideradas relevantes no IPO, pois fornecem um nível de detalhamento e contexto mais avançado, permitindo uma análise mais precisa do comportamento do atacante. O processo organiza as informações em três listas distintas:

- **TTPs:** Técnicas, Táticas e Procedimentos do atacante, expressas em objetos STIX do tipo padrão de ataque.

[5]Registros de rede gerados pelo NIDS.

[6]STIX: Expressão Estruturada de Informações sobre Ameaças (*Structured Threat Information Expression*). Padrão utilizado para compartilhamento de informações de CTI.

- **Outros elementos de CTI:** Informações contextuais, como estratégias e objetivos do atacante.
- **IoCs:** Indicadores de ataque enviados para bloqueio automático no NIDS.

Na detecção de ameaças por meio de análise de rede, nem todas as informações de CTI de alto nível são imediatamente úteis. As TTPs desempenham um papel crucial, pois muitas delas podem ser identificadas diretamente em eventos de rede. Embora as informações contextuais não sejam diretamente acionáveis para a detecção, elas fornecem um suporte valioso para os analistas, auxiliando na interpretação e priorização das ameaças.

2.3.3. Construção de Padrão

No módulo de Construção de Padrão, as TTPs da ameaça são utilizadas para criar estruturas que representam o comportamento de um atacante em rede. A partir de uma lista de TTPs expressas em padrões de ataque no formato STIX e das assinaturas configuradas no NIDS, um novo objeto é gerado no banco de dados, representando o padrão criado. Essas estruturas armazenam eventos de rede que descrevem o comportamento do atacante, com base nas técnicas empregadas e nos alertas de rede relacionados.

Para garantir a geração precisa de padrões de ataque e uma detecção eficaz, tanto o NIDS quanto o orquestrador devem ser configurados com regras personalizadas sincronizadas, capazes de identificar as técnicas do adversário. Utilizando a matriz MITRE ATT&CK, é possível determinar quais TTPs são detectáveis em eventos de rede. Esses eventos são acompanhados por alertas com assinaturas únicas no NIDS, permitindo a criação de regras que sinalizam a presença dessas TTPs durante o monitoramento. Essa configuração integrada assegura que os alertas correspondam a padrões de ataque conhecidos, facilitando a identificação das técnicas por meio da matriz ATT&CK.

No IPO, o padrão é um objeto estruturado com os seguintes atributos:

- **Nome:** Identificador único para o novo padrão criado.
- **Descrição:** Breve descrição sobre a ameaça.
- **Eventos:** Lista de eventos de rede relacionados ao comportamento do atacante.

2.3.4. Correspondência de Padrões

O módulo de Correspondência de Padrões é utilizado pelos operadores de segurança para verificar *logs* de rede em busca de atividades suspeitas. Ao analisar os eventos de rede, o módulo identifica alertas e técnicas de ataque relacionadas, fornecendo um contexto valioso sobre as ameaças. Além disso, ele avalia a similaridade do ataque com os padrões registrados no sistema, permitindo que os operadores interpretem os eventos de rede em termos de possíveis adversários e respondam de forma rápida e eficaz.

O orquestrador calcula a pontuação de correspondência através da porcentagem de TTPs compartilhadas entre eventos de rede e padrões armazenados, conforme a Equação 1.

$$\text{Pontuação de Correspondência} = \frac{|TTPs_{\text{registro}} \cap TTPs_{\text{padrão}}|}{|TTPs_{\text{padrão}}|} \times 100 \qquad (1)$$

Os *logs* analisados são comparados com todos os padrões cadastrados, gerando uma pontuação de correspondência para cada um. Além disso, o analista é informado sobre as TTPs detectadas, o que permite uma contextualização mais precisa da ameaça e uma resposta a incidentes mais eficiente.

2.4. *Setup* Experimental

Para a avaliação do IPO, padrões foram construídos a partir de relatórios de inteligência da TIP, com fontes como MITRE [MITRE 2025], MISP [MISP Project 2025] e AlienVault [AlienVault 2025] conectados. Como parte do IPO, foi implementada uma funcionalidade de simulação para testes. Ela gera *logs* artificiais no formato Suricata[7], replicando cenários de ataque e permitindo avaliar a verificação de registros.

Os dados de inteligência utilizados para gerar os registros de teste foram obtidos do Hybrid Analysis [Hybrid Analysis 2025]. Esses dados foram processados pelo IPO, que extraiu as TTPs e as referências da matriz MITRE ATT&CK, mapeando essas informações para as assinaturas configuradas no NIDS. Como resultado, foram gerados *logs* que refletem o comportamento esperado em um cenário real de detecção de ameaças, com eventos de rede detalhando dados do pacote e alertas correspondentes às técnicas ATT&CK detectadas.

2.4.1. Casos de Teste

Para avaliar o sistema desenvolvido, foram selecionados quatro casos de teste baseados em grupos de ataque. A seleção abrange tanto grupos com histórico significativo de atividades, como Lazarus e APT28, quanto ameaças mais recentes, como Blackcat e Kimsuky. Essa diversidade permite cobrir diferentes tipos de ataques cibernéticos, incluindo *ransomwares*[8] e APTs[9], garantindo uma avaliação abrangente do sistema.

3. Resultados

A Tabela 1 sintetiza as pontuações de correspondência (PC) obtidas para cada caso de teste em relação aos padrões desenvolvidos para as ameaças. Detalhes adicionais sobre cada caso de teste estão disponíveis nos Anexos A e Anexo B.

Tabela 1. Pontuações de Correspondência (PC) obtidos para cada padrão testado.

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%

No caso de teste do Lazarus, observou-se uma correspondência significativa com seu padrão relacionado (56%), mas a maior pontuação foi com o Kimsuky (66%). Esse

[7]Ferramenta NIDS *open-source* e renomada no mercado.

[8]Ataques com objetivo de bloquear acesso ao sistema e extorquir vítimas.

[9]APT: Ataque Persistente Avançado (Advanced Persistent Threat). Ataques que combinam técnicas avançadas para invadir um sistema e permanecer dentro dele por longos períodos de tempo.

resultado pode ser explicado pela variabilidade de metodologias utilizadas pelo Lazarus em diferentes campanhas, que incluem desde ataques de APTs até operações mais diretas, semelhantes às táticas do Kimsuky. Essa sobreposição de técnicas pode ter influenciado a alta correspondência com o padrão do Kimsuky.

O Blackcat apresentou baixa correspondência com todos os padrões, incluindo o seu próprio (33%). O resultado para os outros padrões era esperado, já que o Blackcat é especializado exclusivamente em ransomware, o que o diferencia dos outros grupos. Além disso, a pontuação baixa pode ter sido influenciada pelo número limitado de TTPs associados ao Blackcat, o que torna sua pontuação mais sensível a variações.

O *log* do APT28 mostrou pontuações baixas para todos os padrões, com apenas 30% de correspondência com seu próprio padrão. Assim como no caso do Lazarus, a variabilidade de metodologias ao longo do histórico de atividades do APT28 pode ter contribuído para esse resultado. O grupo é conhecido pelo uso de técnicas variadas em diferentes campanhas, o que dificulta a criação de um padrão único e preciso.

Por fim, o *log* do Kimsuky apresentou alta correspondência com seu padrão (83%), refletindo a qualidade dos relatórios da TIP utilizados para criar o padrão. No entanto, também foi observada uma correspondência significativa com o Lazarus (67%), indicando que os dois grupos compartilham elementos em comum em suas táticas. Esse resultado sugere que, embora os padrões tenham sido eficazes, há uma sobreposição de técnicas entre grupos que pode influenciar as pontuações.

4. Implementação

O código-fonte do Orquestrador de Padrões de Inteligência, incluindo frontend, backend e configurações de containerização (Docker), está disponível publicamente em [Barros 2025b]. Artefatos complementares, como arquivos de configuração e demonstrações, podem ser acessados no repositório [Barros 2025a].

4.1. Requisitos para Demonstração

Para a demonstração no Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) será utilizada uma máquina própria. A apresentação incluirá uma demonstração prática da ferramenta, com a execução de casos de teste baseados em cenários reais. Para garantir a replicabilidade do experimento, será utilizado um ambiente virtualizado previamente configurado.

4.2. Tecnologias Utilizadas

O IPO foi desenvolvido em Python, com o ambiente conteinerizado via Docker para garantir replicabilidade.

- **Backend:** FastAPI para API RESTful.
- **Armazenamento:** PostgreSQL para persistência de dados.
- **Integração CTI:** OpenCTI para gestão de inteligência de ameaças.
- **Detecção de Rede:** Modelo compatível com Suricata (NIDS) para identificação de IoCs/TTPs.
- **Interface:** Dashboard interativo em Next.js.

5. Conclusão

Este trabalho apresentou a implementação de um orquestrador de padrões de CTI para detecção automatizada de ameaças em tráfego de rede, com foco na correlação entre TTPs documentadas e eventos observados em *logs*. Os testes realizados evidenciaram tanto os desafios quanto o potencial dessa abordagem. O Orquestrador de Padrões de Inteligência demonstrou capacidade de identificar TTPs em registros de rede, e obteve casos promissores de correspondência como o do grupo Kimsuky, onde o padrão aplicado alcançou resultados satisfatórios. Contudo, em outros casos, os níveis de correspondência ficaram abaixo do esperado, revelando limitações na abordagem atual. Esses achados indicam que, embora a construção de padrões para identificação de ameaças se mostre viável, a solução requer aprimoramentos para alcançar maior confiabilidade operacional.

A sobreposição de TTPs entre grupos com metodologias similares, como Lazarus e Kimsuky, comprometeu a precisão dos resultados, evidenciando a dificuldade de diferenciação precisa entre atacantes em um cenário com informações contextuais limitadas. Essa dificuldade é ampliada pela quantidade restrita de TTPs detectáveis por rede, tanto no MITRE ATT&CK quanto no sistema, o que impede uma distinção mais clara entre as TTPs observadas. Ainda que essa restrição não represente uma falha do sistema, a limitada variedade de TTPs detectáveis por rede restringe a capacidade de identificar de forma mais precisa as características específicas de cada grupo.

Complementando essa análise, ao examinar padrões de ataques persistentes, observou-se uma diminuição na pontuação de correspondência quando comparado aos registros de ransomware, como os do BlackCat. Isso indica que o IPO demonstra potencial para a categorização de ameaças. Melhorias no processo de mapeamento e no uso de informações adicionais podem fortalecer a capacidade do orquestrador para lidar com diferentes tipos de ameaças de maneira mais eficaz.

Os resultados obtidos sugerem caminhos para a otimização da metodologia proposta. Primeiramente, destaca-se a importância da ampliação da base de conhecimento, com a incorporação de técnicas adicionais do MITRE ATT&CK e de relatórios especializados. Em segundo lugar, recomenda-se o suporte à construção de padrões a partir de múltiplos relatórios, promovendo uma representação mais abrangente e precisa dos comportamentos adversários. Por fim, ressalta-se a necessidade de otimização do código e do processamento de *logs* em larga escala. A combinação dessas medidas, aliada à integração com sistemas SIEM[10] para correlação multidimensional e à exploração de técnicas de inteligência artificial, como aprendizado de máquina e modelos de linguagem natural, representa uma direção promissora para o aprimoramento da acurácia do orquestrador.

Para avançar na avaliação da abordagem, uma possibilidade seria testá-la em ambientes reais ou simulações controladas, explorando cenários variados de ataque. Outra vertente seria a ampliação do escopo do orquestrador para além dos eventos de rede, com a incorporação de múltiplas fontes de dados. Essas iniciativas podem favorecer uma análise mais contextualizada e robusta, contribuindo para uma compreensão mais precisa das capacidades e limitações da solução em situações operacionais.

[10]SIEM (*Security Information and Event Management*). Solução de segurança que ajuda detecção, análise e resposta a ameaças cibernéticas.

Referências

AlienVault (2025). Open threat exchange (otx). https://otx.alienvault.com/. Accessed: 2024-09-10.

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

Barros, G. A. S. d. (2025a). Artefatos do ipo. https://zenodo.org/records/14885398.

Barros, G. A. S. d. (2025b). Documentação do orquestrador de padrões de inteligência. https://github.com/gustavoasb/intelligence_pattern_orchestrator_docker/wiki.

Bromander, S., Jøsang, A., and Eian, M. (2016). Semantic cyberthreat modelling. In *Semantic Technologies for Intelligence, Defense, and Security*.

Chadwick, D. W., Fan, W., Costantino, G., de Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A., and Wang, X.-S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Generation Computer Systems*, 102:710–722.

Hybrid Analysis (2025). Hybrid Analysis. https://www.hybrid-analysis.com/. Accessed: 2024-09-11.

Leite, C., den Hartog, J., Ricardo dos Santos, D., and Costante, E. (2022). Actionable cyber threat intelligence for automated incident response. In Reiser, H. P. and Kyas, M., editors, *Secure IT Systems*, pages 368–385, Cham. Springer International Publishing.

MISP Project (2025). Misp threat intelligence feeds. https://www.misp-project.org/feeds/. Accessed: 2024-09-10.

MITRE (2025). Mitre att&ck framework. https://attack.mitre.org. Accessed: 2024-09-10.

OASIS (2025). Stix (structured threat information expression) documentation. https://oasis-open.github.io/cti-documentation/. Accessed: 2025-02-16.

Perry, L., Shapira, B., and Puzis, R. (2019). No-doubt: Attack attribution based on threat intelligence reports. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 80–85.

Pincovscy, J. A. (2022). Metodologia para inteligência de ameaças cibernéticas com integração de sensores. Dissertação (mestrado em engenharia elétrica), Universidade de Brasília, Brasília.

Pokorny, Z. (2019). *The Threat Intelligence Handbook: Moving toward a security intelligence program*. Annapolis, CyberEdge Group.

Tounsi, W. (2019). *What is Cyber Threat Intelligence and How is it Evolving?*, pages 1–49.

A. Estatísticas

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 virtualiza-

ção com Docker, que foi configurado para ter acesso total aos recursos da máquina.

A.1. Métricas de Processamento

A Tabela 2 resume as principais estatísticas do projeto, apresentando números relacionados à construção de cada padrão utilizado como caso de teste. É importante ressaltar que esses números foram obtidos antes da implementação de um *back-end* dedicado no software, o que pode influenciar diretamente no tempo de execução.

Tabela 2. Estatísticas para cada caso de teste.

	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

A diferença entre TTPs encontrados e mapeados deve-se ao fato de que apenas técnicas detectáveis em rede são passíveis de identificação pelo método utilizado. A inclusão de mais regras no NIDS poderia aumentar esse número, porém limitações naturais relacionadas a TTPs que não dependem de tráfego de rede permanecem.

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 de múltiplas fontes de CTI.

A.2. 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 3.

Tabela 3. Mensagens trocadas entre TIP e diferentes fontes de CTI.

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

De maneira geral, foram adicionados à base de dados: 279.280 entidades, 238.320 relações, 1.110 relatórios e 268.930 observáveis. Embora o MISP seja o responsável pela maior quantidade de dados, um estudo 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.

B. Anexo II - Casos de teste

Esse anexo detalha cada ameaça usada como caso de teste para o trabalho. Destacando seu resultado de forma individual. Esses testes foram realizados antes da implementação da nova interface gráfica.

B.1. Lazarus

Como é possível observar na Figura 2, 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.

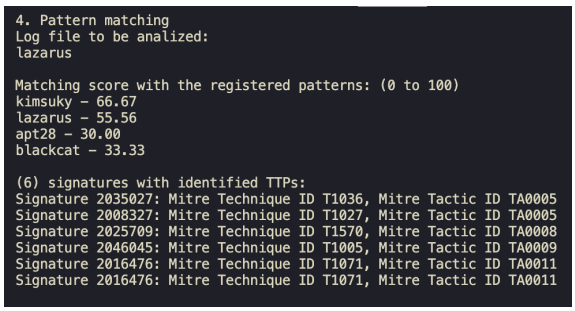

Figura 2. Pontuação de correspondência com um *log* de Lazarus.

B.2. Blackcat

Usando os registros de rede do Blackcat como entrada, as pontuações são as demonstradas na Figura 3. 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.

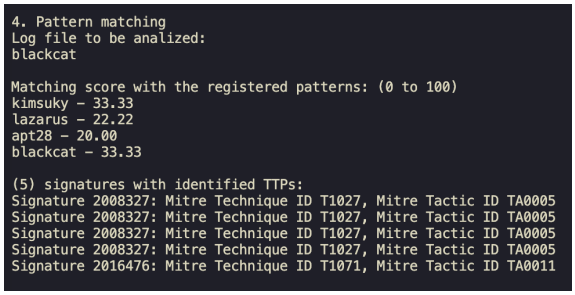

Figura 3. Pontuação de correspondência com um *log* de Blackcat.

B.3. APT28

Como pode ser observado na Figura 4, 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%.

B.4. Kimsuky

Os resultados para o Kimsuky, que podem ser vistos na Figura 5, revelaram uma correspondência de 83% com seu padrão. Além disso, os TTPs do Lazarus foram altamente correspondidos, com 67% de pontuação.

```
4. Pattern matching
Log file to be analized:
apt28

Matching score with the registered patterns: (0 to 100)
kimsuky - 33.33
lazarus - 22.22
apt28 - 30.00
blackcat - 33.33

(3) signatures with identified TTPs:
Signature 2008327: Mitre Technique ID T1027, Mitre Tactic ID TA0005
Signature 2035027: Mitre Technique ID T1036, Mitre Tactic ID TA0005
Signature 2026850: Mitre Technique ID T1021, Mitre Tactic ID TA0008
```

Figura 4. Pontuação de correspondência com um *log* de APT 28.

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

Matching score with the registered patterns: (0 to 100)
kimsuky - 83.33
lazarus - 66.67
apt28 - 30.00
blackcat - 33.33

(11) signatures with identified TTPs:
Signature 2008327: Mitre Technique ID T1027, Mitre Tactic ID TA0005
Signature 2035027: Mitre Technique ID T1036, Mitre Tactic ID TA0005
Signature 2008327: Mitre Technique ID T1027, Mitre Tactic ID TA0005
Signature 2035027: Mitre Technique ID T1036, 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
Signature 2016476: Mitre Technique ID T1071, Mitre Tactic ID TA0011
Signature 2012303: Mitre Technique ID T1041, Mitre Tactic ID TA0011
Signature 2022075: Mitre Technique ID T1486, Mitre Tactic ID TA0040
```

Figura 5. Pontuação de correspondência com um *log* de Kimsuky.

C. Modelo de Detecção de Nível de Maturidade (DML)

Utilizando o modelo de Modelo de Detecção de Nível de Maturidade [Bromander et al. 2016], representado na Figura 6, 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.

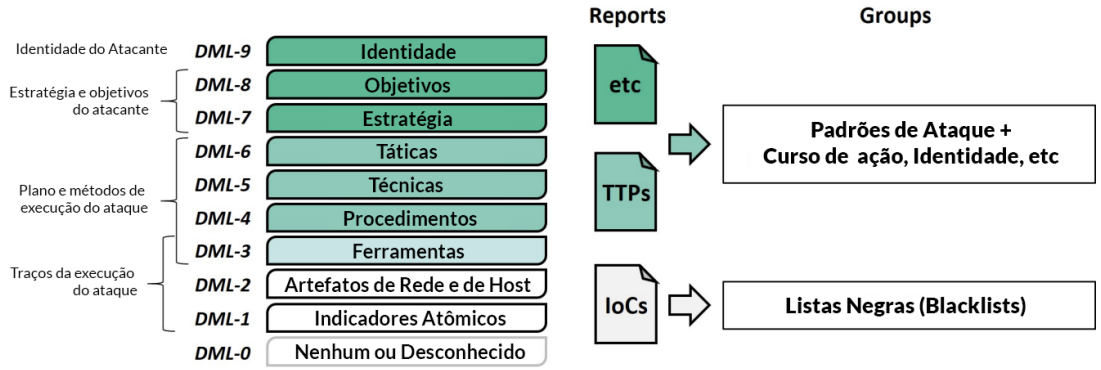

Figura 6. Modelo DML. Fonte: [Bromander et al. 2016]