DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Produção Automatizada de Cyber Threat Intelligence para Monitoramento de Credenciais Expostas em Canais do Telegram

Natália Andrade Marques

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

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Produção Automatizada de Cyber Threat Intelligence para Monitoramento de Credenciais Expostas em Canais do Telegram

Natália Andrade Marques

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

Banca Examinadora

Prof. Robson de Oliveira Albuquerque, Ph.D., FT/UnB
Orientador

Prof. Larte Peotta de Melo, .D., FT/UnB
Examinador Interno

Prof. Vitor F. Fabre D., FT/UnB
Examinador Externo

FICHA CATALOGRÁFICA

MARQUES, NATÁLIA ANDRADE
Produção Automatizada de Cyber Threat Intelligence para Monitoramento de Credenciais Expostas em Canais do Telegram. [Distrito Federal] 2026.
PPEE.MP.126 xvi, 71 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2026).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
PPEE.MP.126Departamento de Engenharia Elétrica

1. Inteligência de Ameaças Cibernéticas	2. Credenciais Comprometidas
3. OSINT	4. Telegram
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

MARQUES, N. A. (2026). *Produção Automatizada de Cyber Threat Intelligence para Monitoramento de Credenciais Expostas em Canais do Telegram*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 71 p.

CESSÃO DE DIREITOS

AUTOR: Natália Andrade Marques
TÍTULO: Produção Automatizada de Cyber Threat Intelligence para Monitoramento de Credenciais Expostas em Canais do Telegram.
GRAU: Mestre em Segurança Cibernética ANO: 2026

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. Do mesmo modo, a Universidade de Brasília tem permissão para divulgar este documento em biblioteca virtual, em formato que permita o acesso via redes de comunicação e a reprodução de cópias, desde que protegida a integridade do conteúdo dessas cópias e proibido o acesso a partes isoladas desse conteúdo. O autor reserva outros direitos de publicação e nenhuma parte deste documento pode ser reproduzida sem a autorização por escrito do autor.

Natália Andrade Marques
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

À minha família.

Esta conquista também é de vocês.

Agradecimentos

A Deus, pela força, sabedoria e perseverança concedidas ao longo desta jornada, especialmente nos momentos em que os desafios pareciam maiores que as minhas capacidades.

Ao Ministério da Gestão e da Inovação em Serviços Públicos (MGI), em especial à equipe da Coordenação-Geral de Tecnologia da Informação (COTEC), pelo apoio institucional, pela confiança e pela oportunidade de desenvolver uma pesquisa aplicada a um contexto de grande relevância para a Administração Pública.

Ao Laboratório LATITUDE, pelo apoio técnico e pela disponibilização da infraestrutura computacional utilizada no desenvolvimento e na execução da Prova de Conceito, contribuindo para a implementação e validação experimental desta pesquisa.

À Fundação de Apoio à Pesquisa do Distrito Federal (FAPDF), pelo apoio e incentivo à pesquisa, contribuindo para o desenvolvimento científico e tecnológico e para a realização deste trabalho.

À Universidade de Brasília (UnB), por tornar possível toda a minha formação acadêmica. Sou profundamente grata pela educação pública, gratuita e de excelência que transformou minha vida, proporcionando oportunidades que marcaram minha trajetória acadêmica, profissional e pessoal.

Ao meu orientador, Professor Dr. Robson de Oliveira Albuquerque, minha mais sincera gratidão. Muito mais do que orientar esta pesquisa, o senhor marcou profundamente minha trajetória acadêmica e profissional. Obrigada pela confiança, pelos ensinamentos, pelas oportunidades e por acreditar no meu potencial desde os primeiros passos da minha formação. Sua orientação, generosidade e exemplo foram fundamentais para a pesquisadora e a profissional que me tornei.

À minha colega de trabalho, Bruna Maria, pelo incentivo, pela parceria e pelas inúmeras trocas de conhecimento que contribuíram para o amadurecimento desta pesquisa.

Por fim, agradeço a todos os colegas, professores, amigos e familiares que, de alguma forma, contribuíram para esta caminhada. Cada palavra de incentivo, cada ensinamento e cada gesto de apoio foram essenciais para que este sonho se tornasse realidade.

RESUMO

O crescimento da disponibilidade de credenciais expostas em fontes abertas representa um dos principais desafios para organizações que buscam identificar precocemente riscos associados ao comprometimento de ativos digitais. Paralelamente, plataformas de mensageria, como o Telegram, passaram a desempenhar papel relevante na disseminação de credenciais, bases de dados vazadas e outras informações sensíveis, tornando-se fontes potenciais para atividades de Cyber Threat Intelligence (CTI). Nesse contexto, esta pesquisa propõe uma arquitetura para o monitoramento automatizado de credenciais expostas divulgadas em grupos públicos do Telegram, visando apoiar a identificação antecipada dessas ocorrências e subsidiar processos de monitoramento e resposta a incidentes. A arquitetura foi estruturada em cinco módulos responsáveis pelas etapas de coleta, processamento, indexação, análise e disseminação da inteligência. A coleta foi realizada por meio da biblioteca Telethon, permitindo a obtenção automatizada de mensagens e arquivos compartilhados em grupos públicos do Telegram. O processamento empregou expressões regulares para identificação e extração de credenciais em diferentes formatos de arquivos, preservando os metadados associados às evidências coletadas. As informações estruturadas foram armazenadas no Elasticsearch, exploradas por meio de painéis analíticos implementados no Kibana e utilizadas na geração automatizada de notificações destinadas aos responsáveis pelos domínios monitorados. A validação da arquitetura foi realizada por meio de uma prova de conceito conduzida durante aproximadamente três meses, contemplando o monitoramento de dois grupos públicos do Telegram, o processamento de aproximadamente 100 arquivos e o acompanhamento de 239 domínios de interesse. Como resultado, foram identificadas e indexadas 9.947 credenciais pertencentes aos domínios monitorados, preservando-se informações relacionadas à origem das evidências, como grupo de divulgação, identificador da mensagem, URL associada e data da publicação. Os resultados obtidos demonstram que a arquitetura foi capaz de automatizar todas as etapas do fluxo de produção de inteligência, desde a aquisição das informações em fontes abertas até sua disponibilização para exploração analítica e geração de alertas. Como principal contribuição, esta pesquisa apresenta uma arquitetura modular para produção de Cyber Threat Intelligence voltada ao monitoramento automatizado de credenciais expostas, integrando mecanismos de coleta, processamento, armazenamento, análise e disseminação em um fluxo contínuo. Além da automatização das atividades operacionais, a solução preserva o contexto das evidências coletadas, favorecendo sua rastreabilidade e apoiando atividades de monitoramento contínuo, investigação e resposta a incidentes.

Palavras-chave: Cyber Threat Intelligence; OSINT; Telegram; Credenciais Expostas; Monitoramento de Ameaças.

ABSTRACT

The increasing availability of exposed credentials in open sources has become a significant challenge for organizations seeking to identify potential risks associated with the compromise of digital assets. At the same time, messaging platforms such as Telegram have emerged as important channels for sharing exposed credentials, leaked databases, and other sensitive information, making them valuable sources for Cyber Threat Intelligence (CTI) activities. In this context, this research proposes an architecture for the automated monitoring of exposed credentials published in public Telegram groups, aiming to support the early identification of credential exposure and enhance cybersecurity monitoring and incident response processes. The proposed architecture is composed of five independent modules responsible for data collection, processing, indexing, analysis, and intelligence dissemination. Data collection was performed using the Telethon library to automatically retrieve messages and files shared in public Telegram groups. The processing module employed regular expressions to identify and extract credentials from different file formats while preserving the metadata associated with each collected piece of evidence. The structured information was stored in Elasticsearch, analyzed through dashboards implemented in Kibana, and used to automatically generate notifications for the organizations associated with the monitored domains. The proposed architecture was validated through a proof of concept conducted over approximately three months, during which two public Telegram groups were continuously monitored. Approximately 100 files were processed while monitoring 239 target domains. As a result, 9,947 exposed credentials associated with the monitored domains were identified and indexed, preserving contextual information such as the source group, message identifier, associated URL, and publication timestamp. The results demonstrate that the proposed architecture successfully automated the complete intelligence production workflow, from data acquisition in open sources to analytical exploration and automated alert generation. The main contribution of this research is the proposal and validation of a modular architecture for Cyber Threat Intelligence focused on the automated monitoring of exposed credentials. By integrating data collection, processing, storage, analysis, and intelligence dissemination into a continuous workflow, the proposed solution not only automates operational tasks but also preserves the contextual information associated with each piece of evidence, supporting continuous monitoring, cybersecurity investigations, and incident response activities.

Keywords: Cyber Threat Intelligence; Open Source Intelligence; Telegram; Exposed Credentials; Threat Monitoring.

SUMÁRIO

1 INTRODUÇÃO 1
1.1 OBJETIVO GERAL 3
1.1.1 OBJETIVOS ESPECÍFICOS 3
1.2 CONTRIBUIÇÕES DESTE TRABALHO 4
1.3 ESTRUTURA DO TRABALHO 5

2 FUNDAMENTAÇÃO TEÓRICA E TRABALHOS CORRELATOS 6
2.1 INTELIGÊNCIA 6
2.1.1 CICLO DE INTELIGÊNCIA 8
2.2 DISCIPLINAS DE INTELIGÊNCIA 11
2.2.1 CYBER THREAT INTELLIGENCE 12
2.2.2 OPEN SOURCE INTELLIGENCE (OSINT) 18
2.3 MÉTODOS E TÉCNICAS APLICADOS A CYBER THREAT INTELLIGENCE 23
2.3.1 MÉTODOS E TÉCNICAS DE COLETA 23
2.3.2 MÉTODOS E TÉCNICAS DE PROCESSAMENTO 27
2.3.3 MÉTODOS E TÉCNICAS DE ANÁLISE E CORRELAÇÃO 28
2.3.4 PLATAFORMAS PARA ARMAZENAMENTO, INDEXAÇÃO, COMPARTILHAMENTO E VISUALIZAÇÃO 30
2.3.5 SÍNTESE COMPARATIVA DOS TRABALHOS CORRELATOS 31

3 DISCUSSÃO DO PROBLEMA E PROPOSTA 34
3.1 METODOLOGIA 34
3.2 PROPOSTA 37
3.3 ARQUITETURA DA SOLUÇÃO 38
3.3.1 MÓDULO DE COLETA DE DADOS 39
3.3.2 MÓDULO DE PROCESSAMENTO 41
3.3.3 MÓDULO DE INDEXAÇÃO DOS DADOS 42
3.3.4 MÓDULO DE ANÁLISE 43
3.3.5 MÓDULO DE ALERTAS 43

4 IMPLEMENTAÇÃO E RESULTADOS DA PROVA DE CONCEITO 45
4.1 AMBIENTE EXPERIMENTAL 45
4.2 IMPLEMENTAÇÃO DA ARQUITETURA 47
4.2.1 IMPLEMENTAÇÃO MÓDULO DE COLETA 48
4.2.2 IMPLEMENTAÇÃO DO MÓDULO DE PROCESSAMENTO 49
4.2.3 IMPLEMENTAÇÃO DO MÓDULO DE INDEXAÇÃO 52
4.2.4 IMPLEMENTAÇÃO DO MÓDULO DE ANÁLISE 54
4.2.5 IMPLEMENTAÇÃO DO MÓDULO DE ALERTAS 57

4.3 Resultados da Prova de Conceito 60
4.3.1 Validação da Arquitetura 61
4.3.2 Discussão dos Resultados 62
4.3.3 Contribuições Alcançadas 63

5 CONCLUSÃO E TRABALHOS FUTUROS 65
5.1 Limitações e Oportunidades de Evolução 66

LISTA DE FIGURAS

2.1 Evolução conceitual entre dado, informação, conhecimento e Inteligência. Adaptado de [1, 2]. 7
2.2 Representação clássica do Ciclo de Inteligência. Adaptado de [2, 3] 9
2.3 Níveis da Cyber Threat Intelligence e seus principais consumidores. Adaptado de [4, 5, 3]. . 15
2.4 Ciclo básico de Cyber Threat Intelligence. Adaptado de [5, 4, 6]. 16

3.1 Ciclo integrado de monitoramento, produção de inteligência e resposta proposto nesta pesquisa. *Fonte: Elaboração própria* 38
3.2 Arquitetura da pipeline proposta nesta pesquisa. *Fonte: Elaboração própria* 39

4.1 Fluxo de execução do módulo de coleta. proposta nesta pesquisa. *Fonte: Elaboração própria.* 49
4.2 Fluxo de execução do módulo de processamento proposta nesta pesquisa. *Fonte: Elaboração própria.* 51
4.3 Fluxo de execução do módulo de indexação proposta nesta pesquisa. *Fonte: Elaboração própria.* 53
4.4 Painel principal desenvolvido para exploração das credenciais comprometidas. Os dados apresentados foram descaracterizados para preservar a confidencialidade das informações coletadas. *Fonte: Elaboração própria.* 55
4.5 Mecanismos de filtragem implementados no painel analítico. (1) filtro por endereço de e-mail; (2) filtro por nome de usuário; (3) filtro por grupo monitorado; (4) filtro temporal. *Fonte: Elaboração própria.* 56
4.6 Distribuição temporal das credenciais indexadas durante a execução da prova de conceito. *Fonte: Elaboração própria.* 57
4.7 Indicador contendo o número total de credenciais indexadas durante a execução da prova de conceito. *Fonte: Elaboração própria.* 57
4.8 Consulta detalhada das credenciais indexadas e respectivos metadados. *Fonte: Elaboração própria.* 58
4.9 Fluxo de execução do módulo de alerta proposta nesta pesquisa. *Fonte: Elaboração própria.* 59
4.10 Execução do módulo de disseminação da inteligência. *Fonte: Elaboração própria.* 60
4.11 Exemplo de notificação gerada automaticamente pelo módulo de disseminação da inteligência. *Fonte: Elaboração própria.* 60

LISTA DE TABELAS

2.1 Evolução do Ciclo de Inteligência encontradas na literatura. 11
2.2 Estratégias de aquisição de dados empregadas em arquiteturas modernas de Cyber Threat Intelligence. 26
2.3 Principais técnicas empregadas no processamento de Cyber Threat Intelligence. 28
2.4 Principais técnicas empregadas na análise e correlação em Cyber Threat Intelligence. 29
2.5 Comparação entre os trabalhos correlatos e a presente pesquisa. 32

3.1 Aplicação da metodologia 5W3H no contexto da pesquisa 36
3.2 Campos armazenados para cada credencial identificada 42

4.1 Tecnologias utilizadas na implementação da Prova de Conceito. 46
4.2 Infraestrutura utilizada durante a execução da Prova de Conceito. 47
4.3 Principais padrões de credenciais identificados durante o processamento. 50
4.4 Principais campos armazenados para cada documento indexado. 53
4.5 Principais análises disponibilizadas pelo módulo de análise. 58
4.6 Resumo dos resultados obtidos durante a prova de conceito. 61

1 INTRODUÇÃO

A transformação digital observada nas últimas décadas ampliou significativamente a dependência de mecanismos de autenticação para acesso a sistemas, aplicações e serviços digitais. Nesse contexto, credenciais de acesso, compostas por identificadores de usuários, endereços de correio eletrônico, senhas, cookies de sessão e tokens de autenticação,constituem atualmente um dos principais elementos de segurança empregados para proteção de recursos computacionais. Consequentemente, o comprometimento dessas informações tornou-se um objetivo recorrente para atores maliciosos, uma vez que credenciais válidas permitem contornar mecanismos de segurança sem a necessidade de exploração direta de vulnerabilidades técnicas. Estudos demonstram que o uso indevido de credenciais legítimas permanece entre os vetores mais frequentes em incidentes de segurança e comprometimentos corporativos [7].

Existem diferentes formas pelas quais credenciais podem ser expostas, entre as quais se destacam os vazamentos de dados *(data breaches)*. Incidentes envolvendo organizações públicas e privadas frequentemente resultam na exposição de milhões de registros contendo nomes de usuários, endereços de correio eletrônico, senhas e outras informações de autenticação. Uma vez divulgados, esses conjuntos de dados passam a circular em fóruns clandestinos, comunidades especializadas e repositórios ilícitos, ampliando sua disponibilidade para diferentes categorias de atacantes. A reutilização de senhas por parte dos usuários potencializa ainda mais esse problema, permitindo que credenciais vazadas sejam reutilizadas em múltiplos serviços por meio de técnicas como credential stuffing [8].

Outro vetor amplamente explorado para obtenção de credenciais consiste nas campanhas de phishing. Essas operações utilizam técnicas de engenharia social para induzir usuários a revelar voluntariamente informações de autenticação em páginas fraudulentas que simulam serviços legítimos [9]. A evolução dos kits de phishing e a disponibilidade de infraestruturas prontas para uso reduziram significativamente as barreiras técnicas para execução desse tipo de ataque. Além disso, a adoção de mecanismos de automação e personalização aumentou a efetividade dessas campanhas, tornando-as uma das principais ameaças observadas por organizações públicas e privadas em escala global.

O roubo de credenciais portanto, não constitui um fenômeno recente, porém a escala e a sofisticação desse ecossistema sofreram profundas transformações ao longo da última década. Inicialmente associado a campanhas de phishing e à disseminação de keyloggers, o processo de obtenção de credenciais evoluiu para um mercado altamente especializado, caracterizado pela divisão de funções entre diferentes atores criminosos. Thomas et al. [10] observaram que credenciais provenientes de vazamentos de dados, campanhas de phishing e malwares especializados alimentavam mercados clandestinos nos quais informações de autenticação eram comercializadas como mercadorias digitais. Estudos posteriores indicam que a profissionalização do cibercrime favoreceu o surgimento de modelos de negócio estruturados, capazes de transformar credenciais comprometidas em produtos amplamente negociados em ecossistemas ilícitos [11].

Nos últimos anos, entretanto, observou-se uma mudança significativa no ecossistema de coleta de credenciais com a ascensão dos chamados infostealers. Diferentemente dos keyloggers tradicionais, os

infostealers são projetados para coletar de forma automatizada uma ampla variedade de informações armazenadas nos dispositivos comprometidos, incluindo credenciais salvas em navegadores, cookies de sessão, tokens de autenticação, dados financeiros e carteiras de criptomoedas [12]. Após a infecção do dispositivo, essas informações são exfiltradas para infraestruturas controladas pelos operadores do malware e posteriormente comercializadas ou distribuídas em comunidades criminosas. Pesquisas recentes apontam que os infostealers passaram a representar uma das principais fontes de credenciais comprometidas disponíveis no ecossistema clandestino contemporâneo [8].

A expansão desse fenômeno foi impulsionada pela consolidação do modelo Malware-as-a-Service (MaaS), que permite a disponibilização de malwares mediante pagamento de assinaturas ou participação nos lucros obtidos pelos operadores [13]. Esse modelo reduziu substancialmente a necessidade de conhecimento técnico avançado para condução de campanhas de roubo de credenciais, favorecendo a proliferação de famílias de malware especializadas e aumentando o volume de informações comprometidas disponíveis para comercialização. Como consequência, o ecossistema criminoso passou a operar de forma semelhante a mercados legítimos, incorporando mecanismos de reputação, suporte técnico e segmentação de produtos [14].

Após sua obtenção, as credenciais passam a integrar um ecossistema de comercialização e compartilhamento altamente estruturado. Fóruns especializados, mercados clandestinos, plataformas de comunicação criptografadas e comunidades dedicadas à troca de informações ilícitas constituem alguns dos principais ambientes utilizados para disseminação desses dados [15]. Nesses espaços, credenciais podem ser comercializadas individualmente, agrupadas por país, setor econômico ou tipo de serviço, ou ainda utilizadas como moeda de troca entre participantes do ecossistema criminoso. Essa dinâmica permite a formação de cadeias de valor nas quais diferentes atores atuam de forma especializada na coleta, revenda e exploração das credenciais comprometidas [16].

Os impactos decorrentes da exposição e utilização indevida de credenciais ultrapassam o comprometimento de contas individuais. Credenciais roubadas frequentemente são utilizadas como vetor inicial para invasões corporativas, campanhas de ransomware, fraudes financeiras, espionagem cibernética e comprometimento de infraestruturas críticas. Relatórios recentes indicam que o uso de credenciais válidas permanece entre os principais fatores associados a incidentes de segurança em organizações de diferentes setores econômicos [7]. Nesse contexto, compreender os mecanismos de obtenção, disseminação e exploração de credenciais comprometidas torna-se fundamental para o desenvolvimento de estratégias eficazes de monitoramento, inteligência de ameaças e mitigação de riscos cibernéticos [17] [7].

Diante do aumento contínuo de vazamentos de dados e da crescente disponibilidade de credenciais comprometidas em diferentes ambientes do ecossistema cibercriminoso, o monitoramento contínuo e automatizado de fontes abertas emerge como uma capacidade essencial para as atividades de Inteligência de Ameaças Cibernéticas. A rápida identificação de credenciais expostas permite que organizações adotem medidas de contenção e mitigação antes que essas informações sejam efetivamente exploradas por atores maliciosos. Mesmo na ausência de evidências de uso indevido, a exposição de uma credencial corporativa representa um indicativo relevante de risco, demandando ações como a revogação preventiva de acessos, redefinição de senhas, investigação de possíveis comprometimentos e monitoramento das contas afetadas.

Diante do exposto, entende-se que soluções de monitoramento devem ir além da simples coleta de

dados provenientes de vazamentos. Para que a informação obtida possa apoiar processos de tomada de decisão, é necessário incorporar mecanismos capazes de realizar enriquecimento contextual, correlação de eventos, identificação de ativos de interesse, filtragem por domínios organizacionais e geração tempestiva de alertas. Dessa forma, grandes volumes de dados estruturados ou não estruturados podem ser transformados em inteligência acionável, permitindo a identificação precoce de exposições, a redução do tempo de resposta a incidentes e o fortalecimento da postura de segurança das organizações frente às ameaças associadas ao comprometimento de credenciais.

Assim sendo, torna-se evidente a necessidade de mecanismos capazes de monitorar continuamente fontes abertas potencialmente associadas à divulgação de credenciais comprometidas. A adoção de processos automatizados de coleta, processamento e análise permite ampliar a capacidade de detecção de exposições relevantes, reduzindo a dependência de atividades manuais e possibilitando respostas mais rápidas aos riscos identificados.

Esta pesquisa propõe uma prova de conceito voltada à identificação de credenciais comprometidas por meio da aplicação de técnicas de Open Source Intelligence (OSINT). Especificamente, o estudo concentra-se na coleta, processamento e análise de dados disponibilizados em canais públicos da plataforma Telegram associados ao compartilhamento de credenciais expostas. Como resultado, pretende-se demonstrar a viabilidade do monitoramento contínuo dessas fontes para apoio às atividades de Inteligência de Ameaças Cibernéticas, contribuindo para a identificação precoce de exposições de credenciais e para a compreensão dos riscos decorrentes de sua exploração por atores maliciosos.

1.1 OBJETIVO GERAL

Desenvolver uma arquitetura automatizada em modelo de prova de conceito (POC) para monitoramento de credenciais expostas em canais públicos do Telegram, integrando as etapas de coleta, processamento, indexação, análise e disseminação de Cyber Threat Intelligence, de forma a apoiar a identificação precoce de credenciais comprometidas pertencentes a domínios de interesse e subsidiar atividades de prevenção, detecção e resposta a incidentes de segurança cibernética.

1.1.1 Objetivos Específicos

Para alcançar o objetivo geral desta pesquisa, foram definidos os seguintes objetivos específicos:

- Realizar uma revisão da literatura sobre Inteligência, Open Source Intelligence (OSINT) e Cyber Threat Intelligence (CTI), identificando métodos, técnicas e arquiteturas utilizadas na produção de Inteligência aplicada à cibersegurança;
- Desenvolver um mecanismo automatizado para monitoramento contínuo de canais públicos do Telegram, permitindo a coleta de mensagens e arquivos potencialmente relacionados ao compartilhamento de credenciais comprometidas;
- Implementar um processo de extração e normalização de credenciais, identificando informações

relevantes, como usuário, senha, domínio, URL e metadados associados às evidências coletadas;

- Desenvolver um mecanismo de identificação de credenciais pertencentes a domínios previamente definidos, permitindo direcionar o monitoramento para organizações de interesse;
- Implementar um processo de indexação das informações coletadas em uma plataforma de busca e análise, possibilitando consultas eficientes e organização estruturada dos dados;
- Desenvolver painéis analíticos para visualização das informações produzidas, apoiando atividades de monitoramento e análise de Cyber Threat Intelligence;
- Avaliar a arquitetura proposta por meio de uma prova de conceito baseada no monitoramento de canais públicos do Telegram, analisando sua capacidade de identificar credenciais comprometidas pertencentes aos domínios monitorados.

1.2 CONTRIBUIÇÕES DESTE TRABALHO

As principais contribuições desta dissertação podem ser sintetizadas nos seguintes aspectos:

- Proposição de uma arquitetura metodológica integrada para produção de Cyber Threat Intelligence, estabelecendo um fluxo contínuo entre aquisição de dados em fontes abertas, processamento e estruturação de credenciais expostas, indexação, análise e disseminação das informações produzidas;
- Desenvolvimento e implementação de um *pipeline* automatizado para monitoramento de canais e grupos públicos do Telegram, integrando acesso programático à plataforma, extração baseada em regras e expressões regulares, normalização dos dados, indexação no Elasticsearch, análise por meio do Kibana e geração automatizada de alertas;
- Direcionamento da produção de inteligência a ativos de interesse, por meio da identificação e filtragem de credenciais expostas associadas a domínios previamente definidos, permitindo contextualizar as ocorrências de acordo com as necessidades das organizações monitoradas;
- Validação da arquitetura por meio de uma Prova de Conceito executada durante três meses, demonstrando a viabilidade operacional da integração entre as etapas de coleta, processamento, indexação, análise e disseminação no monitoramento contínuo de credenciais expostas;
- Consolidação de uma revisão da literatura sobre Inteligência, Open Source Intelligence e Cyber Threat Intelligence, abrangendo conceitos, métodos, técnicas e arquiteturas relacionados à obtenção, processamento, análise e disseminação de informações aplicadas à segurança cibernética;
- Produção científica decorrente da pesquisa, com a apresentação do trabalho *Proposal of an OSINT Pipeline for Monitoring Exposed Credentials in Underground Telegram Channels* na *Second Summer School on Artificial Intelligence in Cybersecurity (CYBER-AI 2026)*, com publicação prevista como *Proceeding Paper* no periódico *Engineering Proceedings* [18].

1.3 ESTRUTURA DO TRABALHO

Esta dissertação está organizada em cinco capítulos, além desta introdução.

O Capitulo 2 apresenta a fundamentação teórica da pesquisa, abordando os conceitos de Inteligência, Open Source Intelligence (OSINT) e Cyber Threat Intelligence (CTI), bem como os métodos e técnicas empregados na produção de Inteligência aplicada à cibersegurança. Também são discutidas as principais arquiteturas, plataformas e trabalhos relacionados ao monitoramento automatizado de ameaças e credenciais expostas.

O Capítulo 3 descreve a metodologia adotada na pesquisa e apresenta a arquitetura proposta, detalhando os componentes responsáveis pela coleta, processamento, extração, indexação, análise e visualização das informações obtidas a partir de canais públicos do Telegram.

O Capítulo 4 apresenta os resultados obtidos durante a implementação e avaliação da arquitetura proposta, discutindo a capacidade da solução para identificação de credenciais comprometidas, bem como as principais limitações observadas durante a realização da prova de conceito.

Por fim, o Capítulo 5 apresenta as conclusões da pesquisa, destacando as principais contribuições alcançadas, as limitações identificadas e as possibilidades de evolução da arquitetura por meio de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA E TRABALHOS CORRELATOS

Este capítulo apresenta os fundamentos teóricos que sustentam o desenvolvimento desta pesquisa, abordando os principais conceitos relacionados à Inteligência, Open Source Intelligence (OSINT) e Cyber Threat Intelligence (CTI), bem como os métodos, técnicas e tecnologias empregados na produção de Inteligência aplicada à segurança cibernética. Além da fundamentação conceitual, são analisados trabalhos correlatos que propõem arquiteturas, plataformas e mecanismos para coleta, processamento, análise e disseminação de informações provenientes de fontes abertas, com ênfase no monitoramento de ameaças e credenciais comprometidas. Essa revisão permite compreender o estado da arte da área, identificar as principais contribuições da literatura e evidenciar as lacunas que motivam a proposta apresentada nesta dissertação.

2.1 INTELIGÊNCIA

A Inteligência constitui um processo de produção de conhecimento destinado a reduzir incertezas e apoiar a tomada de decisão em ambientes caracterizados por elevada complexidade e disponibilidade limitada de informações confiáveis. Embora o termo seja frequentemente associado aos contextos militar e governamental, seus princípios passaram a ser amplamente empregados em diferentes áreas do conhecimento, incluindo segurança pública, gestão de riscos, negócios e, mais recentemente, cibersegurança. Independentemente do domínio de aplicação, a Inteligência possui como propósito central transformar dados dispersos em conhecimento estruturado, contextualizado e acionável, permitindo que indivíduos e organizações compreendam melhor determinado cenário e adotem decisões fundamentadas.

A evolução tecnológica observada nas últimas décadas modificou significativamente a forma como informações são produzidas, armazenadas e compartilhadas. A digitalização de processos organizacionais, a expansão da Internet e a popularização de plataformas digitais produziram um volume crescente de dados disponíveis em diferentes formatos e origens. Entretanto, a disponibilidade dessas informações não implica, necessariamente, maior capacidade de compreensão do ambiente analisado. Pelo contrário, o excesso de dados frequentemente amplia a dificuldade de identificar informações realmente relevantes, tornando indispensáveis mecanismos capazes de selecionar, correlacionar, interpretar e contextualizar os elementos coletados. Nesse cenário, a Inteligência assume papel fundamental ao estabelecer métodos sistemáticos para transformar grandes volumes de dados em conhecimento útil ao processo decisório [2].

Historicamente, Sherman Kent é reconhecido como um dos principais responsáveis pela consolidação da Inteligência como disciplina científica. Em sua obra clássica, o autor estabelece que Inteligência pode ser compreendida simultaneamente como conhecimento, organização e processo. Como conhecimento, representa o produto final entregue aos tomadores de decisão; como organização, corresponde às estruturas responsáveis pela produção desse conhecimento; e, como processo, engloba o conjunto de atividades desti-

nadas à obtenção, análise e disseminação das informações necessárias para apoiar decisões estratégicas [1]. Essa visão permanece atual e constitui a base conceitual de grande parte das metodologias contemporâneas empregadas em diferentes domínios de Inteligência.

Clark amplia essa perspectiva ao destacar que o principal diferencial da Inteligência não está na simples obtenção de informações, mas na capacidade analítica de produzir conhecimento por meio da integração de múltiplas fontes. Segundo o autor, informações isoladas raramente são suficientes para explicar determinado fenômeno. Somente a correlação entre diferentes evidências, associada à avaliação da confiabilidade das fontes e à interpretação contextual dos dados disponíveis, permite construir conhecimento capaz de reduzir incertezas e orientar decisões. Dessa forma, a atividade analítica torna-se o elemento central da produção de Inteligência, diferenciando-a de atividades meramente informacionais ou de monitoramento [2].

Essa distinção torna-se mais evidente quando se observa a relação existente entre dado, informação, conhecimento e Inteligência. Embora frequentemente utilizados como sinônimos, esses conceitos representam diferentes níveis de maturidade da informação ao longo do processo analítico. Dados correspondem a registros elementares, normalmente desprovidos de significado quando analisados isoladamente. A organização e contextualização desses dados produzem informações, que passam a representar determinado evento ou situação. Quando interpretadas à luz de objetivos específicos e combinadas ao conhecimento especializado dos analistas, essas informações originam conhecimento. Finalmente, a Inteligência corresponde ao conhecimento produzido de maneira ordenada para atender necessidades específicas de decisão, considerando contexto, confiabilidade, oportunidade e relevância das evidências disponíveis.



Figura 2.1: Evolução conceitual entre dado, informação, conhecimento e Inteligência. Adaptado de [1, 2].

A Figura 2.1 representa essa evolução conceitual, observa-se que o aumento do valor analítico das informações ocorre à medida que os dados passam por sucessivas etapas de contextualização e interpretação. Consequentemente, Inteligência não deve ser compreendida como um conjunto de informações armazenadas, mas como o resultado de um processo estruturado de análise capaz de produzir conhecimento direcionado às necessidades dos tomadores de decisão [19].

Embora as definições clássicas tenham sido desenvolvidas em contextos estratégicos governamentais, sua aplicação permanece plenamente válida em ambientes organizacionais contemporâneos. Estudos recentes demonstram que organizações produzem diariamente grandes volumes de informações relacionadas aos seus ativos tecnológicos, usuários, vulnerabilidades e incidentes de segurança. Entretanto, apenas uma pequena parcela desses dados é efetivamente convertida em conhecimento capaz de apoiar decisões relacionadas à gestão de riscos e à proteção dos ativos organizacionais. Essa limitação decorre, principalmente, da ausência de processos estruturados de produção de Inteligência, evidenciando que a simples disponibilidade de dados não implica maior capacidade de compreensão do cenário de ameaças [5].

A literatura recente também evidencia uma mudança importante na forma como a Inteligência passou a ser produzida. Tradicionalmente, a atividade era conduzida predominantemente por especialistas humanos, responsáveis pela coleta, análise e elaboração de produtos de Inteligência. Atualmente, observa-se crescente incorporação de mecanismos automatizados capazes de apoiar diferentes etapas desse processo. Revisões metodologicas recentes mostram que técnicas de mineração de dados, aprendizado de máquina, processamento de linguagem natural, grafos de conhecimento e inteligência artificial vêm sendo empregadas para ampliar a capacidade de coleta, processamento e correlação de grandes volumes de informações provenientes de ambientes digitais [20, 21]. Embora essas tecnologias modifiquem significativamente a forma como a Inteligência é produzida, seu objetivo permanece alinhado aos princípios estabelecidos por [1, 2]: produzir conhecimento confiável para reduzir incertezas e apoiar decisões.

Sob essa perspectiva, Inteligência deve ser compreendida como um processo contínuo de produção de conhecimento e não como um produto isolado. Sua efetividade depende da integração entre pessoas, processos e tecnologias capazes de coletar informações relevantes, interpretar seu significado, avaliar sua confiabilidade e disseminar os resultados produzidos aos responsáveis pela tomada de decisão. Esse entendimento constitui o fundamento sobre o qual se desenvolveram as modernas abordagens de Inteligência aplicadas ao domínio cibernético, discutidas nas próximas seções desta dissertação.

2.1.1 Ciclo de Inteligência

A atividade de Inteligência é tradicionalmente organizada por meio do denominado Ciclo de Inteligência, um modelo conceitual que estrutura a produção de conhecimento em etapas sucessivas e interdependentes. Embora existam variações entre organizações governamentais, militares e corporativas, a literatura converge para um conjunto de fases responsáveis por transformar necessidades informacionais em produtos de Inteligência capazes de apoiar a tomada de decisão. Mais do que uma sequência operacional, o ciclo representa um processo iterativo, no qual o conhecimento produzido retroalimenta continuamente novas demandas de informação, promovendo o aperfeiçoamento permanente das atividades de Inteligência [2, 3, 1].

Nas abordagens clássicas, o ciclo é composto pelas etapas de planejamento, coleta, processamento, análise e disseminação. O planejamento corresponde à definição dos objetivos de Inteligência e das necessidades informacionais que deverão ser atendidas. Em seguida, a etapa de coleta concentra-se na obtenção de informações provenientes de diferentes fontes. O processamento organiza, filtra e prepara os dados obtidos para a análise, etapa responsável pela produção do conhecimento propriamente dito. Por fim, a Inteligência produzida é disseminada aos tomadores de decisão, permitindo que os resultados obtidos apoiem

ações estratégicas, táticas ou operacionais. Apesar de sua aparente linearidade, diversos autores ressaltam que essas etapas apresentam forte retroalimentação, tornando o ciclo um processo contínuo de produção de conhecimento e não uma sequência rígida de atividades [2, 3, 5].

A Figura 2.2 ilustra a representação clássica do Ciclo de Inteligência. Embora originalmente concebido para atividades governamentais e militares, esse modelo permanece como referência para diferentes domínios de aplicação, incluindo a Inteligência competitiva, financeira e cibernética. Sua permanência ao longo das últimas décadas decorre da capacidade de organizar sistematicamente a produção de conhecimento, independentemente das tecnologias empregadas em cada etapa.

A evolução dos ambientes digitais, entretanto, modificou significativamente a forma como essas atividades são executadas. O crescimento exponencial da quantidade de informações disponíveis, associado à diversidade das fontes e à velocidade de propagação das ameaças, tornou inviável a execução exclusivamente manual do ciclo. Como consequência, arquiteturas modernas passaram a incorporar mecanismos automatizados de coleta, processamento, enriquecimento e correlação capazes de lidar com grandes volumes de dados provenientes de ambientes heterogêneos. Nesse contexto, observa-se que os fundamentos do Ciclo de Inteligência permanecem preservados, enquanto os métodos empregados em cada etapa evoluíram significativamente em função dos avanços tecnológicos [4, 20, 21].

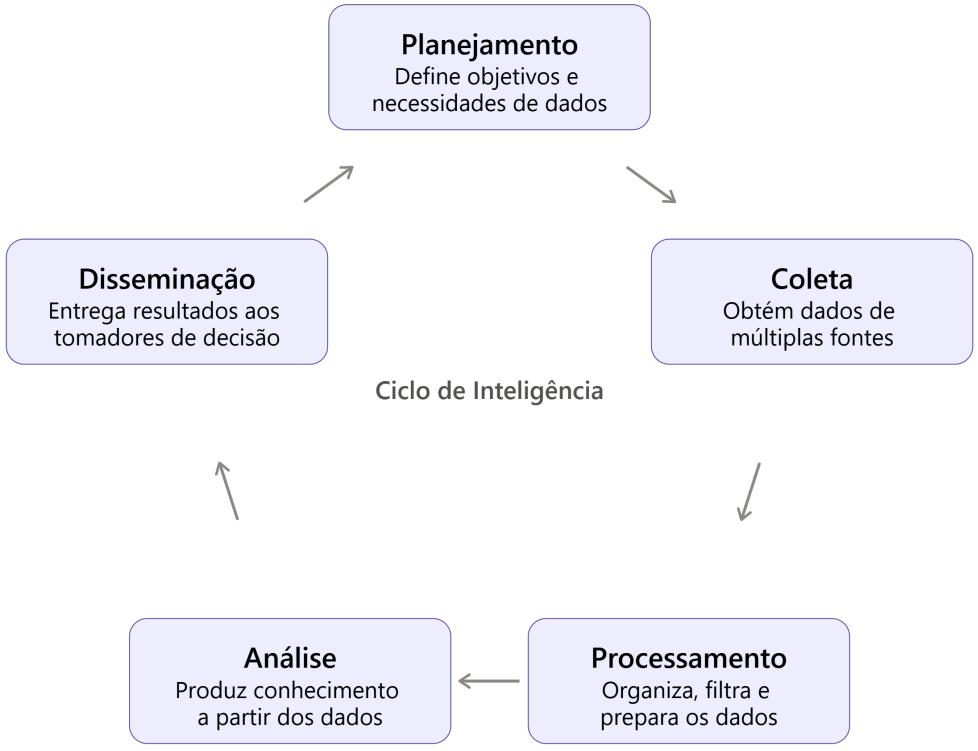


Figura 2.2: Representação clássica do Ciclo de Inteligência. Adaptado de [2, 3]

Essa evolução também é observada na literatura recente sobre Cyber Threat Intelligence. Saeed et al. [5] propõem um framework organizado em três componentes principais: base de conhecimento, modelos de detecção e painéis de visualização. Embora utilize terminologias distintas do ciclo clássico, a arquitetura preserva os mesmos princípios fundamentais, uma vez que as bases de conhecimento concentram as informações coletadas, os modelos de detecção realizam atividades de processamento e análise, enquanto

os painéis representam mecanismos de disseminação da Inteligência produzida. De forma semelhante, Chatziamanetoglou e Rantos[6] demonstram que pesquisas recentes envolvendo blockchain e CTI continuam estruturando suas arquiteturas segundo o ciclo tradicional, concentrando os principais avanços nas etapas de compartilhamento, preservação da integridade e rastreabilidade das informações produzidas.

O desenvolvimento de mecanismos de automação também impulsionou mudanças importantes nas etapas de processamento e análise. Guo et al. [22] propõem um framework capaz de extrair, correlacionar e fundir Inteligência proveniente de múltiplas fontes por meio da construção de grafos de conhecimento, reduzindo inconsistências entre informações estruturadas e não estruturadas. De forma complementar, Lin et al. [23] apresentam mecanismos para correlacionar produtos de CTI com evidências observadas em ambientes reais (*sightings*), permitindo avaliar a qualidade da Inteligência disponível e ampliar automaticamente o conhecimento produzido. Esses estudos evidenciam que o processamento contemporâneo da Inteligência ultrapassa atividades de simples organização dos dados, incorporando técnicas avançadas de enriquecimento, correlação e validação das informações coletadas.

Paralelamente, observa-se crescente interesse na aplicação de técnicas de Inteligência Artificial para apoiar diferentes etapas do ciclo. Revisões recentes mostram que algoritmos de aprendizado de máquina, modelos de linguagem, processamento de linguagem natural e métodos baseados em grafos vêm sendo utilizados para automatizar a extração de entidades, identificar padrões ocultos e antecipar comportamentos adversários em ambientes digitais [24, 20, 21]. Embora essas tecnologias ampliem significativamente a capacidade analítica dos sistemas modernos, os estudos convergem ao afirmar que a produção de Inteligência continua dependente da interpretação humana, especialmente nas etapas relacionadas à contextualização, avaliação da confiabilidade das fontes e apoio ao processo decisório.

Outra transformação importante observada na literatura refere-se à etapa de disseminação da Inteligência. Tradicionalmente restrita à elaboração de relatórios destinados aos tomadores de decisão, essa atividade passou a incorporar mecanismos colaborativos de compartilhamento entre organizações. Alaeifar et al. [25] demonstram que arquiteturas modernas de CTI priorizam modelos colaborativos capazes de facilitar o intercâmbio de informações entre diferentes organizações, respeitando requisitos relacionados à interoperabilidade, privacidade e padronização dos dados. Em complemento, Reittinger et al. [26] destacam que fatores como confiança, reputação e incentivos institucionais exercem papel decisivo para ampliar a efetividade dos ecossistemas de compartilhamento de Inteligência, indicando que aspectos organizacionais possuem importância equivalente aos desafios tecnológicos envolvidos nesse processo.

Dessa forma, observa-se que o Ciclo de Inteligência permanece como o principal modelo conceitual para organização das atividades relacionadas à produção de conhecimento. Entretanto, sua aplicação contemporânea incorpora tecnologias capazes de automatizar etapas tradicionalmente executadas por analistas, ampliando significativamente a capacidade de coletar, processar, correlacionar e disseminar informações provenientes de ambientes digitais. Assim, mais do que substituir o modelo clássico, as abordagens atuais representam uma evolução de seus princípios fundamentais, preservando sua estrutura conceitual enquanto adaptam seus mecanismos operacionais às demandas impostas pelo cenário cibernético contemporâneo.

A adaptação do Ciclo de Inteligência ao contexto digital deu origem a abordagens específicas para o domínio da cibersegurança, nas quais os processos tradicionais passaram a ser aplicados à identificação, análise e antecipação de ameaças cibernéticas.

Tabela 2.1: Evolução do Ciclo de Inteligência encontradas na literatura.

Autor	Modelo	Principal contribuição
Clark (2006)	Ciclo clássico	Estrutura as atividades em planejamento, coleta, processamento, análise e disseminação.
Lowenthal (2025)	Processo decisório	Reforça o caráter iterativo do ciclo e sua função de reduzir incertezas.
Saeed et al. (2023)	Framework organizacional	Integra bases de conhecimento, modelos de detecção e dashboards.
Chatziamanetoglou e Rantos (2024)	CTI + Blockchain	Amplia as etapas de disseminação, confiança e compartilhamento.
Guo et al. (2023)	Extração e fusão	Introduz mecanismos de enriquecimento e correlação da Inteligência.
Lin et al. (2023)	Avaliação de CTI	Correlaciona produtos de Inteligência com evidências reais para enriquecimento da CTI.

2.2 DISCIPLINAS DE INTELIGÊNCIA

A transformação digital observada nas últimas décadas modificou profundamente o ambiente em que organizações públicas e privadas desenvolvem suas atividades. A crescente dependência de infraestruturas digitais, aliada à expansão da computação em nuvem, Internet das Coisas (IoT), serviços distribuídos e plataformas colaborativas, ampliou significativamente a superfície de ataque das organizações e elevou a complexidade do cenário de ameaças. Nesse contexto, os modelos tradicionais de segurança, predominantemente baseados em mecanismos reativos de prevenção e detecção, passaram a demonstrar limitações diante da velocidade de evolução dos ataques e da elevada capacidade adaptativa dos agentes maliciosos. Como consequência, os princípios da atividade de Inteligência passaram a ser incorporados ao domínio cibernético como forma de antecipar ameaças, compreender o comportamento dos adversários e apoiar decisões relacionadas à gestão dos riscos digitais [4, 5, 27].

Diferentemente das métodos convencionais de monitoramento, a Inteligência aplicada à cibersegurança não se limita à identificação de eventos ou incidentes isolados. Seu propósito consiste em transformar grandes volumes de informações provenientes de diferentes fontes em conhecimento contextualizado, capaz de apoiar decisões estratégicas, táticas e operacionais. Essa transformação ocorre por meio da integração de informações técnicas, contextuais e comportamentais, permitindo compreender não apenas o que ocorreu, mas também quem são os possíveis adversários, quais técnicas estão sendo empregadas, quais ativos podem ser afetados e quais ações devem ser priorizadas para reduzir a exposição ao risco [28, 4, 5].

O crescimento exponencial da quantidade de dados disponíveis em ambientes digitais representa um dos principais fatores que impulsionaram essa evolução. Informações relevantes sobre ameaças são continuamente publicadas em bases de vulnerabilidades, repositórios públicos, fóruns especializados, redes sociais, plataformas de mensageria, mercados clandestinos e diversos outros ambientes digitais. Embora essas informações possuam elevado potencial para apoiar atividades defensivas, sua heterogeneidade, volatilidade e elevado volume tornam inviável uma análise exclusivamente manual. Assim, a Inteligência aplicada ao domínio cibernético passou a incorporar mecanismos automatizados capazes de coletar, organizar, correlacionar e enriquecer essas informações, permitindo produzir conhecimento em tempo compatível com a dinâmica das ameaças contemporâneas [21, 20, 29].

Essa evolução também modificou o papel desempenhado pelos analistas de segurança. Tradicionalmente responsáveis pela execução manual das atividades de coleta e análise, esses profissionais passaram a atuar de forma cada vez mais orientada pela interpretação dos resultados produzidos por sistemas automatizados. Nesse cenário, técnicas de aprendizado de máquina, processamento de linguagem natural, grafos de conhecimento e modelos de inteligência artificial assumem funções relacionadas à extração de entidades, identificação de padrões, enriquecimento semântico e correlação entre múltiplas fontes de informação, permitindo que os analistas concentrem seus esforços na validação das evidências, contextualização dos resultados e apoio à tomada de decisão [24, 20, 22].

Paralelamente aos avanços tecnológicos, observa-se uma mudança significativa na forma como o conhecimento produzido é compartilhado entre organizações. O caráter distribuído das ameaças cibernéticas faz com que informações obtidas por uma organização possam contribuir diretamente para a proteção de outras instituições pertencentes ao mesmo setor ou cadeia de suprimentos. Consequentemente, mecanismos colaborativos de compartilhamento tornaram-se estratégicos na produção de Inteligência cibernética. Revisões recentes destacam que arquiteturas modernas privilegiam padrões interoperáveis, mecanismos de confiança, preservação da integridade dos dados e modelos de governança capazes de estimular o intercâmbio seguro de informações entre diferentes organizações [25, 26, 6].

Outro aspecto amplamente discutido na literatura refere-se à necessidade de avaliar continuamente a qualidade da Inteligência produzida. Diferentemente de outras áreas do conhecimento, decisões relacionadas à segurança cibernética frequentemente precisam ser tomadas em ambientes caracterizados por informações incompletas, conflitantes ou sujeitas a rápida obsolescência. Dessa forma, atributos como confiabilidade, atualidade, relevância, completude e precisão tornam-se elementos essenciais para assegurar que a Inteligência efetivamente contribua para o processo decisório. Ali et al. [28] propõem um conjunto de métricas destinadas justamente à avaliação da qualidade dos produtos de Inteligência, demonstrando que mecanismos sistemáticos de validação aumentam significativamente sua utilidade operacional. Complementarmente, Lin et al. [23] demonstra que a correlação entre produtos de Inteligência e evidências observadas em ambientes reais constitui um importante mecanismo para validar e enriquecer continuamente o conhecimento produzido.

Nesse contexto, observa-se que a Inteligência aplicada ao domínio cibernético representa uma evolução natural dos princípios clássicos discutidos nas seções anteriores. O processo continua fundamentado na coleta, processamento, análise e disseminação de informações; entretanto, essas atividades passam a ser executadas em ambientes caracterizados por elevado volume de dados, múltiplas fontes de informação, necessidade de automação e intensa colaboração entre organizações. Mais do que uma adaptação tecnológica, essa evolução representa uma mudança na forma como organizações compreendem o cenário de ameaças, deslocando o foco da resposta reativa para a antecipação de riscos e para a produção contínua de conhecimento estratégico.

2.2.1 Cyber Threat Intelligence

O crescimento da superfície de ataque das organizações, impulsionado pela transformação digital, pela expansão dos serviços conectados e pelo aumento da sofisticação das ameaças cibernéticas, evidenciou limitações dos modelos tradicionais de segurança baseados exclusivamente em mecanismos preventivos

e reativos. Soluções como antivírus, firewalls e sistemas de detecção de intrusão continuam desempenhando papel fundamental na proteção dos ativos computacionais; entretanto, sua atuação concentra-se, predominantemente, na identificação ou mitigação de eventos já iniciados. Em um cenário caracterizado pela atuação contínua de grupos criminosos organizados, campanhas persistentes e rápida disseminação de novas técnicas de ataque, tornou-se necessário adotar abordagens capazes de antecipar ameaças e apoiar decisões antes que incidentes produzam impactos significativos. Nesse contexto, consolida-se o conceito de *Cyber Threat Intelligence* (CTI), cuja finalidade consiste em transformar informações relacionadas ao ambiente de ameaças em conhecimento acionável para apoiar atividades de prevenção, detecção, resposta e gestão de riscos [4, 5, 28].

Embora o termo CTI tenha sido amplamente difundido apenas na última década, seus fundamentos derivam diretamente dos princípios clássicos da atividade de Inteligência apresentados nas seções anteriores. Assim como ocorre na Inteligência tradicional, a CTI não corresponde simplesmente ao conjunto de informações obtidas sobre ameaças cibernéticas, mas ao resultado de um processo estruturado de coleta, processamento, análise e disseminação de conhecimento orientado às necessidades dos tomadores de decisão. Essa distinção é importante porque evidencia que indicadores técnicos isolados, listas de endereços IP maliciosos ou registros de vulnerabilidades não constituem Inteligência por si só. Somente após serem contextualizados, correlacionados e analisados em função do ambiente organizacional essas informações tornam-se produtos de CTI capazes de apoiar decisões estratégicas, táticas ou operacionais [2, 28].

A literatura recente apresenta diferentes definições para Cyber Threat Intelligence, porém observa-se convergência quanto aos seus objetivos centrais. Santos et al. [4] definem CTI como um conjunto de processos destinados à produção de conhecimento sobre ameaças, vulnerabilidades, adversários e técnicas empregadas em ataques cibernéticos, permitindo aumentar a capacidade das organizações de antecipar riscos e fortalecer sua postura defensiva. De forma semelhante, Saeed et al. [5] destacam que a CTI integra informações provenientes de múltiplas fontes para produzir conhecimento capaz de apoiar modelos de detecção, bases de conhecimento e mecanismos de visualização voltados ao aumento da resiliência organizacional. Complementando essas abordagens, Ali et al. [28] enfatizam que a efetividade da CTI depende não apenas da quantidade de informações disponíveis, mas principalmente de atributos relacionados à qualidade da Inteligência produzida, como precisão, completude, relevância, atualidade e confiabilidade.

Essa evolução também modificou o papel desempenhado pela Inteligência nas operações de segurança. Tradicionalmente, equipes de segurança concentravam seus esforços na análise de alertas gerados por dispositivos de proteção, atuando de maneira predominantemente reativa após a ocorrência de eventos suspeitos. Com a consolidação da CTI, a Inteligência passa a orientar diferentes atividades do ciclo de defesa, permitindo identificar campanhas em andamento, compreender objetivos dos adversários, priorizar vulnerabilidades críticas e direcionar ações de monitoramento antes da materialização dos ataques. Como consequência, observa-se uma mudança de paradigma na qual a Inteligência deixa de representar um produto complementar às operações de segurança e passa a constituir elemento estruturante dos processos de defesa cibernética [27, 29, 20].

O caráter multidimensional da CTI também é amplamente discutido na literatura. Diferentemente de métodos focadas exclusivamente em indicadores técnicos, a CTI incorpora informações relacionadas aos agentes de ameaça, suas motivações, capacidades, infraestrutura utilizada, campanhas observadas,

ativos potencialmente afetados e impactos esperados para determinada organização. Dessa forma, a CTI passa a integrar elementos técnicos e contextuais, permitindo compreender não apenas como um ataque pode ocorrer, mas também por que determinado adversário escolhe um alvo específico, quais objetivos pretende atingir e quais medidas podem ser adotadas para reduzir sua probabilidade de sucesso. Essa visão amplia significativamente o potencial da Inteligência como instrumento de apoio ao processo decisório, aproximando-a das necessidades estratégicas das organizações [25, 26, 6].

Além disso, a consolidação da CTI impulsionou o desenvolvimento de novos modelos de produção de conhecimento baseados na integração de diferentes tecnologias. Técnicas de mineração de dados, processamento de linguagem natural, aprendizado de máquina, grafos de conhecimento e Inteligência Artificial passaram a ser incorporadas às arquiteturas modernas de CTI com o objetivo de automatizar atividades relacionadas à extração de entidades, correlação de eventos, enriquecimento semântico e identificação de padrões complexos em grandes volumes de dados. Embora essas tecnologias ampliem significativamente a capacidade operacional dos sistemas de Inteligência, a literatura destaca que seu principal objetivo permanece alinhado aos fundamentos clássicos da atividade de Inteligência: produzir conhecimento confiável capaz de apoiar decisões relacionadas à proteção dos ativos organizacionais.

2.2.1.1 Níveis de CTI

A produção de Cyber Threat Intelligence não atende a um único perfil de usuário nem possui um formato uniforme de apresentação. Diferentes decisões exigem diferentes níveis de detalhamento, horizonte temporal e grau de contextualização das informações produzidas. Dessa forma, a literatura organiza a CTI em níveis distintos, permitindo que os produtos de Inteligência sejam direcionados às necessidades específicas dos diferentes atores envolvidos na segurança cibernética. Embora existam pequenas variações entre autores, observa-se consenso quanto à divisão da CTI em quatro níveis principais: estratégico, operacional, tático e técnico [3, 4, 5].

O nível estratégico destina-se aos gestores responsáveis pela definição das políticas de segurança, gestão de riscos e direcionamento dos investimentos organizacionais. Nesse nível, a Inteligência concentra-se na compreensão do cenário de ameaças, tendências de longo prazo, impactos para o negócio, aspectos regulatórios e riscos associados à organização. As informações produzidas apresentam elevado grau de contextualização e reduzido detalhamento técnico, permitindo apoiar decisões relacionadas ao planejamento estratégico da segurança cibernética. Em geral, os produtos desse nível assumem a forma de relatórios executivos, análises de tendências e avaliações de risco direcionadas à alta administração [4, 28, 27].

A Inteligência operacional ocupa um nível intermediário entre a visão estratégica e as atividades técnicas de defesa. Seu objetivo consiste em compreender campanhas maliciosas, perfis de adversários, objetivos dos ataques, infraestrutura utilizada e possíveis impactos para setores específicos. Esse nível de Inteligência subsidia equipes responsáveis pelo planejamento das operações de segurança, resposta a incidentes e atividades de caça a ameaças (*Threat Hunting*), permitindo priorizar recursos e direcionar ações defensivas de acordo com o comportamento observado dos agentes maliciosos [29, 5, 25].

No nível tático, a CTI passa a concentrar-se nas técnicas, táticas e procedimentos empregados pelos adversários. As informações produzidas buscam responder como determinado grupo conduz suas opera-

ções, quais vulnerabilidades explora, quais ferramentas utiliza e quais padrões de comportamento podem ser observados ao longo das diferentes fases do ataque. Esse tipo de Inteligência possui elevada relevância para analistas de segurança, equipes de monitoramento e profissionais responsáveis pela implementação de mecanismos de detecção, possibilitando adaptar controles de segurança de acordo com a evolução das ameaças observadas [29, 22, 23].

Por fim, a Inteligência técnica representa o nível mais granular da CTI. Nessa categoria encontram-se indicadores de comprometimento (*Indicators of Compromise – IoCs*), endereços IP maliciosos, domínios, hashes, assinaturas, regras de detecção e outros artefatos utilizados diretamente por ferramentas de segurança durante atividades de monitoramento e resposta. Embora possuam elevada utilidade operacional, esses indicadores apresentam curto ciclo de vida devido à rápida adaptação dos adversários, exigindo atualização contínua e mecanismos automatizados de validação e enriquecimento das informações coletadas [28, 24, 22]. A Figura 2.3 sintetiza a organização da CTI segundo seus diferentes níveis de atuação. Observa-se que, à medida que se avança do nível estratégico para o técnico, aumenta o detalhamento das informações produzidas, enquanto diminui o horizonte temporal das análises. Em contrapartida, os produtos estratégicos apresentam maior contextualização e apoiam decisões de longo prazo, ao passo que a Inteligência técnica concentra-se na detecção e mitigação imediata de ameaças.

Embora classificados em diferentes níveis, esses produtos não devem ser compreendidos como estruturas independentes. Pelo contrário, a efetividade da Cyber Threat Intelligence depende da integração entre informações estratégicas, operacionais, táticas e técnicas, permitindo que o conhecimento produzido em um nível complemente e fortaleça os demais. Essa integração constitui um dos principais diferenciais das arquiteturas modernas de CTI e estabelece as bases para o ciclo de produção de Inteligência discutido na próxima subseção.



Figura 2.3: Níveis da Cyber Threat Intelligence e seus principais consumidores. Adaptado de [4, 5, 3].

2.2.1.2 Ciclo de Inteligência de CTI

Cyber Threat Intelligence pode ser compreendida como um processo contínuo de transformação de dados brutos em conhecimento acionável, capaz de apoiar decisões relacionadas à prevenção, detecção, resposta e mitigação de ameaças cibernéticas. Embora seus fundamentos sejam derivados do Ciclo de Inteligência tradicional, a literatura demonstra que a CTI incorporou novos processos destinados a lidar com características próprias do ambiente cibernético, como elevado volume de informações, diversidade das fontes, rápida obsolescência dos indicadores e necessidade de atualização contínua. Dessa forma, o ciclo de produção da CTI preserva os princípios clássicos da Inteligência, porém incorpora mecanismos de automação, enriquecimento, correlação e compartilhamento que ampliam significativamente sua capacidade operacional [2, 3, 4].

Esse processo, não ocorre de forma estritamente linear, mas como um processo contínuo e iterativo, no qual os resultados obtidos em cada etapa influenciam as atividades subsequentes. Esse ciclo inicia-se com a **coleta**, **processamento**, **análise**, **disseminação** e **retroalimentação**, conforme ilustrado na figura 2.4. Embora diferentes autores utilizem terminologias específicas para cada fase, observa-se elevada convergência quanto às atividades desempenhadas em cada uma delas.

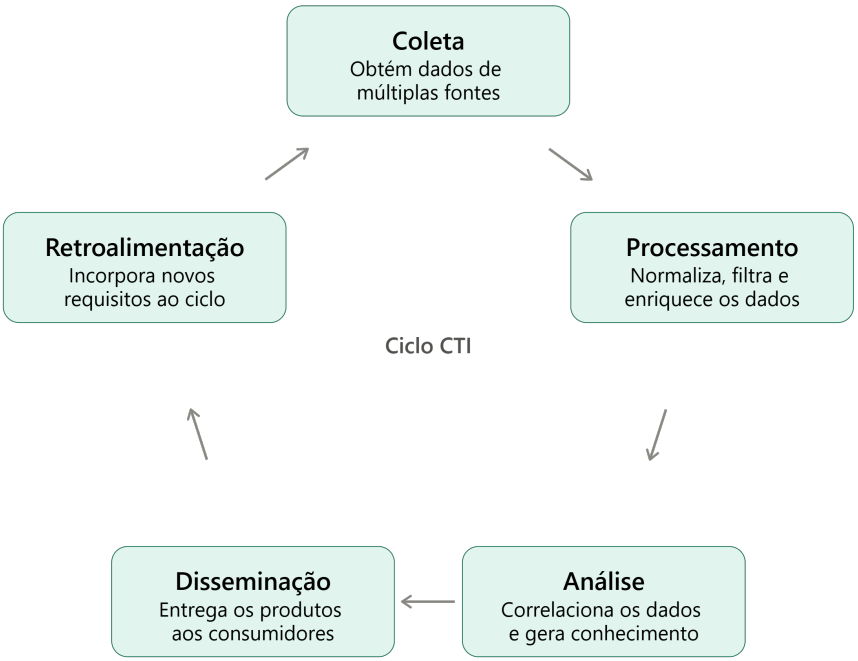


Figura 2.4: Ciclo básico de Cyber Threat Intelligence. Adaptado de [5, 4, 6].

A etapa de coleta representa o ponto de entrada do ciclo e tem como principal objetivo obter informações relevantes sobre ameaças, vulnerabilidades, agentes maliciosos e incidentes de segurança. A literatura destaca que a efetividade dessa etapa depende menos da quantidade de fontes monitoradas e mais da capacidade de selecionar informações compatíveis com os objetivos da organização.

Atualmente, arquiteturas modernas de CTI integram informações provenientes de bases de vulnerabilidades, relatórios técnicos, redes sociais, fóruns especializados, plataformas de compartilhamento de Inteligência, repositórios públicos, ambientes da *dark web* e serviços de mensageria, permitindo ampliar

significativamente a cobertura do monitoramento realizado [27, 30, 25].

Após a coleta, os dados obtidos passam pela etapa de processamento, responsável por transformar informações heterogêneas em estruturas passíveis de análise. Essa fase envolve atividades como remoção de duplicidades, normalização de formatos, extração de entidades, identificação de indicadores, enriquecimento semântico e organização das informações em modelos estruturados. Guo et al. [22] destacam que a construção de grafos de conhecimento permite integrar informações provenientes de diferentes fontes e reduzir inconsistências entre dados estruturados e não estruturados. De forma complementar, Han et al. [24] demonstram que técnicas baseadas em aprendizado profundo e *few-shot learning* ampliam significativamente a capacidade de extrair eventos e argumentos relacionados a ataques cibernéticos, enquanto Albarrak et al. [21] ressaltam o papel crescente do Processamento de Linguagem Natural na automatização dessas atividades.

A análise constitui o núcleo do ciclo de produção da CTI, sendo responsável por transformar informações processadas em conhecimento útil ao processo decisório. Diferentemente da simples organização dos dados, essa etapa envolve atividades de correlação, contextualização e interpretação das evidências disponíveis, permitindo compreender relações entre eventos, identificar padrões de comportamento e antecipar possíveis cenários de ameaça. Lin et al. [23] demonstram que a correlação entre produtos de CTI e evidências observadas em ambientes reais possibilita identificar lacunas na Inteligência disponível e enriquecer continuamente o conhecimento produzido. Em complemento, Mahboubi et al. [29] destacam que técnicas modernas de Threat Hunting dependem diretamente dessa capacidade analítica para formular hipóteses, validar comportamentos suspeitos e identificar ameaças que permanecem invisíveis aos mecanismos tradicionais de detecção.

A etapa de disseminação corresponde à disponibilização da Inteligência produzida aos diferentes consumidores, considerando suas necessidades específicas e níveis de atuação. Enquanto gestores estratégicos necessitam de análises voltadas à avaliação de riscos e tendências, equipes operacionais demandam informações relacionadas a campanhas, adversários e possíveis impactos, ao passo que analistas técnicos utilizam indicadores diretamente aplicáveis às ferramentas de monitoramento e resposta. Nesse contexto, a literatura evidencia crescente adoção de plataformas colaborativas de compartilhamento de CTI, permitindo que diferentes organizações troquem informações de forma padronizada, segura e interoperável. Trabalhos recentes demonstram que mecanismos de confiança, reputação e incentivos institucionais constituem fatores determinantes para ampliar a efetividade desses ecossistemas colaborativos [25, 26, 6].

Finalmente, o ciclo é concluído pela etapa de retroalimentação, responsável por avaliar a efetividade dos produtos de Inteligência produzidos e identificar novas necessidades informacionais. Essa característica diferencia a CTI de processos estáticos de monitoramento, uma vez que o conhecimento gerado em um ciclo influencia diretamente as prioridades e requisitos dos ciclos subsequentes. Além disso, mecanismos sistemáticos de avaliação da qualidade da Inteligência tornam-se fundamentais para garantir que os produtos disseminados permaneçam relevantes diante da rápida evolução do cenário de ameaças. Eli et al. [28] demonstram que atributos como precisão, completude, relevância e atualidade constituem métricas essenciais para mensurar a efetividade dos produtos de CTI, enquanto que Barrios et al. [20] ressaltam que a integração entre Inteligência Artificial e supervisão humana representa uma das principais tendências para o aperfeiçoamento contínuo desse ciclo.

Observa-se, portanto, que o ciclo de produção da Cyber Threat Intelligence representa uma evolução dos modelos clássicos de Inteligência, incorporando mecanismos capazes de lidar com a velocidade, complexidade e heterogeneidade das informações produzidas no ambiente cibernético. Embora tecnologias como Inteligência Artificial, Processamento de Linguagem Natural e grafos de conhecimento tenham ampliado significativamente a capacidade de automatização das atividades de coleta, processamento e análise, a literatura converge ao afirmar que a produção de CTI continua fundamentada nos princípios tradicionais da atividade de Inteligência: produzir conhecimento confiável, contextualizado e oportuno para apoiar decisões em diferentes níveis organizacionais. Essa estrutura estabelece as bases para compreender as diferentes fontes utilizadas na produção da CTI, tema abordado na próxima subseção.

2.2.2 Open Source Intelligence (OSINT)

A disponibilidade crescente de informações em ambientes digitais transformou profundamente a atividade de Inteligência nas últimas décadas. Enquanto os modelos tradicionais eram predominantemente dependentes de fontes restritas e processos centralizados de coleta, a expansão da Internet, das plataformas digitais e dos serviços baseados em dados públicos ampliou significativamente o acesso a informações potencialmente relevantes para atividades de defesa, segurança e gestão de riscos. Nesse cenário, a *Open Source Intelligence* (OSINT) consolidou-se como uma disciplina dedicada à identificação, coleta, processamento e análise de informações provenientes de fontes publicamente acessíveis, permitindo produzir conhecimento útil para apoiar processos decisórios em diferentes níveis organizacionais [31, 27, 32].

Embora frequentemente associada apenas à coleta de informações disponíveis na Internet, a literatura demonstra que a OSINT representa um processo de Inteligência muito mais amplo. Van Puyvelde et al. [31] argumentam que a evolução da OSINT não constitui uma ruptura com os princípios clássicos da atividade de Inteligência, mas sim uma adaptação desses princípios ao contexto de abundância informacional característico da sociedade digital. Sob essa perspectiva, a coleta em fontes abertas continua subordinada às mesmas etapas fundamentais de planejamento, análise e disseminação presentes no Ciclo de Inteligência, diferenciando-se principalmente pela diversidade das fontes disponíveis e pelo elevado volume de dados produzidos continuamente [31, 2, 3].

Essa evolução também modificou o papel desempenhado pelas fontes abertas na produção de conhecimento. Historicamente, atividades de OSINT concentravam-se em documentos oficiais, publicações governamentais, jornais, revistas e outros meios tradicionais de comunicação. Atualmente, o ecossistema de fontes abertas passou a incorporar plataformas de redes sociais, fóruns especializados, repositórios colaborativos, bases públicas de vulnerabilidades, mecanismos de busca, plataformas de compartilhamento de código, serviços de mensageria, blogs técnicos e diversas outras fontes digitais que produzem informações em tempo quase real. Como consequência, a atividade de Inteligência passou a lidar com volumes de dados significativamente superiores aos observados em modelos tradicionais, exigindo novas técnicas para seleção, filtragem e validação das informações coletadas [32, 27, 33].

Apesar da elevada disponibilidade de informações públicas, diversos autores ressaltam que a principal dificuldade da OSINT não está relacionada ao acesso às fontes, mas à capacidade de transformar grandes volumes de dados heterogêneos em conhecimento confiável [28, 23, 32]. Informações provenientes de fontes abertas frequentemente apresentam inconsistências, duplicidades, ausência de contexto, desatuali-

zação e diferentes níveis de credibilidade, tornando indispensável a adoção de mecanismos de validação e correlação entre múltiplas evidências. Nesse sentido, a produção de Inteligência baseada em fontes abertas depende menos da quantidade de informações disponíveis e mais da qualidade dos processos empregados para avaliar sua confiabilidade, contextualizar seu significado e integrar diferentes evidências em produtos analíticos consistentes

Outro aspecto amplamente discutido na literatura refere-se ao crescente emprego de técnicas de Inteligência Artificial para apoiar atividades de OSINT. et al. Browne et al. [33] identificam um crescimento significativo da utilização de aprendizado de máquina, processamento de linguagem natural, visão computacional e modelos de linguagem para automatizar tarefas relacionadas à coleta, classificação, extração de entidades, sumarização e correlação de informações provenientes de fontes abertas. De maneira semelhante, Barrios et al. [20] destacam que arquiteturas modernas de Inteligência tendem a combinar capacidades analíticas humanas com mecanismos automatizados de processamento, permitindo lidar com volumes de dados incompatíveis com abordagens exclusivamente manuais. Entretanto, ambos os trabalhos ressaltam que essas tecnologias devem atuar como mecanismos de apoio à atividade analítica, e não como substitutas da interpretação realizada por especialistas.

No domínio da cibersegurança, a OSINT passou a desempenhar papel estratégico na produção de Cyber Threat Intelligence. Informações relacionadas à divulgação de vulnerabilidades, campanhas maliciosas, grupos de ameaça, infraestrutura utilizada por atacantes, indicadores de comprometimento e vazamentos de dados frequentemente tornam-se públicas antes mesmo da exploração em larga escala. Consequentemente, organizações passaram a incorporar processos contínuos de monitoramento de fontes abertas como mecanismo para antecipar riscos e apoiar atividades de prevenção, detecção e resposta a incidentes. Essa integração entre OSINT e CTI constitui atualmente uma das principais tendências observadas na literatura especializada, aproximando os processos clássicos da atividade de Inteligência das demandas operacionais impostas pelo ambiente cibernético contemporâneo [27, 4, 29].

Observa-se, portanto, que a Open Source Intelligence evoluiu de um conjunto de técnicas voltadas à exploração de informações públicas para uma disciplina estruturada de produção de conhecimento, capaz de integrar diferentes fontes, métodos analíticos e tecnologias de processamento automatizado. Essa evolução ampliou significativamente o papel da OSINT na produção de Inteligência aplicada à cibersegurança, tornando-a um dos principais mecanismos de obtenção de informações para arquiteturas modernas de Cyber Threat Intelligence. Nesse contexto, compreender as características das diferentes categorias de fontes abertas torna-se fundamental para entender como essas informações são incorporadas aos processos contemporâneos de produção de Inteligência, tema abordado na próxima subseção.

2.2.2.1 Fontes abertas

A literatura normalmente classifica essas fontes em diferentes categorias de acordo com sua origem, natureza e finalidade. Entre as principais destacam-se bases públicas de vulnerabilidades, repositórios colaborativos de código, relatórios técnicos produzidos por organizações especializadas, plataformas de redes sociais, fóruns de discussão, blogs técnicos, serviços de mensageria, ambientes da *deep* e *dark web*, mecanismos de busca e plataformas dedicadas ao compartilhamento de Inteligência. Cada uma dessas categorias apresenta características particulares quanto ao volume de informações, velocidade de atualiza-

ção, confiabilidade e potencial para produção de conhecimento, tornando necessária a utilização conjunta de diferentes fontes para obtenção de uma visão mais abrangente do cenário de ameaças [32, 33, 27].

Entre as fontes estruturadas, destacam-se bases públicas de vulnerabilidades, como o *National Vulnerability Database* (NVD), avisos emitidos por CERTs, boletins de fabricantes e bancos públicos de indicadores de comprometimento. Essas fontes apresentam elevado grau de padronização e confiabilidade, constituindo importantes mecanismos para identificação de vulnerabilidades conhecidas, exploração de falhas e atualização de mecanismos de defesa. Entretanto, sua natureza predominantemente reativa faz com que muitas informações sejam disponibilizadas somente após a divulgação pública das vulnerabilidades ou da identificação de campanhas maliciosas, reduzindo sua capacidade de antecipação em determinados cenários [4, 5, 28].

Em complemento às bases estruturadas, observa-se crescente utilização de fontes não estruturadas, como blogs técnicos, fóruns especializados, repositórios públicos, plataformas colaborativas e redes sociais. Embora essas fontes apresentem maior heterogeneidade e menor padronização, frequentemente disponibilizam informações inéditas sobre vulnerabilidades, ferramentas utilizadas por agentes maliciosos, novas campanhas de ataque e discussões técnicas que antecedem publicações formais. Como consequência, arquiteturas modernas de CTI vêm incorporando técnicas de Processamento de Linguagem Natural, aprendizado de máquina e extração automática de entidades para transformar grandes volumes de dados textuais em conhecimento estruturado e passível de correlação [22, 21, 33].

Garkava et al. [30] investigam o funcionamento de mercados ilícitos estabelecidos no Telegram por meio da metodologia de rime script analysis, analisando 16 canais e grupos públicos e privados utilizados para comercialização de dados sensíveis. Os autores demonstram que esses ambientes apresentam uma estrutura relativamente organizada, composta por vendedores, compradores e administradores responsáveis por estabelecer regras de funcionamento, mecanismos de reputação e estratégias para divulgação dos conteúdos comercializados. Entre as informações compartilhadas destacam-se credenciais de acesso, informações financeiras, dados pessoais e bases de dados comprometidas, evidenciando que a plataforma passou a desempenhar papel relevante como ambiente de negociação e disseminação de ativos utilizados em atividades cibercriminosas. Além de descrever a dinâmica desses mercados, o estudo propõe medidas de prevenção situacional para reduzir sua efetividade, reforçando a importância do monitoramento contínuo dessas comunidades para fins de investigação e produção de Inteligência

Essas evidências demonstram que plataformas de mensageria deixaram de atuar apenas como canais de comunicação entre usuários para consolidarem-se como importantes ambientes de produção, compartilhamento e comercialização de informações relacionadas à segurança cibernética. Consequentemente, esses ambientes passaram a constituir fontes relevantes para atividades de Cyber Threat Intelligence, especialmente quando o objetivo consiste em identificar precocemente indicadores associados a campanhas maliciosas, credenciais comprometidas e outras evidências de interesse para os processos de monitoramento e resposta a incidentes [30, 27].

Apesar das vantagens proporcionadas pela diversidade de fontes abertas, a literatura ressalta que nenhuma fonte, individualmente, é capaz de representar de forma completa o cenário de ameaças. Informações obtidas em ambientes distintos frequentemente apresentam níveis variados de qualidade, confiabilidade, granularidade e atualidade, tornando indispensável a correlação entre múltiplas evidências durante

a produção da Inteligência. Nesse contexto, mecanismos de enriquecimento semântico, fusão de dados e validação cruzada assumem papel fundamental para reduzir inconsistências, eliminar redundâncias e aumentar a confiabilidade dos produtos de CTI. Trabalhos recentes demonstram que a integração entre diferentes fontes produz resultados significativamente superiores quando comparada à utilização isolada de qualquer ambiente de coleta [23, 22, 28].

Observa-se, portanto, que a diversidade de fontes abertas constitui um dos principais fatores responsáveis pela evolução da Cyber Threat Intelligence nas últimas décadas. A combinação entre bases estruturadas, fontes textuais, plataformas colaborativas e serviços de mensageria amplia significativamente a capacidade das organizações de monitorar o ambiente de ameaças e produzir conhecimento contextualizado para apoio à tomada de decisão. Entre essas diferentes categorias, as plataformas de mensageria vêm despertando crescente interesse da comunidade científica devido ao elevado volume de informações compartilhadas e à rapidez com que novos conteúdos são disponibilizados, aspecto que fundamenta sua utilização como objeto de investigação nesta dissertação.

2.2.2.2 Critérios para seleção de fontes OSINT

Entretanto, essa grande disponibilidade de fontes abertas trouxe novos desafios para a produção de Cyber Threat Intelligence. Se, por um lado, a diversidade de ambientes digitais amplia significativamente a quantidade de informações potencialmente relevantes, por outro, torna inviável o monitoramento indiscriminado de todas as fontes disponíveis. Dessa forma, a seleção das fontes a serem monitoradas constitui uma etapa estratégica do processo de Inteligência, influenciando diretamente a qualidade, a oportunidade e a confiabilidade dos produtos gerados. A literatura recente destaca que arquiteturas modernas de CTI devem estabelecer critérios objetivos para priorizar fontes capazes de fornecer informações alinhadas às necessidades informacionais da organização e ao contexto operacional em que estão inseridas [27, 32, 4].

Entre os critérios mais frequentemente discutidos na literatura destaca-se a relevância da informação para os objetivos da Inteligência. Nem toda informação disponível em fontes abertas apresenta valor analítico para determinada organização, sendo necessário avaliar sua capacidade de responder aos requisitos definidos durante o planejamento da atividade de Inteligência. Nesse contexto, informações relacionadas a campanhas maliciosas, vulnerabilidades exploradas ativamente, indicadores de comprometimento, credenciais expostas e atividades conduzidas por agentes de ameaça tendem a apresentar maior relevância para processos de Cyber Threat Intelligence quando comparadas a conteúdos genéricos ou pouco contextualizados [2, 3, 27].

Sobretudo, o cenário cibernético caracteriza-se pela rápida evolução das ameaças e pela constante adaptação dos agentes maliciosos, reduzindo significativamente o tempo de vida útil de muitos indicadores técnicos. Como consequência, fontes capazes de disponibilizar informações em tempo próximo aos eventos observados tornam-se particularmente relevantes para atividades de monitoramento contínuo e resposta antecipada. Trabalhos recentes demonstram que a capacidade de reduzir o intervalo entre a divulgação de uma ameaça e sua identificação pelas organizações representa um dos principais fatores responsáveis pelo aumento da efetividade da CTI [28, 23, 29].

A confiabilidade das fontes constitui um aspecto essencial para a produção de Inteligência. Informa-

ções provenientes de ambientes abertos podem apresentar diferentes níveis de credibilidade, sofrer manipulações deliberadas ou conter dados incompletos e desatualizados. Dessa forma, a literatura recomenda que mecanismos de validação, atribuição de confiança e correlação entre múltiplas fontes sejam empregados continuamente durante o processo de produção da Inteligência. A utilização de evidências provenientes de diferentes ambientes reduz a probabilidade de falsos positivos, aumenta a robustez das análises e contribui para a produção de conhecimento mais consistente e confiável [28, 22, 23].

Além da relevância e da confiabilidade, aspectos relacionados ao volume e à diversidade das informações também influenciam a seleção das fontes monitoradas. Fontes caracterizadas por elevado fluxo de publicações e diversidade temática tendem a fornecer maior quantidade de indicadores potencialmente úteis, mas exigem mecanismos automatizados capazes de realizar filtragem, normalização e priorização das informações coletadas. Revisões recentes demonstram que técnicas de aprendizado de máquina, processamento de linguagem natural e Inteligência Artificial vêm sendo cada vez mais empregadas para apoiar essas atividades, permitindo transformar grandes volumes de dados não estruturados em conhecimento passível de análise [33, 20, 21].

Outro critério relevante refere-se à acessibilidade da fonte e à viabilidade de coleta contínua. Embora diversas informações relevantes estejam disponíveis em ambientes restritos ou dependam de credenciais específicas para acesso, fontes públicas apresentam vantagens relacionadas à escalabilidade, facilidade de integração com ferramentas automatizadas e menor complexidade operacional. Além disso, a utilização de informações publicamente disponíveis favorece a reprodutibilidade das pesquisas e reduz limitações relacionadas ao acesso a bases proprietárias ou comerciais, aspecto particularmente importante em estudos acadêmicos voltados ao desenvolvimento de arquiteturas de Cyber Threat Intelligence [31, 32, 27].

Nos últimos anos, plataformas de mensageria tornaram-se de grande relevancia nesse ecossistema. Diferentemente de fóruns tradicionais, esses ambientes caracterizam-se pela elevada velocidade de disseminação das informações, facilidade de criação de comunidades e reduzido custo operacional para os agentes envolvidos. Estudos demonstram que plataformas como o Telegram são utilizadas não apenas para compartilhamento de informações entre pesquisadores e profissionais de segurança, mas também para comercialização de bases de dados, distribuição de ferramentas maliciosas e coordenação de atividades ilícitas. Essas características tornam plataformas como o Telegram particularmente relevantes para atividades de Cyber Threat Intelligence voltadas à identificação precoce de vazamentos e indicadores associados a campanhas maliciosas [30, 27, 29].

Dessa forma, fica evidente que a seleção de fontes OSINT deve considerar simultaneamente critérios relacionados à relevância, atualidade, confiabilidade, volume, diversidade e acessibilidade das informações disponíveis. Esses fatores influenciam diretamente a qualidade da Inteligência produzida e determinam a capacidade das arquiteturas de CTI em identificar precocemente eventos de interesse. Nesse contexto, a escolha de plataformas de mensageria como fonte de monitoramento não decorre apenas de sua popularidade, mas principalmente de sua capacidade de disponibilizar informações relevantes em tempo oportuno, justificando seu crescente emprego em pesquisas voltadas à produção de Inteligência cibernética.

2.3 MÉTODOS E TÉCNICAS APLICADOS A CYBER THREAT INTELLIGENCE

Conforme abordado, a produção de Cyber Threat Intelligence envolve um conjunto de métodos e técnicas responsáveis por transformar dados provenientes de diferentes fontes em conhecimento estruturado e útil ao processo decisório. Embora o ciclo de Inteligência estabeleça as etapas gerais para produção da Inteligência, sua operacionalização no domínio cibernético exige arquiteturas computacionais capazes de lidar com grandes volumes de dados heterogêneos, coletados continuamente em ambientes dinâmicos e distribuídos. Nesse contexto, diferentes soluções têm sido propostas para automatizar atividades de coleta, processamento, análise, correlação, armazenamento e disseminação das informações, reduzindo o tempo necessário para transformar evidências de ameaças em produtos de Inteligência acionáveis [5, 20].

A evolução dessas arquiteturas acompanha o crescimento da complexidade do cenário de ameaças cibernéticas e a diversificação das fontes de informação utilizadas na produção da CTI. Além das bases tradicionais de vulnerabilidades e indicadores de comprometimento, plataformas de mensageria, redes sociais, repositórios públicos, fóruns especializados e outras fontes abertas passaram a integrar os processos de coleta e análise, demandando mecanismos automatizados capazes de adquirir, estruturar e correlacionar informações provenientes de ambientes com diferentes níveis de estruturação e confiabilidade. Como consequência, a literatura tem direcionado esforços para o desenvolvimento de pipelines modulares e escaláveis, fundamentados em técnicas de Processamento de Linguagem Natural, Inteligência Artificial, representação estruturada do conhecimento e plataformas especializadas para gerenciamento de grandes volumes de dados [34, 22, 33].

Dessa forma, esta seção apresenta os principais métodos e técnicas empregados na produção da Cyber Threat Intelligence, abordando as arquiteturas de coleta, as estratégias de aquisição de dados, os mecanismos de processamento, análise e correlação das informações, bem como as plataformas utilizadas para armazenamento, compartilhamento e visualização da Inteligência produzida. O objetivo é apresentar o estado da arte das tecnologias empregadas na operacionalização da CTI, estabelecendo a base conceitual necessária para compreensão da arquitetura proposta nesta dissertação.

2.3.1 Métodos e técnicas de coleta

A coleta de informações representa a etapa inicial do processo de produção da Cyber Threat Intelligence (CTI) e constitui um dos principais fatores que influenciam a qualidade dos produtos de Inteligência. Embora os modelos clássicos de Inteligência já reconhecessem a importância da obtenção sistemática de informações para reduzir incertezas, a crescente disponibilidade de dados em ambientes digitais modificou profundamente a forma como essa atividade é conduzida. Atualmente, arquiteturas modernas de CTI caracterizam-se pela integração contínua de múltiplas fontes de informação, combinando mecanismos automatizados de aquisição, processamento e enriquecimento capazes de lidar com grandes volumes de dados produzidos em tempo quase real. Como consequência, a coleta deixou de representar uma atividade predominantemente manual para tornar-se um processo contínuo, distribuído e altamente automatizado, fundamental para a antecipação de ameaças cibernéticas [4, 5, 31].

Uma das arquiteturas mais completas identificadas na literatura é apresentada por Balasubramanian et

al. [34] por meio da plataforma TSTEM (*Threat Sensing, Tracking and Early Monitoring*). Os autores propõem uma arquitetura cognitiva composta por módulos independentes responsáveis pela coleta, processamento, enriquecimento e visualização de Cyber Threat Intelligence. A etapa de coleta integra diferentes fontes abertas utilizando *web crawlers*, APIs, mecanismos de *streaming* e ferramentas como Scrapy e Apache Kafka, permitindo a aquisição contínua de informações provenientes de páginas Web, redes sociais e outras fontes abertas. Segundo os autores, a utilização de uma arquitetura baseada em microsserviços favorece a escalabilidade da solução e reduz o tempo entre a publicação de novas evidências e sua disponibilização para análise, evidenciando uma tendência de adoção de pipelines distribuídos em plataformas modernas de CTI

Sob uma perspectiva mais ampla, Santos et al. [4] realizaram uma revisão sistemática envolvendo 43 estudos sobre Cyber Threat Intelligence e observaram que as arquiteturas contemporâneas convergem para modelos modulares compostos por etapas independentes de coleta, processamento, análise e disseminação. Os autores destacam que a diversidade das fontes monitoradas exige a combinação de diferentes mecanismos de aquisição de dados, incluindo APIs, bases públicas de vulnerabilidades, plataformas colaborativas, repositórios de código, redes sociais e fontes OSINT. Como resultado, defendem que arquiteturas de CTI devem priorizar flexibilidade e capacidade de integração entre diferentes mecanismos de coleta, em vez de depender de uma única tecnologia ou fonte de informação.

Resultados semelhantes são apresentados por Saeed et al. [5] que propõem um framework conceitual para implementação de Cyber Threat Intelligence em ambientes organizacionais. O trabalho organiza a produção da Inteligência em diferentes camadas, nas quais a coleta representa o primeiro componente operacional responsável por alimentar todo o restante da arquitetura. Os autores ressaltam que a efetividade das etapas posteriores depende diretamente da qualidade e da abrangência das informações obtidas durante a aquisição dos dados, recomendando a integração entre fontes estruturadas e não estruturadas para ampliar a cobertura do monitoramento.

A evolução das plataformas de mensageria também impulsionou mudanças importantes nas arquiteturas de coleta. Diferentemente dos ambientes tradicionais da Web, plataformas como Telegram apresentam elevada velocidade de publicação, grande quantidade de comunidades especializadas e intenso compartilhamento de informações relacionadas à segurança cibernética. Em resposta a essas características, diversos trabalhos passaram a desenvolver arquiteturas específicas para coleta nesses ambientes.

Baumgartner et al. [35] apresentam estratégias específicas para coleta em plataformas de mensageria com uma infraestrutura para aquisição contínua de mensagens públicas do Telegram, construída com o objetivo de disponibilizar um grande conjunto de dados para pesquisas envolvendo análise de comunidades e comportamento de usuários. A arquitetura proposta demonstra a viabilidade técnica da coleta automatizada em larga escala, permitindo o monitoramento contínuo de milhares de canais públicos. Entretanto, o trabalho limita-se à construção do conjunto de dados, não contemplando etapas de extração, correlação ou produção de Cyber Threat Intelligence

La Morgia et al. [36] propõem uma estratégia voltada à descoberta automática de canais do Telegram por meio de um mecanismo de expansão incremental (*snowball crawling*). A arquitetura explora as conexões existentes entre canais para identificar automaticamente novas comunidades potencialmente relevantes, reduzindo a dependência de listas previamente conhecidas e ampliando a cobertura da coleta. Os

autores demonstram que essa estratégia aumenta significativamente a capacidade de descoberta de novas fontes, aspecto considerado essencial em ambientes caracterizados pela constante criação de novos grupos e canais

Outro aspecto recorrente na literatura refere-se à necessidade de integrar informações provenientes de diferentes categorias de fontes. Bases públicas de vulnerabilidades, relatórios técnicos, plataformas colaborativas, redes sociais, repositórios de código, fóruns especializados e serviços de mensageria produzem informações com diferentes níveis de estruturação, periodicidade e confiabilidade. Consequentemente, arquiteturas contemporâneas empregam mecanismos capazes de coletar simultaneamente dados estruturados e não estruturados, utilizando estratégias específicas para cada ambiente monitorado. Essa diversidade amplia significativamente a cobertura da Inteligência produzida, permitindo correlacionar evidências provenientes de múltiplas origens e reduzir lacunas observacionais durante o monitoramento do cenário de ameaças [27, 32, 4].

No que diz respeito a técnicas de coleta, não existe uma técnica única de coleta capaz de atender às necessidades de todos os cenários. Em vez disso, arquiteturas contemporâneas combinam diferentes mecanismos de aquisição de dados, selecionados de acordo com as características das fontes, a frequência de atualização das informações e os objetivos da Inteligência. Essa diversidade permite ampliar a cobertura do monitoramento, reduzir lacunas observacionais e aumentar a capacidade de antecipação de ameaças emergentes [4, 5, 27].

A literatura identifica diferentes estratégias para aquisição de informações em arquiteturas de CTI, variando desde mecanismos estruturados de consulta até técnicas voltadas à extração automática de informações não estruturadas. Entre as abordagens mais utilizadas destacam-se APIs, *web crawling*, *web scraping*, agentes automatizados (*bots*) e mecanismos de processamento contínuo de fluxos de dados (*streaming*). Cada técnica apresenta características particulares quanto ao tipo de fonte suportada, escalabilidade, complexidade de implementação e capacidade de atualização, tornando sua escolha dependente das necessidades específicas da arquitetura de Inteligência. A Tabela 2.2 apresenta uma síntese comparativa dessas principais estratégias identificadas na literatura.

As APIs representam uma das estratégias mais utilizadas para obtenção de dados estruturados em arquiteturas modernas de CTI. Esse mecanismo permite acesso controlado às informações disponibilizadas por diferentes plataformas, reduzindo inconsistências durante a coleta e facilitando a integração entre sistemas. Além de possibilitar consultas automatizadas, APIs normalmente oferecem mecanismos de autenticação, controle de acesso, paginação e atualização incremental, tornando-se particularmente adequadas para monitoramento contínuo de bases de vulnerabilidades, indicadores de comprometimento e plataformas de compartilhamento de Inteligência [37, 4, 5].

Quando as informações não são disponibilizadas por meio de interfaces estruturadas, arquiteturas de CTI frequentemente recorrem a técnicas de *web crawling* e *web scraping*. Enquanto o *crawler* é responsável pela navegação automática entre páginas e descoberta de novos conteúdos, o *scraping* concentra-se na extração das informações de interesse presentes nesses ambientes. Essas técnicas são amplamente empregadas no monitoramento de fóruns especializados, blogs técnicos, repositórios públicos e diferentes ambientes da Web, permitindo ampliar significativamente o conjunto de fontes monitoradas. Entretanto, sua utilização exige mecanismos adicionais de tratamento de mudanças estruturais nas páginas, remoção

de ruídos e normalização dos dados coletados [33, 34, 27].

Tabela 2.2: Estratégias de aquisição de dados empregadas em arquiteturas modernas de Cyber Threat Intelligence.

Técnica	**Aplicação**	**Vantagens**	**Limitações**
APIs	Bases estruturadas, plataformas de CTI e serviços Web	Dados estruturados, autenticação, atualização incremental e integração simplificada	Dependência da disponibilidade e das restrições impostas pela API
Web Crawling	Descoberta automática de páginas e novas fontes	Elevada cobertura e expansão automática das fontes monitoradas	Complexidade de navegação e mudanças na estrutura dos ambientes monitorados
Web Scraping	Extração de informações de páginas Web	Flexibilidade para coleta de dados não estruturados	Sensível a alterações de layout e necessidade de manutenção frequente
Bots por Avatares	Redes sociais e plataformas de mensageria	Monitoramento contínuo e baixa latência na aquisição de novos conteúdos	Dependência das políticas e limitações das plataformas monitoradas
Streaming	Feeds contínuos de eventos e Inteligência	Atualização em tempo próximo ao real e processamento contínuo	Elevado volume de dados e necessidade de processamento distribuído

[34, 27, 33, 37]

Outra estratégia amplamente adotada consiste na utilização de agentes automatizados (*bots*) para monitoramento contínuo de plataformas específicas. Diferentemente de mecanismos tradicionais de coleta periódica, esses agentes permanecem continuamente conectados às fontes monitoradas permitindo identificar novas publicações poucos instantes após sua disponibilização. Essa abordagem é particularmente relevante em ambientes caracterizados por elevada velocidade de propagação das informações, como plataformas de mensageria e redes sociais, nas quais indicadores relacionados a campanhas maliciosas, vazamentos de credenciais e infraestrutura utilizada por agentes de ameaça podem tornar-se obsoletos em curtos intervalos de tempo. Vale ressaltar que em muitos casos os Bots dependem de avatares que simulam uma persona, para conseguir realizar o monitoramento e se manter presente na rede social ou forum [29, 34, 38].

Plataformas de mensageria representam um caso particular dentro das estratégias de coleta em CTI. Diferentemente das páginas Web tradicionais, esses ambientes organizam as informações em canais, grupos e conversas continuamente atualizados, exigindo mecanismos específicos para autenticação, descoberta de comunidades e aquisição das mensagens publicadas. Trabalhos recentes demonstram diferentes estratégias para coleta automatizada nesses ambientes, incluindo expansão incremental de canais monitorados, coleta contínua baseada em eventos e construção de grandes conjuntos de dados destinados ao treinamento de modelos de Inteligência Artificial. Essas técnicas evidenciam a crescente importância das plataformas de mensageria como fontes relevantes para produção de Cyber Threat Intelligence [35, 36, 38].

2.3.2 Métodos e técnicas de processamento

Após a aquisição das informações provenientes de diferentes fontes, as arquiteturas de Cyber Threat Intelligence iniciam uma etapa de processamento responsável por transformar dados heterogêneos em informações estruturadas e passíveis de análise. Essa fase representa um dos principais desafios da CTI contemporânea, uma vez que os dados coletados apresentam diferentes formatos, níveis de estruturação, idiomas, granularidades e graus de confiabilidade. Dessa forma, o processamento constitui um conjunto de atividades voltadas à limpeza, transformação, normalização e organização das informações, preparando-as para as etapas posteriores de correlação, enriquecimento e produção de Inteligência. A literatura destaca que a qualidade dos produtos de CTI depende diretamente da eficiência dessas etapas intermediárias, sendo insuficiente concentrar esforços apenas na ampliação da capacidade de coleta [4, 5, 22].

Em arquiteturas modernas de CTI, o processamento normalmente é organizado em pipelines compostos por diferentes módulos especializados, responsáveis por executar sucessivamente tarefas de pré-processamento, extração de informações relevantes e estruturação dos dados. Essa abordagem modular permite desacoplar as diferentes etapas do processamento, favorecendo escalabilidade, reutilização dos componentes e adaptação da arquitetura a novas fontes de informação. Além disso, pipelines estruturados possibilitam automatizar atividades tradicionalmente executadas de forma manual, reduzindo o tempo necessário para disponibilizar novas evidências às equipes responsáveis pela análise das ameaças [34, 39, 22].

As primeiras etapas do processamento concentram-se na preparação dos dados coletados. Informações provenientes de diferentes ambientes frequentemente apresentam duplicidades, inconsistências de codificação, formatos distintos e conteúdos irrelevantes ao objetivo da Inteligência. Em consequência, arquiteturas de CTI empregam procedimentos de limpeza, padronização e normalização capazes de remover ruídos, uniformizar representações e organizar atributos provenientes de múltiplas fontes. Essas atividades reduzem inconsistências durante as etapas posteriores de análise e aumentam a qualidade dos dados utilizados para produção da Inteligência [4, 33, 21].

Após a preparação inicial dos dados, arquiteturas contemporâneas empregam técnicas de extração automática para identificar entidades, eventos e relacionamentos relevantes ao contexto da segurança cibernética. O avanço das técnicas de Processamento de Linguagem Natural (Natural Language Processing – NLP) permitiu automatizar a identificação de indicadores de comprometimento, vulnerabilidades, campanhas de ataque, grupos de ameaça, ferramentas utilizadas por atacantes e demais elementos frequentemente presentes em relatórios de CTI e informações provenientes de fontes abertas. Trabalhos recentes demonstram que modelos baseados em aprendizado profundo e aprendizado com poucos exemplos (*few-shot learning*) apresentam resultados superiores aos métodos tradicionais na extração de eventos cibernéticos, principalmente em cenários caracterizados pela escassez de dados rotulados [24, 21, 33].

Entre as técnicas propostas para estruturação das informações extraídas, destaca-se a utilização de modelos conjuntos de reconhecimento de entidades e extração de relações. Guo et al. [22] e Marchiori et al. [40] propõem um framework capaz de extrair simultaneamente entidades e seus relacionamentos a partir de fontes estruturadas e não estruturadas, reduzindo problemas de propagação de erros presentes em arquiteturas sequenciais. De maneira semelhante, o Iacovazzi et al. [41] automatiza a identificação dos principais objetos definidos pelo padrão STIX em relatórios de CTI, permitindo converter documentos textuais em representações estruturadas e semanticamente consistentes. Essas técnicas demonstram a tendência da li-

teratura em substituir processos manuais de interpretação por mecanismos automatizados de representação do conhecimento. A Tabela 2.3 apresenta uma síntese comparativa dessas principais estratégias identificadas na literatura no que diz respeito a processamento de dados.

Tabela 2.3: Principais técnicas empregadas no processamento de Cyber Threat Intelligence.

Etapa	**Objetivo**	**Principais técnicas**
Limpeza	Remover inconsistências e ruídos	Filtragem, deduplicação e tratamento de dados
Normalização	Uniformizar a representação das informações	Padronização de atributos, formatos e codificação
Extração	Identificar entidades e eventos relevantes	NLP, NER, Deep Learning e Few-shot Learning
Estruturação	Representar o conhecimento extraído	STIX, grafos de conhecimento e modelos relacionais
Enriquecimento	Contextualizar informações coletadas	Correlação entre fontes, bases externas e IoCs

[22, 24, 40, 21].

Observa-se, portanto, que o processamento deixou de representar apenas uma etapa intermediária entre a coleta e a análise para assumir papel central nas arquiteturas modernas de Cyber Threat Intelligence. A crescente utilização de técnicas de Inteligência Artificial, Processamento de Linguagem Natural, representação estruturada do conhecimento e modelos de extração automática evidencia uma evolução em direção a pipelines capazes de transformar grandes volumes de dados heterogêneos em conhecimento estruturado, contextualizado e adequado às etapas posteriores de correlação e análise. Nesse contexto, o enriquecimento das informações extraídas tornou-se um componente essencial para ampliar o valor analítico dos dados coletados, aspecto discutido na próxima subseção dedicada aos métodos de análise e correlação em Cyber Threat Intelligence.

2.3.3 Métodos e técnicas de análise e correlação

A etapa de análise representa o núcleo do processo de produção da Cyber Threat Intelligence, sendo responsável por transformar informações estruturadas em conhecimento capaz de apoiar a tomada de decisão. Após o processamento inicial dos dados, arquiteturas modernas de CTI empregam diferentes mecanismos para identificar relações entre eventos, validar evidências, contextualizar indicadores de comprometimento e inferir comportamentos associados a campanhas maliciosas. Diferentemente das etapas anteriores, cujo objetivo consiste na preparação dos dados, a análise busca produzir conhecimento contextualizado, reduzindo incertezas e aumentando a capacidade das organizações de antecipar ameaças cibernéticas [4, 5, 28].

Entre as principais técnicas empregadas nessa etapa destacam-se a correlação entre múltiplas fontes de informação, o enriquecimento de indicadores de comprometimento, a fusão de dados, a construção de grafos de conhecimento e a aplicação de modelos baseados em Inteligência Artificial. Essas abordagens permitem relacionar informações provenientes de diferentes ambientes, identificar padrões de comporta-

mento e produzir uma visão mais abrangente das ameaças observadas. A Tabela 2.4 sintetiza as principais técnicas de análise identificadas na literatura e suas respectivas finalidades.

Tabela 2.4: Principais técnicas empregadas na análise e correlação em Cyber Threat Intelligence.

Técnica	**Objetivo**	**Aplicações**
Correlação de dados	Relacionar informações provenientes de diferentes fontes	Associação de IoCs, campanhas e infraestrutura maliciosa
Enriquecimento	Adicionar contexto às informações coletadas	Consulta a bases externas, MITRE ATT&CK, CVE, WHOIS e DNS
Fusão de dados	Integrar evidências heterogêneas	Consolidação de informações estruturadas e não estruturadas
Grafos de conhecimento	Representar entidades e seus relacionamentos	Identificação de atores, campanhas e infraestrutura
Inteligência Artificial	Automatizar análises e identificar padrões	Classificação, predição e apoio à tomada de decisão

[23, 22, 20, 28].

A correlação entre múltiplas fontes constitui uma das atividades mais importantes da CTI moderna. Ali et al. [28] demonstram que a comparação entre informações provenientes de feeds de Inteligência e evidências observadas em ambientes reais permite identificar tanto falsos positivos quanto indicadores ainda não contemplados pelas bases de CTI existentes. Além de aumentar a confiabilidade das informações produzidas, essa estratégia possibilita enriquecer continuamente a Inteligência disponível, ampliando a cobertura dos indicadores utilizados pelas organizações

Complementando essa abordagem, Guo et al. [22] propõem um framework de extração e fusão de Inteligência baseado em grafos de conhecimento, no qual entidades e relacionamentos extraídos de diferentes fontes são integrados em uma representação única. Essa estratégia reduz redundâncias, melhora a consistência das informações e facilita a identificação de conexões entre campanhas, grupos de ameaça, vulnerabilidades e indicadores de comprometimento. A utilização de grafos também favorece análises mais complexas, permitindo representar relações que dificilmente seriam identificadas por mecanismos tradicionais de processamento sequencial.

Outra tendência observada na literatura refere-se ao crescente emprego de Inteligência Artificial para apoiar atividades de análise. Técnicas de aprendizado de máquina, aprendizado profundo e modelos de linguagem vêm sendo utilizadas para classificar ameaças, identificar padrões de comportamento e prever possíveis desdobramentos de campanhas maliciosas. Barrios-González et al. [20] destacam que essas tecnologias ampliam significativamente a capacidade analítica das plataformas de CTI, enquanto Mahboubi et al. [29] ressaltam que os modelos automatizados devem atuar como mecanismos de apoio ao analista, preservando a formulação de hipóteses e a interpretação contextual como atividades essencialmente humanas.

Entretanto, a qualidade das análises produzidas depende diretamente da qualidade dos dados utilizados.

O trabalho de Ali et al. [28] argumenta que atributos como precisão, completude, relevância e atualidade devem ser continuamente avaliados durante a produção da CTI, uma vez que informações desatualizadas ou inconsistentes podem comprometer o processo decisório. Dessa forma, mecanismos de validação, pontuação de confiança e atualização contínua das bases de conhecimento tornam-se componentes essenciais das arquiteturas modernas de Inteligência.

Observa-se, portanto, que a análise em Cyber Threat Intelligence deixou de restringir-se à interpretação manual de informações para incorporar técnicas avançadas de correlação, enriquecimento e representação do conhecimento. A integração entre múltiplas fontes, aliada ao emprego de Inteligência Artificial e modelos de representação estruturada, permite produzir conhecimento mais preciso, contextualizado e adequado ao apoio à tomada de decisão. Essa evolução também impulsionou o desenvolvimento de plataformas especializadas para armazenamento, compartilhamento e visualização da Inteligência produzida, tema abordado na próxima subseção.

2.3.4 Plataformas para armazenamento, indexação, compartilhamento e visualização

A crescente quantidade de informações produzidas ao longo do ciclo de Cyber Threat Intelligence tornou insuficientes os mecanismos tradicionais de armazenamento e gerenciamento de dados. Como consequência, arquiteturas modernas passaram a incorporar plataformas especializadas capazes de armazenar, indexar, compartilhar e visualizar grandes volumes de informações provenientes de múltiplas fontes. Essas plataformas permitem centralizar indicadores de comprometimento, campanhas, vulnerabilidades, atores de ameaça e demais evidências coletadas, proporcionando maior eficiência na produção e disseminação da Inteligência. Além disso, favorecem a interoperabilidade entre diferentes organizações e ferramentas, aspecto considerado fundamental para o fortalecimento dos ecossistemas de compartilhamento de CTI [37, 25, 4].

Um dos principais avanços observados na literatura refere-se à adoção de padrões voltados à representação e ao compartilhamento estruturado das informações. O Structured Threat Information Expression (STIX) consolidou-se como um dos formatos mais utilizados para modelar objetos relacionados à segurança cibernética, permitindo representar indicadores de comprometimento, campanhas, vulnerabilidades, identidades, infraestruturas e relacionamentos entre esses elementos de forma padronizada. Complementarmente, o Trusted Automated eXchange of Intelligence Information (TAXII) estabelece mecanismos para compartilhamento automatizado dessas informações entre diferentes plataformas, promovendo interoperabilidade e reduzindo esforços de integração entre sistemas heterogêneos [37, 40, 36].

A adoção desses padrões impulsionou o desenvolvimento de plataformas especializadas para gerenciamento da Cyber Threat Intelligence. Soluções como o Malware Information Sharing Platform (MISP) e o Open Cyber Threat Intelligence (OpenCTI) permitem centralizar informações provenientes de diferentes fontes, compartilhar indicadores de comprometimento entre organizações e representar relacionamentos complexos entre entidades de interesse. Essas plataformas também disponibilizam mecanismos de enriquecimento automático, controle de acesso, colaboração entre analistas e integração nativa com padrões como STIX e TAXII, tornando-se componentes amplamente empregados em arquiteturas modernas de CTI [37, 25, 36].

Além das plataformas especializadas, a literatura demonstra crescente utilização de mecanismos de indexação e busca para suportar o armazenamento e a recuperação eficiente de grandes volumes de dados de Inteligência. Motores de busca distribuídos, como o Elasticsearch, possibilitam indexar informações semi-estruturadas provenientes de múltiplas fontes, oferecendo consultas em tempo próximo ao real, agregações estatísticas e elevada escalabilidade horizontal. Essas características tornam essa tecnologia particularmente adequada para arquiteturas de CTI que processam continuamente grandes volumes de indicadores de comprometimento, eventos e artefatos relacionados à segurança cibernética. Trabalhos recentes demonstram a utilização do Elasticsearch como componente central em arquiteturas de coleta e análise de CTI, evidenciando seu potencial para suportar atividades de armazenamento, pesquisa e correlação de informações [34, 42, 37].

Outra técnica empregada consiste na utilização de bancos de dados orientados a grafos para representação explícita dos relacionamentos existentes entre diferentes entidades da Inteligência. Diferentemente dos bancos orientados a documentos, essas plataformas priorizam a modelagem das conexões entre atores, campanhas, vulnerabilidades, indicadores e infraestruturas, favorecendo atividades de correlação e investigação. Trabalhos como os de Guo et al. [22] demonstram que a utilização de grafos de conhecimento permite integrar informações provenientes de diferentes fontes e identificar relações complexas entre eventos cibernéticos, ampliando significativamente a capacidade analítica das plataformas de CTI [40, 36].

Além do armazenamento e da indexação, a visualização das informações constitui uma etapa essencial para transformar grandes volumes de dados em conhecimento útil aos analistas. Dashboards interativos, consultas analíticas e representações gráficas permitem identificar tendências, acompanhar indicadores de comprometimento, monitorar campanhas e apoiar atividades de investigação e resposta a incidentes. A literatura destaca que mecanismos eficientes de visualização reduzem a sobrecarga cognitiva dos analistas e favorecem a compreensão do cenário de ameaças, tornando as plataformas de visualização componentes indispensáveis das arquiteturas modernas de Cyber Threat Intelligence [4, 25, 34].

2.3.5 Síntese Comparativa dos Trabalhos Correlatos

Os trabalhos correlatos apresentados nas seções anteriores evidenciam diferentes formas de obtenção, processamento e estruturação de dados para produção de Cyber Threat Intelligence. As pesquisas analisadas abrangem desde estudos sobre a utilização de OSINT para cibersegurança proativa até arquiteturas automatizadas para coleta, extração, correlação e estruturação de informações relacionadas a ameaças. Também foram identificados trabalhos que utilizam o Telegram como fonte de dados, seja para construção de grandes conjuntos de dados, seja para identificação e extração automatizada de informações relacionadas à segurança cibernética.

Embora esses estudos apresentem elementos relacionados à solução desenvolvida nesta dissertação, existem diferenças quanto ao objeto monitorado, às técnicas empregadas e, principalmente, à finalidade da informação produzida. Nesse sentido, a Tabela 2.5 sintetiza os principais trabalhos analisados e os compara com a presente pesquisa, considerando as fontes de dados utilizadas, os métodos empregados, as formas de avaliação e suas principais características.

A presente pesquisa diferencia-se principalmente pelo objeto monitorado e pela finalidade operacional

da arquitetura. Em vez de construir um conjunto de dados geral sobre o Telegram ou um dataset contendo diferentes categorias de IoCs, a solução proposta direciona a produção de CTI para a identificação de credenciais expostas associadas a ativos de interesse previamente definidos. Para isso, a arquitetura integra a aquisição programática de mensagens e arquivos, a extração de credenciais por meio de regras e expressões regulares, a normalização e filtragem pelos domínios monitorados, a indexação das ocorrências, sua análise e a disseminação automatizada por meio de alertas.

Tabela 2.5: Comparação entre os trabalhos correlatos e a presente pesquisa.

Trabalho	**Fonte de dados**	**Método**	**Avaliação**	**Principal característica**
Avrahami et al. [27]	Literatura científica e profissional	Revisão sobre OSINT aplicada à cibersegurança	Análise qualitativa da literatura	Discute o emprego de OSINT para cibersegurança proativa e sua relação com a produção de CTI.
Guo et al. [22]	CTI estruturada e não estruturada	Extração e fusão de informações de inteligência	Avaliação experimental	Extração de entidades e relações e integração das informações para construção de *Knowledge Graph*.
Balasubramanian et al. [34]	Fontes abertas	Coleta, NLP, classificação e extração	Avaliação experimental	TSTEM: *pipeline* automatizado para produção de CTI baseado em arquitetura de microsserviços.
Baumgartner et al. [35]	Canais públicos do Telegram	Coleta automatizada de dados do Telegram	Dataset em larga escala	Construção de dataset geral do Telegram, abrangendo aproximadamente 27,8 mil canais, 317 milhões de mensagens e 2,2 milhões de usuários.
Arikkat et al. [38]	Canais relacionados à CTI no Telegram	*Pipeline* automatizado, classificação baseada em IA e extração de IoCs	Classificação de conteúdo	Construção automatizada de dataset de CTI a partir de mensagens do Telegram, incluindo diferentes categorias de IoCs.
Esta pesquisa	**Canais e grupos públicos do Telegram**	**API, Regex, normalização, filtragem, indexação, análise e alertas**	**PoC executada durante três meses**	**Monitoramento contínuo de credenciais expostas associadas a 239 domínios de interesse, integrando coleta, processamento, indexação, análise e disseminação.**

A análise dos trabalhos correlatos evidencia que a literatura apresenta contribuições relevantes para diferentes etapas da produção de CTI, incluindo aquisição de dados provenientes de fontes abertas, extração e estruturação de informações de ameaças, construção de conjuntos de dados e utilização do Telegram como fonte de informações relacionadas à segurança cibernética. Entretanto, nos trabalhos analisados, não foi identificada a integração dessas etapas em um fluxo contínuo especificamente direcionado ao moni-

toramento de credenciais expostas associadas a ativos de interesse previamente definidos, contemplando desde a aquisição automatizada dos dados até sua análise e disseminação aos responsáveis pelos ativos monitorados. Essa lacuna delimita o problema científico explorado nesta pesquisa.

Diante dessa lacuna, a contribuição metodológica desta pesquisa consiste na proposição e validação de uma arquitetura integrada para produção de Cyber Threat Intelligence, estruturada como um fluxo contínuo que articula coleta, processamento, indexação, análise e disseminação. A contribuição não reside isoladamente nas técnicas empregadas em cada etapa, uma vez que mecanismos como acesso por API, expressões regulares, indexação e visualização já são conhecidos na literatura, mas na organização e integração desses mecanismos em um processo orientado ao monitoramento de credenciais expostas associadas a ativos de interesse. A arquitetura estabelece, assim, um encadeamento entre a obtenção de dados provenientes de fontes abertas, sua transformação em registros estruturados, a contextualização em relação aos domínios monitorados e a disponibilização das ocorrências para análise e disseminação.

3 DISCUSSÃO DO PROBLEMA E PROPOSTA

A crescente ocorrência de vazamentos de dados tem contribuído para o aumento da disponibilidade de credenciais expostas em diferentes ambientes digitais. Credenciais contendo combinações de login e senha são frequentemente compartilhadas, comercializadas ou redistribuídas em comunidades associadas ao cibercrime, tornando-se recursos valiosos para a realização de acessos não autorizados, fraudes, campanhas de phishing, movimentação lateral e outras atividades maliciosas. Estudos recentes indicam que credenciais comprometidas permanecem entre os principais vetores utilizados por agentes maliciosos para obtenção de acesso inicial a ambientes corporativos, evidenciando a necessidade de mecanismos capazes de identificar precocemente sua exposição [8, 7].

Paralelamente, observa-se uma mudança significativa na dinâmica de divulgação dessas informações. Embora fóruns clandestinos e marketplaces especializados continuem sendo utilizados para comercialização de dados comprometidos, plataformas de comunicação instantânea passaram a desempenhar papel cada vez mais relevante nesse ecossistema. Entre elas, o Telegram destaca-se pela facilidade de criação de grupos, canais e comunidades capazes de compartilhar grandes volumes de informações, incluindo bases de dados vazadas, credenciais corporativas e conteúdos associados a operações conduzidas por agentes maliciosos. Pesquisas recentes demonstram que a plataforma vem sendo amplamente utilizada para disseminação de dados roubados e coordenação de atividades ilícitas, tornando-se uma fonte relevante para atividades de monitoramento e produção de inteligência [30, 17].

Apesar da ampla disponibilidade dessas informações em fontes abertas, muitas organizações ainda enfrentam dificuldades para identificar rapidamente quando credenciais associadas aos seus domínios são expostas. Em diversos casos, o tempo transcorrido entre a divulgação da credencial e sua identificação pelos responsáveis pela segurança pode permitir sua exploração por terceiros, ampliando os impactos decorrentes do incidente. Esse cenário evidencia uma lacuna operacional relacionada ao monitoramento contínuo de fontes abertas potencialmente associadas à divulgação de credenciais comprometidas, bem como à transformação dessas informações em inteligência acionável para apoio à tomada de decisão [8, 23].

3.1 METODOLOGIA

A metodologia adotada nesta pesquisa foi concebida com o objetivo de propor e validar uma prova de conceito para o monitoramento contínuo de credenciais comprometidas divulgadas em fontes abertas, com foco em canais e grupos da plataforma Telegram frequentemente utilizados para compartilhamento de bases vazadas. Busca-se descrever, de forma sistemática e reprodutível, o processo metodológico empregado para conceber uma arquitetura capaz de coletar, processar, correlacionar e analisar credenciais potencialmente associadas a organizações previamente definidas, transformando dados brutos obtidos em fontes abertas em inteligência acionável para apoio à tomada de decisão.

A pesquisa possui natureza aplicada, uma vez que busca solucionar um problema prático relacionado

à identificação tempestiva de credenciais comprometidas, por meio do desenvolvimento de uma pipeline computacional composto por módulos de coleta, processamento, indexação, análise e geração de alertas. Adicionalmente, a solução foi concebida para operar de forma contínua, reduzindo o intervalo entre a divulgação de uma credencial e sua identificação pelas organizações potencialmente afetadas.

A proposta fundamenta-se na inte gração de conceitos provenientes de Open Source Intelligence (OSINT), Cyber Threat Intelligence (CTI) e resposta a incidentes, permitindo não apenas a identificação de credenciais expostas, mas também contextualização e disseminação para os responsáveis pela proteção dos ativos monitorados.

A primeira etapa da metodologia consistiu na realização de um levantamento bibliográfico e análise crítica da literatura relacionada à Inteligência de Ameaças Cibernéticas, Open Source Intelligence, monitoramento de ameaças, credenciais comprometidas e utilização de plataformas de comunicação como fontes de obtenção de informações relevantes para defesa cibernética. Essa etapa permitiu identificar limitações observadas em abordagens tradicionais de monitoramento, especialmente no que se refere à identificação automatizada de credenciais divulgadas em ambientes dinâmicos e descentralizados, como grupos e canais do Telegram.

Posteriormente, foi definida uma estrutura metodológica baseada na adaptação do modelo 5W3H, empregada como mecanismo de apoio à definição dos requisitos informacionais necessários para caracterização dos eventos observados. A utilização dessa metodologia permitiu estruturar os metadados coletados em torno das dimensões What, Who, Where, When, Why, How, How Many e How Much, possibilitando uma representação mais completa do contexto associado às credenciais identificadas. Além de orientar a modelagem dos dados armazenados pela solução, essa estrutura também foi utilizada como referência para a definição dos indicadores, consultas e *dashboards* desenvolvidos para apoio às atividades de análise e produção de inteligência.

Com base nesses elementos, desenvolveu-se uma arquitetura composta por módulos independentes de coleta, processamento e análise. O módulo de coleta é responsável pelo monitoramento automatizado dos ambientes selecionados, realizando a obtenção periódica de mensagens e arquivos compartilhados. O módulo de processamento executa a extração, normalização e correlação das credenciais identificadas, associando-as a domínios previamente monitorados. Por fim, o módulo de análise utiliza mecanismos de indexação, visualização e geração de alertas para transformar os dados coletados em informações capazes de apoiar processos de investigação, resposta e mitigação de riscos.

Por meio dessa estratégia metodológica, busca-se demonstrar a viabilidade da utilização integrada de técnicas de OSINT e CTI para identificação contínua de credenciais comprometidas, contribuindo para o fortalecimento da consciência situacional cibernética e para a redução do tempo necessário para detecção e resposta a potenciais exposições de credenciais organizacionais. A Tabela 3.1 apresenta a adaptação da metodologia 5W3H para o contexto desta pesquisa.

Além da metodologia 5W3H, a concepção da solução também foi influenciada pelo modelo OODA (Observe, Orientar, Decidir e agir), originalmente proposto por Boyd [43] para apoiar processos decisórios em ambientes dinâmicos e caracterizados por elevada incerteza. Embora desenvolvido inicialmente para aplicações militares, o modelo tem sido amplamente empregado em contextos de segurança e defesa cibernética devido à sua capacidade de representar ciclos contínuos de observação, análise, tomada de decisão

Tabela 3.1: Aplicação da metodologia 5W3H no contexto da pesquisa

Dimensão	**Aplicação na pesquisa**
What	Credencial comprometida identificada
Who	Usuário responsável pela publicação da informação
Where	Canal ou grupo de origem da divulgação
When	Data e horário da publicação
Why	Contexto observado para a divulgação da informação
How	Forma de disponibilização da credencial (texto, arquivo compactado, lista, entre outros)
How Many	Quantidade de credenciais identificadas
How Much	Potencial impacto da exposição, avaliado posteriormente pelos analistas

e resposta.

No contexto do monitoramento de credenciais comprometidas, a simples identificação de uma exposição não constitui, por si só, um resultado de inteligência. Embora mecanismos automatizados de coleta e armazenamento sejam capazes de identificar grandes volumes de dados potencialmente relevantes, o valor estratégico dessas informações está diretamente relacionado à sua capacidade de apoiar decisões e orientar ações de proteção. Sob essa perspectiva, a presente pesquisa parte do entendimento de que credenciais expostas devem ser tratadas como indicadores de potenciais ameaças, cuja relevância depende de um processo contínuo de contextualização, análise e resposta.

A integração entre o ciclo de inteligência [44] e o modelo OODA foi concebida com o objetivo de transformar dados obtidos em fontes abertas em inteligência acionável. Nesse modelo, a observação (*Observar*) materializa-se por meio do monitoramento contínuo de grupos e canais do Telegram utilizados para compartilhamento de credenciais e bases de dados comprometidas. Essa atividade amplia a capacidade de percepção do ambiente monitorado e permite a identificação tempestiva de novos eventos de interesse.

A etapa de orientação (*Orientar*) corresponde ao conjunto de atividades responsáveis pela transformação dos dados coletados em informações contextualizadas. Nessa fase, são executados os processos de extração, normalização, correlação e enriquecimento dos registros identificados, incorporando elementos capazes de ampliar a compreensão do cenário observado. A aplicação da metodologia 5W3H desempenha papel fundamental nesse processo, uma vez que fornece uma estrutura para organização dos metadados coletados, permitindo caracterizar não apenas a credencial identificada, mas também seu contexto de divulgação, origem e potencial relevância para os objetivos de monitoramento definidos.

A decisão (*Decidir*) está associada à produção da inteligência propriamente dita. Diferentemente de abordagens centradas exclusivamente na análise técnica dos dados, essa etapa busca interpretar os eventos observados à luz das necessidades informacionais da organização, identificando prioridades, potenciais impactos e possíveis cursos de ação. O conhecimento produzido passa a representar um insumo para o processo decisório, contribuindo para a construção de uma compreensão mais abrangente do cenário de ameaças.

Por sua vez, a ação (*Agir*) corresponde à materialização da inteligência produzida em medidas concretas de resposta. Essas ações podem incluir a emissão de alertas, a comunicação aos responsáveis pelos

ativos monitorados, a revogação preventiva de credenciais comprometidas, a abertura de processos investigativos ou outras medidas compatíveis com a criticidade do evento identificado. Os resultados obtidos a partir dessas ações retroalimentam o processo analítico, promovendo o refinamento contínuo dos critérios de monitoramento e das capacidades de detecção da solução.

Dessa forma, o modelo proposto de coleta e armazenamento de dados estabelece um ciclo contínuo de monitoramento, interpretação e resposta. A integração entre CTI, 5W3H, OODA e práticas de resposta a incidentes permite que eventos observados em fontes abertas sejam continuamente convertidos em conhecimento contextualizado e, posteriormente, em ações voltadas à mitigação de riscos. Como resultado, busca-se fortalecer a consciência situacional cibernética das organizações monitoradas, ampliando sua capacidade de identificar, compreender e responder de forma tempestiva às exposições de credenciais observadas no ambiente digital.

3.2 PROPOSTA

A metodologia proposta é operacionalizada por meio de um ciclo integrado de monitoramento e resposta, composto pelas etapas de direção, planejamento, coleta, processamento, análise e produção, disseminação e retroalimentação. Essas etapas são complementadas por atividades relacionadas à detecção, notificação, análise de impacto, tomada de decisão e resposta, permitindo que a inteligência produzida seja continuamente incorporada ao processo de monitoramento.

A Figura 3.1 apresenta o ciclo de inteligencia desenvolvido, o modelo consolida elementos oriundos do ciclo de Inteligência de Ameaças Cibernéticas, da metodologia 5W3H, do modelo OODA e dos processos de resposta a incidentes, estabelecendo um fluxo contínuo de coleta, análise, disseminação e retroalimentação da inteligência produzida.

Adotar o modelo possibilita uma relação direta entre a produção de inteligência e a execução de ações de resposta, podendo reduzir o intervalo entre a identificação de um evento relevante e a adoção de medidas destinadas à mitigação dos riscos associados. Para materializar esse fluxo, foi desenvolvida uma arquitetura composta por três módulos principais: coleta, processamento e análise.

O ciclo apresentado na Figura 3.1 define a lógica operacional responsável por orientar a obtenção, processamento, análise e disseminação da inteligência produzida. Entretanto, para que esse fluxo pudesse ser executado de forma contínua e automatizada, tornou-se necessária a implementação de uma arquitetura capaz de operacionalizar cada uma das etapas previstas no modelo. Nesse contexto, a solução proposta foi estruturada em módulos especializados responsáveis pela coleta das informações, processamento dos dados obtidos, armazenamento dos registros produzidos e disponibilização dos resultados para análise e resposta. A arquitetura desenvolvida busca garantir que os dados obtidos em fontes abertas sejam progressivamente transformados em informações contextualizadas e posteriormente em inteligência acionável, preservando a integração entre os processos de monitoramento, análise e mitigação descritos anteriormente.

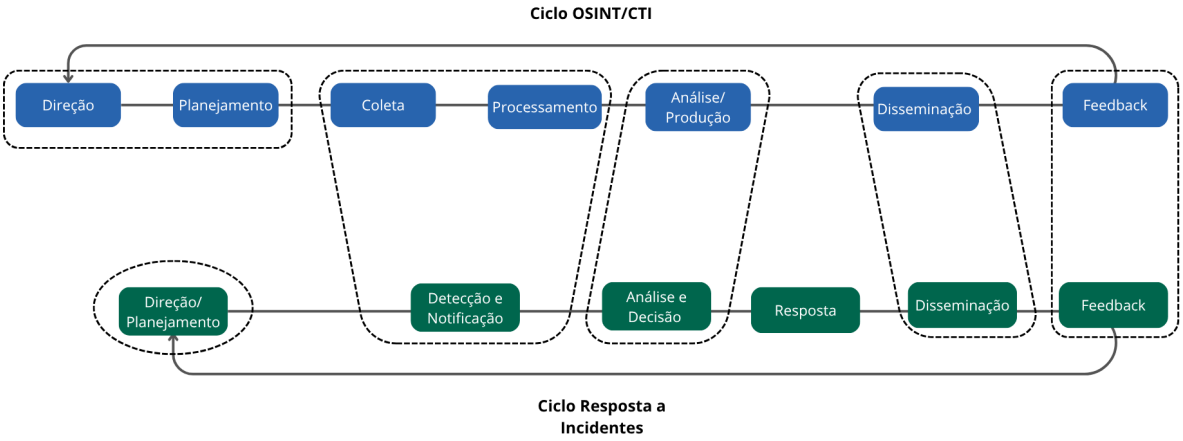


Figura 3.1: Ciclo integrado de monitoramento, produção de inteligência e resposta proposto nesta pesquisa.
Fonte: Elaboração própria

3.3 ARQUITETURA DA SOLUÇÃO

Para materializar esse fluxo, foi desenvolvida uma arquitetura composta por módulos responsáveis pela coleta, processamento, indexação, análise e disseminação das informações produzidas durante o monitoramento. Essa organização busca estabelecer um fluxo contínuo de aquisição, tratamento e exploração dos dados, permitindo que informações potencialmente relevantes sejam convertidas em inteligência acionável para apoio às atividades de monitoramento e resposta.

A arquitetura foi projetada considerando características frequentemente observadas em ambientes de divulgação de dados vazados, como elevado volume de informações, diversidade de formatos de compartilhamento e necessidade de rápida identificação de eventos relevantes. Dessa forma, cada módulo possui responsabilidades específicas e complementares, contribuindo para a construção de um processo escalável e passível de adaptação a diferentes cenários de monitoramento. A Figura 3.2 apresenta a arquitetura geral da solução proposta e o fluxo de informações entre seus componentes.

O fluxo operacional inicia-se pela aquisição de dados em grupos e canais monitorados, prossegue com a extração e correlação das credenciais identificadas e culmina na indexação e disponibilização das informações para consulta, visualização e geração de alertas. Essa estrutura permite que novas exposições sejam continuamente incorporadas ao processo analítico, favorecendo a manutenção da consciência situacional cibernética sobre os ativos monitorados.

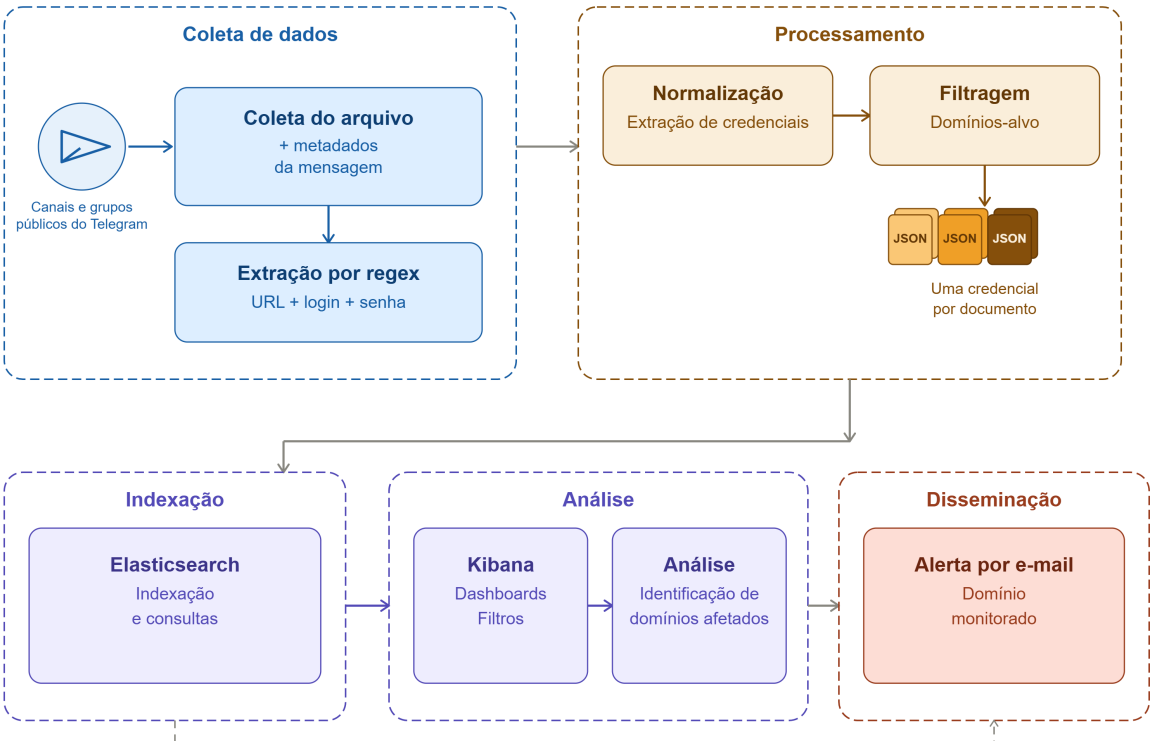


Figura 3.2: Arquitetura da pipeline proposta nesta pesquisa.
Fonte: Elaboração própria

3.3.1 Módulo de Coleta de dados

O módulo de coleta é responsável pelo monitoramento automatizado de grupos e canais públicos do Telegram previamente definidos. Implementado em Python por meio da biblioteca Telethon. Além das mensagens textuais, o módulo também realiza o download automático dos arquivos compartilhados nos ambientes monitorados. São suportados diferentes formatos de arquivos, incluindo arquivos compactados protegidos por senha. Nesses casos, a solução busca automaticamente informações presentes na mensagem associada, permitindo a abertura e processamento do conteúdo quando a senha está disponível.

Além dos arquivos coletados, o módulo preserva metadados considerados relevantes para a análise posterior, incluindo data e horário da publicação, nome do grupo ou canal de origem e identificador do usuário responsável pelo compartilhamento. Esses elementos são posteriormente utilizados para contextualização e correlação das informações processadas.

Entretanto, a coleta de informações em ambientes potencialmente frequentados por agentes maliciosos impõe desafios adicionais relacionados à segurança operacional (Operational Security – OPSEC) do processo de monitoramento. A exposição direta de perfis institucionais ou de pesquisadores pode resultar na identificação das atividades de observação, comprometendo a continuidade da coleta e potencialmente expondo a infraestrutura utilizada para monitoramento.

Com o objetivo de mitigar esses riscos, a estratégia de coleta foi concebida com base no emprego de avatares digitais através da aquisição de um número virtual anônimo adquirido via plataforma baseada em blockchain (Fragment – TON), especificamente destinados às atividades de monitoramento. Esses

avatares consistem em identidades digitais controladas utilizadas exclusivamente para acesso aos ambientes monitorados, reduzindo a exposição de perfis pessoais ou institucionais durante o processo de obtenção das informações.

A utilização de avatares também contribui para a segregação das atividades operacionais da pesquisa, permitindo que os processos de monitoramento sejam conduzidos de forma independente dos ambientes corporativos e das identidades dos pesquisadores envolvidos. Sob a perspectiva de inteligência, essa prática está alinhada aos princípios de OPSEC amplamente empregados em atividades de coleta, investigação e monitoramento, nos quais a preservação da capacidade de observação constitui um requisito fundamental para manutenção da efetividade da operação.

Vale ressaltar que o restante do processo de coleta foi concebido de forma predominantemente passiva, restringindo-se à observação, recuperação e processamento das informações disponibilizadas nos ambientes monitorados. Dessa forma, a solução não realiza interações com os participantes dos grupos observados, não promove disseminação de conteúdo e não executa atividades destinadas à obtenção ativa de acesso privilegiado aos ambientes analisados.

A seleção dos grupos e canais monitorados foi realizada com base em sua relevância para os objetivos da pesquisa, priorizando ambientes nos quais foram observados compartilhamentos recorrentes de credenciais comprometidas e bases de dados vazadas. Considerando a natureza dinâmica dessas comunidades, caracterizada pela criação, migração e desativação frequente de canais, o processo de monitoramento foi concebido de forma flexível, permitindo a inclusão ou remoção de fontes sem necessidade de alterações estruturais na solução.

Uma vez estabelecida a presença nos grupos e canais monitorados, o processo de coleta é executado periodicamente em intervalos de seis horas, permitindo a identificação de novas mensagens publicadas desde a última execução. Durante cada ciclo de monitoramento são recuperadas informações associadas às mensagens e aos arquivos compartilhados nos ambientes monitorados.

Os dados obtidos durante a coleta apresentam elevado grau de diversidade, tanto em relação aos tipos de arquivos quanto à forma como as credenciais são representadas. Diferentes grupos e canais utilizam convenções distintas para divulgação das informações, frequentemente combinando registros estruturados e não estruturados em arquivos contendo milhares de entradas. Essa diversidade dificulta a realização de análises automatizadas e exige mecanismos capazes de transformar os dados coletados em informações padronizadas e passíveis de exploração analítica.

Outro aspecto relevante diz respeito à persistência da coleta. Em ecossistemas caracterizados por elevada volatilidade, a perda de acesso a uma fonte monitorada pode resultar na interrupção do fluxo informacional e na consequente redução da visibilidade sobre eventos de interesse. Dessa forma, a solução foi projetada para preservar a continuidade operacional da coleta ao longo do tempo, garantindo a manutenção do acesso às fontes monitoradas e a recuperação periódica de novos conteúdos disponibilizados pelos usuários.

Ao final de cada ciclo de coleta, os dados obtidos são armazenados temporariamente e encaminhados ao módulo de processamento, responsável pela identificação, extração e normalização das credenciais encontradas.

3.3.2 Módulo de Processamento

O módulo de processamento é responsável pela extração, normalização e filtragem das credenciais identificadas. Inicialmente, os registros coletados são correlacionados com uma lista de domínios previamente definidos como objetos de interesse para identificar automaticamente credenciais potencialmente associadas às organizações monitoradas, reduzindo o esforço analítico necessário para triagem dos eventos identificados.

Posteriormente, os dados que passaram pela triagem são analisados por meio de expressões regulares desenvolvidas para identificar padrões compatíveis com credenciais comprometidas, incluindo registros contendo URL, login e senha ou combinações compostas apenas por login e senha. Cada credencial identificada é convertida em um documento JSON independente, enriquecido com metadados contextuais, tais como grupo de origem, usuário responsável pela publicação, data da postagem e domínio associado à credencial.

3.3.2.1 Estrutura dos Dados Produzidos

Um dos principais desafios associados à análise de credenciais comprometidas consiste na elevada heterogeneidade dos dados coletados. Informações provenientes de diferentes grupos frequentemente apresentam estruturas distintas, níveis variados de completude e formatos incompatíveis entre si, dificultando sua correlação e exploração analítica.

Com o objetivo de padronizar os registros produzidos durante o processo de monitoramento, a solução proposta adota um modelo de representação baseado na individualização das credenciais identificadas. Dessa forma, cada credencial extraída durante o processamento é convertida em um registro independente, preservando simultaneamente os atributos de autenticação identificados e os metadados necessários para contextualização do evento observado.

Além de facilitar consultas e correlações posteriores, a individualização das credenciais possibilita que cada ocorrência seja analisada em conjunto com os metadados associados à sua divulgação. A preservação de informações como domínio, grupo de origem, usuário responsável pela publicação, data da divulgação e data da coleta permite correlacionar eventos observados em diferentes momentos e fontes monitoradas.

Essa estrutura possibilita identificar, por exemplo, credenciais repetidamente associadas a um mesmo domínio, observar o reaparecimento de registros idênticos em grupos distintos e verificar a frequência com que determinados ativos são mencionados ao longo do período monitorado. Da mesma forma, a associação temporal entre os registros permite acompanhar a evolução do volume de credenciais divulgadas para um determinado domínio, identificando aumentos significativos na quantidade de exposições observadas em intervalos específicos.

A modelagem adotada também favorece a identificação de persistência da exposição. Credenciais associadas a um mesmo domínio que continuam sendo observadas ao longo de múltiplos ciclos de coleta ou em diferentes fontes monitoradas podem indicar que o comprometimento permanece circulando no ecossistema monitorado, mesmo após sua divulgação inicial. Sob a perspectiva da inteligência, essa informação pode representar um indicativo relevante para priorização de atividades de investigação e mitigação.

Adicionalmente, a identificação de credenciais duplicadas permite distinguir eventos efetivamente novos de republicações de vazamentos previamente observados. Essa diferenciação contribui para reduzir ruídos analíticos e possibilita uma avaliação mais precisa do comportamento das exposições associadas aos ativos monitorados. Dessa forma, os registros deixam de representar apenas combinações isoladas de autenticação e passam a constituir elementos observáveis de um cenário mais amplo de exposição, fornecendo subsídios para construção de indicadores, identificação de tendências e apoio à tomada de decisão.

A estrutura dos registros foi definida com base nos requisitos informacionais identificados durante a aplicação da metodologia 5W3H, permitindo que cada credencial seja acompanhada de informações relacionadas à sua origem, contexto de divulgação e momento de coleta. Como resultado, os registros produzidos não representam apenas combinações de login e senha, mas elementos contextualizados capazes de apoiar atividades de análise e produção de inteligência. A Tabela 3.2 apresenta os principais atributos armazenados para cada credencial identificada.

Tabela 3.2: Campos armazenados para cada credencial identificada

Campo	**Descrição**
usuário	Usuário ou e-mail identificado
senha	Senha associada ao registro
url	URL identificada no vazamento
dominio	Domínio extraído da URL
grupo	Grupo ou canal de origem
remetente	Usuário responsável pela publicação
data_publicacao	Data da mensagem original
data_coleta	Data da coleta pelo sistema
origem	Fonte do dado (Telegram)

3.3.3 Módulo de Indexação dos dados

Após a conclusão do processamento, os registros estruturados produzidos pela solução são encaminhados ao módulo de indexação. Essa etapa tem como objetivo transformar os dados extraídos das fontes monitoradas em uma base persistente de conhecimento, permitindo consultas, correlações e análises posteriores.

Para atender a esse propósito, foi utilizado o *Elasticsearch* como mecanismo de armazenamento e indexação dos registros produzidos. A escolha dessa tecnologia decorre de sua capacidade de processar grandes volumes de dados semiestruturados, realizar consultas em tempo real e suportar operações de agregação necessárias para exploração analítica das informações coletadas.

Cada credencial identificada durante o processamento é indexada como um documento independente. Assim, permite preservar a granularidade dos eventos observados e favorece a realização de consultas baseadas em diferentes atributos, como domínio, usuário, grupo de origem, remetente ou período de divulgação. Além disso, a indexação individual possibilita que múltiplas ocorrências relacionadas a um mesmo domínio ou credencial sejam correlacionadas ao longo do tempo.

O conjunto de documentos indexados constitui uma base de conhecimento sobre credenciais com-

prometidas observadas durante o monitoramento, permitindo consultas retrospectivas, análises históricas e correlação entre eventos identificados em diferentes períodos e fontes monitoradas."Dessa forma, o módulo de indexação atua como elemento intermediário entre o processamento e a análise, fornecendo a infraestrutura necessária para transformação dos registros produzidos em informações passíveis de exploração analítica e produção de inteligência.

3.3.4 Módulo de Análise

O módulo de análise constitui a etapa responsável por transformar os registros armazenados durante a indexação em informações passíveis de exploração analítica e apoio à tomada de decisão. Enquanto os módulos anteriores concentram-se na obtenção, tratamento e armazenamento dos dados, o módulo de análise tem como objetivo permitir a identificação de padrões, tendências e eventos relevantes associados às credenciais comprometidas observadas durante o monitoramento.

Para atender a esse propósito, os dados indexados são explorados por meio de consultas, agregações e mecanismos de visualização capazes de sintetizar grandes volumes de informações em representações mais compreensíveis para os analistas. Essa capacidade é particularmente importante em cenários envolvendo milhares de credenciais, nos quais a análise individual dos registros torna-se operacionalmente inviável.

A partir dos dados armazenados, torna-se possível identificar a frequência de exposição de determinados domínios, acompanhar a evolução temporal das ocorrências, observar a distribuição das credenciais entre diferentes fontes monitoradas e identificar recorrências associadas a usuários, grupos ou serviços específicos.

A camada de análise também possibilita a realização de consultas direcionadas a objetos específicos de interesse. Dessa forma, analistas podem investigar rapidamente credenciais associadas a um domínio, serviço ou período temporal específico, reduzindo o esforço necessário para localização e contextualização das informações relevantes.

Com o objetivo de apoiar essas atividades, a solução utiliza o *Kibana* como plataforma de exploração e visualização dos dados indexados. Os *dashboards* desenvolvidos permitem consolidar informações provenientes dos diferentes ciclos de monitoramento, oferecendo uma visão centralizada dos eventos observados e facilitando o acompanhamento contínuo dos ativos monitorados.

Além de apoiar atividades investigativas, o módulo de análise desempenha papel fundamental na construção da consciência situacional cibernética. Ao consolidar informações históricas, contextuais e quantitativas sobre as exposições identificadas, a solução permite que os responsáveis pelo monitoramento compreendam não apenas a existência de credenciais comprometidas, mas também sua frequência, persistência e evolução ao longo do tempo. Como resultado, os dados coletados passam a representar elementos capazes de subsidiar processos de avaliação de risco, priorização de ações e tomada de decisão.

3.3.5 Módulo de Alertas

Considerando que a identificação tempestiva de credenciais comprometidas é um dos principais objetivos da solução proposta, foi desenvolvido um mecanismo automatizado de geração de alertas destinado à

notificação de eventos relevantes observados durante o monitoramento.

O acionamento dos alertas ocorre durante o processamento das credenciais extraídas dos dados coletados. Sempre que uma credencial associada a um domínio previamente definido como objeto de interesse é identificada, o sistema produz uma notificação automática destinada aos responsáveis pelo monitoramento. Essa estratégia busca reduzir o intervalo entre a divulgação da credencial em fontes abertas e sua identificação pelos analistas responsáveis pela proteção dos ativos monitorados.

Os alertas gerados incluem informações suficientes para apoiar uma avaliação inicial do evento identificado, tais como o domínio monitorado, a quantidade de credenciais encontradas, o endereço de e-mail identificado, a URL associada ao registro, o grupo ou canal de origem da divulgação e o identificador da mensagem utilizada como fonte da informação. Esses elementos permitem que os analistas localizem rapidamente as evidências correspondentes e iniciem procedimentos de verificação e resposta.

Como medida para reduzir a exposição de informações sensíveis, as notificações não incluem as senhas comprometidas nem a totalidade dos atributos armazenados no repositório de dados. O acesso às informações completas permanece restrito ao ambiente analítico implementado no Kibana, onde os registros podem ser consultados por usuários autorizados. Essa estratégia busca equilibrar a agilidade na disseminação da inteligência com a preservação da confidencialidade das informações coletadas.

Embora o mecanismo implementado não realize classificação automática de criticidade ou avaliação de impacto, os alertas fornecem evidências suficientes para apoiar a análise humana e subsidiar processos de resposta. Dessa forma, a responsabilidade pela interpretação da relevância da ocorrência e pela definição das medidas corretivas permanece sob responsabilidade dos analistas encarregados do monitoramento.

Sob a perspectiva da Inteligência de Ameaças Cibernéticas, o sistema de alertas representa o mecanismo de disseminação imediata da inteligência produzida durante o monitoramento. Ao comunicar rapidamente a identificação de credenciais potencialmente associadas aos ativos monitorados, a solução contribui para reduzir o tempo necessário para detecção da exposição e apoiar a adoção de medidas preventivas ou corretivas pelos responsáveis pela segurança da organização.

4 IMPLEMENTAÇÃO E RESULTADOS DA PROVA DE CONCEITO

Este capítulo apresenta a implementação da prova de conceito desenvolvida para validar a metodologia proposta nesta pesquisa, bem como os resultados obtidos durante sua execução. Diferentemente dos capítulos anteriores, dedicados à fundamentação teórica e à descrição da arquitetura conceitual, esta etapa tem como objetivo demonstrar a viabilidade técnica da solução desenvolvida e analisar sua capacidade de transformar informações obtidas em fontes abertas em produtos de Inteligência de Ameaças Cibernéticas.

Inicialmente, são descritos o ambiente experimental e os principais componentes utilizados na implementação da arquitetura proposta, incluindo os módulos responsáveis pela coleta, processamento, indexação, análise e disseminação das informações. Em seguida, são apresentados os resultados obtidos durante a execução contínua da prova de conceito, contemplando a validação da metodologia, a análise dos dados produzidos e uma discussão sobre as contribuições da solução para atividades de monitoramento de credenciais comprometidas.

É importante destacar que a implementação desenvolvida não teve como objetivo produzir uma plataforma comercial de monitoramento, mas validar a aplicabilidade da metodologia proposta em um ambiente controlado. Dessa forma, os resultados apresentados devem ser interpretados como evidências da viabilidade técnica da arquitetura desenvolvida e de sua capacidade de apoiar atividades de Cyber Threat Intelligence por meio da integração entre coleta automatizada, contextualização das informações, preservação de metadados, exploração analítica e disseminação da inteligência produzida.

Nota: Todas as capturas de tela apresentadas nesta seção foram parcialmente descaracterizadas para preservar a confidencialidade das informações coletadas durante a prova de conceito. Foram ocultados endereços eletrônicos, credenciais, URLs e outros dados potencialmente sensíveis, mantendo-se apenas os elementos necessários para demonstrar o funcionamento da arquitetura e validar os resultados obtidos.

4.1 AMBIENTE EXPERIMENTAL

A validação da metodologia proposta foi realizada por meio de uma Prova de Conceito (PoC) implementada em um ambiente experimental desenvolvido para automatizar o monitoramento de credenciais expostas divulgadas em canais e grupos públicos do Telegram. O ambiente foi concebido para reproduzir as etapas do fluxo de produção de Inteligência de Ameaças Cibernéticas descrito no Capítulo 3, contemplando os processos de coleta, processamento, indexação, análise e disseminação das informações produzidas ao longo do monitoramento.

A arquitetura da solução foi implementada de forma modular, permitindo que cada componente executasse uma função específica no fluxo de processamento. Essa organização reduz o acoplamento entre os módulos, facilita a manutenção da solução e possibilita sua evolução incremental, uma vez que alterações

em um componente podem ser realizadas com menor impacto sobre as demais etapas da arquitetura. Durante a execução da Prova de Conceito, os módulos foram acionados de forma sequencial, constituindo um fluxo contínuo de processamento iniciado pela coleta automatizada dos dados e finalizado pela análise das informações e pela geração de alertas destinados aos responsáveis pelos domínios monitorados.

A implementação foi desenvolvida utilizando a linguagem de programação *Python*, em virtude de sua ampla utilização em aplicações de automação, análise de dados e segurança da informação, além da disponibilidade de bibliotecas para integração com plataformas de mensageria, processamento de dados e sistemas de armazenamento. A comunicação com o Telegram foi realizada por meio da biblioteca *Telethon*, utilizada como cliente para acesso programático à API da plataforma e obtenção das mensagens, arquivos e metadados das fontes monitoradas.

Como repositório central das informações, foi utilizado o *Elasticsearch* versão 8.15.3, responsável pela indexação e persistência dos documentos produzidos pelo *pipeline*. A infraestrutura de indexação foi composta por um cluster Elasticsearch com três nós, executado em ambiente Linux. O acesso ao serviço foi realizado por meio da interface HTTP disponibilizada pelo Elasticsearch, utilizando a porta padrão 9200/TCP. A utilização de múltiplos nós permitiu distribuir os componentes responsáveis pelo armazenamento e disponibilização dos dados utilizados durante a Prova de Conceito.

Para exploração analítica dos registros, foi empregado o *Kibana*, integrado ao Elasticsearch e disponibilizado por meio de sua porta padrão 5601/TCP. A ferramenta foi utilizada para realização de consultas, aplicação de filtros, agregações e construção de painéis para visualização dos dados produzidos durante o monitoramento. O mecanismo de disseminação da inteligência também foi implementado em *Python*, permitindo o envio automatizado de notificações relacionadas às novas ocorrências identificadas para os domínios monitorados.

Durante a validação experimental, o módulo de coleta foi configurado para executar ciclos automáticos a cada seis horas, recuperando as novas mensagens disponibilizadas desde a execução anterior. Os dados coletados eram encaminhados aos módulos subsequentes de processamento, indexação, análise e disseminação, estabelecendo um *pipeline* periódico e incremental de produção de inteligência capaz de acompanhar a evolução das informações disponibilizadas nas fontes monitoradas.

A Tabela 4.1 apresenta um resumo das principais tecnologias empregadas na implementação da Prova de Conceito.

Tabela 4.1: Tecnologias utilizadas na implementação da Prova de Conceito.

Componente	**Tecnologia utilizada**
Linguagem de programação	Python 3.11
Coleta de dados	Telethon (cliente Python para a API do Telegram)
Armazenamento e indexação	Elasticsearch 8.15.3 – cluster com três nós
Interface do Elasticsearch	HTTP – porta padrão 9200/TCP
Visualização e análise	Kibana 8.15.3
Interface do Kibana	HTTP – porta padrão 5601/TCP
Sistema de notificações	Python + SMTP OAuth2

Além das tecnologias empregadas, a caracterização do ambiente de execução é importante para contextualizar as condições sob as quais a Prova de Conceito foi desenvolvida. A infraestrutura utilizada contem-

plou ambiente baseado em Linux e um cluster Elasticsearch composto por três nós para armazenamento e indexação das informações produzidas pelo *pipeline*. A Tabela 4.2 apresenta os principais parâmetros conhecidos do ambiente utilizado durante os experimentos.

Tabela 4.2: Infraestrutura utilizada durante a execução da Prova de Conceito.

Parâmetro	**Configuração**
Sistema operacional	Ubuntu Server 24.04.4 LTS
Arquitetura do sistema	x86_64
Memória RAM	16 GB
Ambiente de execução	Máquina virtual em ambiente Linux
Infraestrutura de indexação	Cluster Elasticsearch composto por três nós
Elasticsearch	Versão 8.15.3 – porta padrão 9200/TCP
Kibana	Interface Web – porta padrão 5601/TCP
Versão do Python	3.11
Fontes monitoradas	Dois canais/grupos públicos do Telegram
Domínios monitorados	239 domínios de interesse

Conforme apresentado nas Tabelas 4.1 e 4.2, a Prova de Conceito foi desenvolvida utilizando tecnologias empregadas em ambientes de processamento, armazenamento e análise de dados aplicados à Inteligência de Ameaças Cibernéticas. A utilização de uma arquitetura modular, associada a um cluster Elasticsearch composto por três nós, permitiu integrar as diferentes etapas da solução e disponibilizar os dados processados para consulta e análise por meio do Kibana. Embora a implementação tenha sido realizada em escala experimental, o ambiente permitiu validar a execução integrada das etapas de coleta, processamento, indexação, análise e disseminação previstas na arquitetura proposta.

4.2 IMPLEMENTAÇÃO DA ARQUITETURA

A implementação foi organizada de forma modular, refletindo a estrutura apresentada no Capítulo 3. Cada módulo desempenha uma função específica no ciclo operacional da arquitetura, abrangendo desde a coleta automatizada das informações nas fontes monitoradas até a disseminação da inteligência produzida aos responsáveis pelos domínios monitorados. Essa organização facilita a compreensão do funcionamento da solução, bem como sua manutenção e evolução para atender a novos requisitos ou incorporar outras fontes de dados.

A seguir, são detalhadas as principais decisões de implementação adotadas em cada módulo, descrevendo os componentes utilizados, o fluxo de processamento das informações e a integração entre as diferentes etapas da arquitetura. Ao final do capítulo, são apresentados os resultados obtidos durante a Prova de Conceito, permitindo avaliar o comportamento da solução em um cenário de monitoramento contínuo de credenciais expostas.

4.2.1 Implementação Módulo de Coleta

O módulo de coleta constitui o ponto de entrada da arquitetura proposta, sendo responsável pela obtenção automatizada dos dados provenientes das fontes monitoradas. Sua principal função consiste em recuperar continuamente mensagens e arquivos publicados em grupos públicos do Telegram, preservando não apenas o conteúdo coletado, mas também os metadados necessários para contextualização das informações ao longo das etapas subsequentes da pipeline. Em arquiteturas de *Cyber Threat Intelligence*, essa etapa é fundamental, pois a qualidade das análises produzidas depende diretamente da integridade e da rastreabilidade das informações obtidas durante a coleta.

A implementação do módulo foi realizada utilizando a biblioteca *Telethon*, que fornece uma interface programática para comunicação com a API oficial do Telegram. A autenticação foi realizada por meio de uma conta dedicada (*avatar digital*), criada exclusivamente para execução da pesquisa, permitindo o acesso aos grupos públicos previamente selecionados para monitoramento. Essa estratégia reduz a exposição da identidade do pesquisador durante a coleta e facilita o gerenciamento da atividade de monitoramento ao longo da execução da prova de conceito.

O processo de coleta foi configurado para execução automática em intervalos de seis horas, recuperando apenas as mensagens publicadas desde o último ciclo de execução. Essa estratégia reduz o volume de dados processados em cada iteração, evita a coleta repetida de informações previamente analisadas e mantém a base de dados continuamente atualizada com novos conteúdos disponibilizados nas fontes monitoradas.

Além das mensagens textuais, o módulo também realiza a identificação e o download automático dos arquivos compartilhados nos grupos monitorados. Foram considerados arquivos nos formatos `TXT`, `CSV`, `XML`, `ZIP` e `RAR`, uma vez que esses formatos são frequentemente utilizados para disponibilização de listas contendo credenciais comprometidas. Durante o processo de download, o sistema verifica automaticamente se os arquivos compactados possuem proteção por senha. Quando essa situação é identificada, são realizadas tentativas de abertura utilizando as senhas explicitamente divulgadas nas mensagens do próprio grupo, permitindo recuperar conteúdos que normalmente permaneceriam inacessíveis durante uma coleta convencional.

Além do conteúdo das mensagens e dos arquivos obtidos, o módulo preserva um conjunto de metadados utilizados nas etapas posteriores de processamento e análise. Entre os principais atributos armazenados destacam-se a identificação do grupo monitorado, o identificador da mensagem, o link para a publicação original, a identificação do usuário responsável pela postagem, a data e horário da publicação, o nome e o tipo do arquivo compartilhado, bem como informações relacionadas à existência de senha para acesso ao conteúdo. A preservação desses metadados permite manter a rastreabilidade das evidências coletadas e ampliar o contexto disponível para análise de inteligência.

A Figura 4.1 apresenta o fluxo de execução do módulo de coleta implementado nesta pesquisa.

Conforme ilustrado na Figura 4.1, o processo inicia com a autenticação do avatar digital na plataforma Telegram e a verificação dos grupos monitorados. Em seguida, são recuperadas apenas as mensagens publicadas desde a última execução da rotina, reduzindo o processamento de dados redundantes. Para cada mensagem identificada, o sistema verifica a existência de arquivos anexos e realiza automaticamente seu

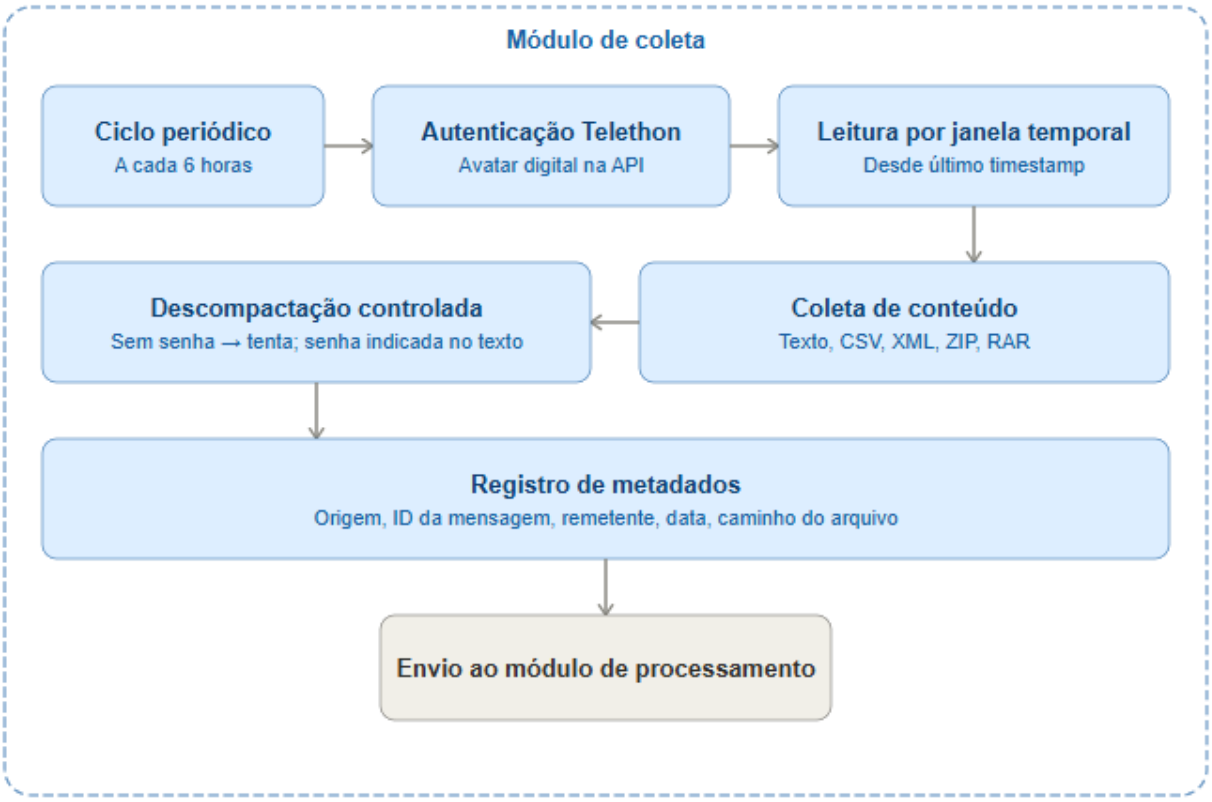


Figura 4.1: Fluxo de execução do módulo de coleta. proposta nesta pesquisa.
Fonte: Elaboração própria.

download. Caso o arquivo esteja protegido por senha, são executadas tentativas de extração utilizando as senhas disponibilizadas nas próprias mensagens do grupo. Por fim, o conteúdo coletado e todos os metadados associados são encaminhados ao módulo de processamento, responsável pela extração e estruturação das credenciais comprometidas.

A implementação desse módulo permitiu automatizar integralmente a aquisição das informações provenientes do Telegram, reduzindo a necessidade de intervenção manual durante o monitoramento e garantindo a preservação dos elementos necessários para contextualização das evidências coletadas. Dessa forma, a etapa de coleta fornece os insumos que sustentam todas as fases subsequentes da arquitetura proposta, contribuindo para a produção contínua de Inteligência de Ameaças Cibernéticas.

4.2.2 Implementação do Módulo de Processamento

Após a conclusão da etapa de coleta, os dados obtidos são encaminhados ao módulo de processamento, responsável por identificar, extrair, estruturar e enriquecer as informações de interesse presentes nas mensagens e arquivos recuperados. Enquanto o módulo de coleta concentra-se na aquisição das evidências, esta etapa transforma dados originalmente não estruturados em registros organizados, aptos para armazenamento, consulta e análise nas etapas subsequentes da arquitetura.

Em seguida, o conteúdo textual é normalizado para reduzir inconsistências relacionadas à codificação de caracteres, caracteres especiais e diferenças de formatação. Esse procedimento estabelece um formato

uniforme para os dados antes da aplicação dos mecanismos de identificação das credenciais, reduzindo falhas decorrentes da heterogeneidade dos arquivos compartilhados nos grupos monitorados.

A identificação das credenciais foi implementada por meio de um conjunto de expressões regulares desenvolvidas para reconhecer diferentes padrões de divulgação observados durante a fase exploratória da pesquisa. Diferentemente de soluções que consideram apenas o formato convencional *usuário:senha*, o mecanismo implementado contempla múltiplas estruturas de apresentação das credenciais, incluindo combinações contendo endereço eletrônico, nome de usuário, senha, URL, protocolo de acesso e diferentes separadores entre os campos.

A Tabela 4.3 apresenta os principais padrões reconhecidos pelo mecanismo de processamento.

Tabela 4.3: Principais padrões de credenciais identificados durante o processamento.

Padrão	**Exemplo**
Usuário : Senha	usuario:senha
E-mail : Senha	usuario@email.com:senha
URL : Usuário : Senha	https://site.com:usuario:senha
Usuário : Senha : URL	usuario:senha:https://site.com
Protocolo + URL + Credenciais	android://usuario@com.google.android.gm:senha
Campos separados por "|"	usuario|senha|url
Campos separados por ","	usuario,senha,url

Conforme apresentado na Tabela 4.3, o mecanismo de processamento foi desenvolvido para suportar diferentes formatos de divulgação das credenciais comprometidas, refletindo a heterogeneidade observada nas informações compartilhadas em grupos do Telegram. Essa flexibilidade aumenta a capacidade de recuperação das evidências e reduz perdas decorrentes de variações na forma de publicação dos dados.

Após a identificação das credenciais, cada ocorrência é convertida em um documento independente no formato JSON. Durante essa etapa são associados tanto os atributos extraídos das credenciais quanto os metadados preservados pelo módulo de coleta. Cada documento passa a conter informações como domínio identificado, URL, login, senha, protocolo de acesso, data e horário da publicação, grupo monitorado, usuário responsável pela postagem, identificador da mensagem, arquivo de origem e demais informações necessárias para rastreabilidade da evidência.

Além da extração das credenciais, o módulo realiza a filtragem dos registros de acordo com a lista de domínios monitorados definida para a pesquisa. Essa lista contempla domínios pertencentes aos órgãos participantes da prova de conceito, permitindo direcionar o processamento para informações relevantes ao contexto analisado e reduzindo o armazenamento de registros sem interesse para os objetivos da pesquisa.

A Figura 4.2 apresenta o fluxo de execução implementado para o módulo de processamento.

Conforme ilustrado na Figura 4.2, o processamento é iniciado pela leitura dos arquivos coletados, seguida da normalização dos dados, identificação das credenciais por meio das expressões regulares, associação dos metadados provenientes da coleta e geração dos documentos estruturados em formato JSON. Esses documentos constituem a unidade básica de informação utilizada nas etapas de indexação, análise e disseminação da inteligência.

A implementação desse módulo permitiu transformar dados heterogêneos, distribuídos em diferentes

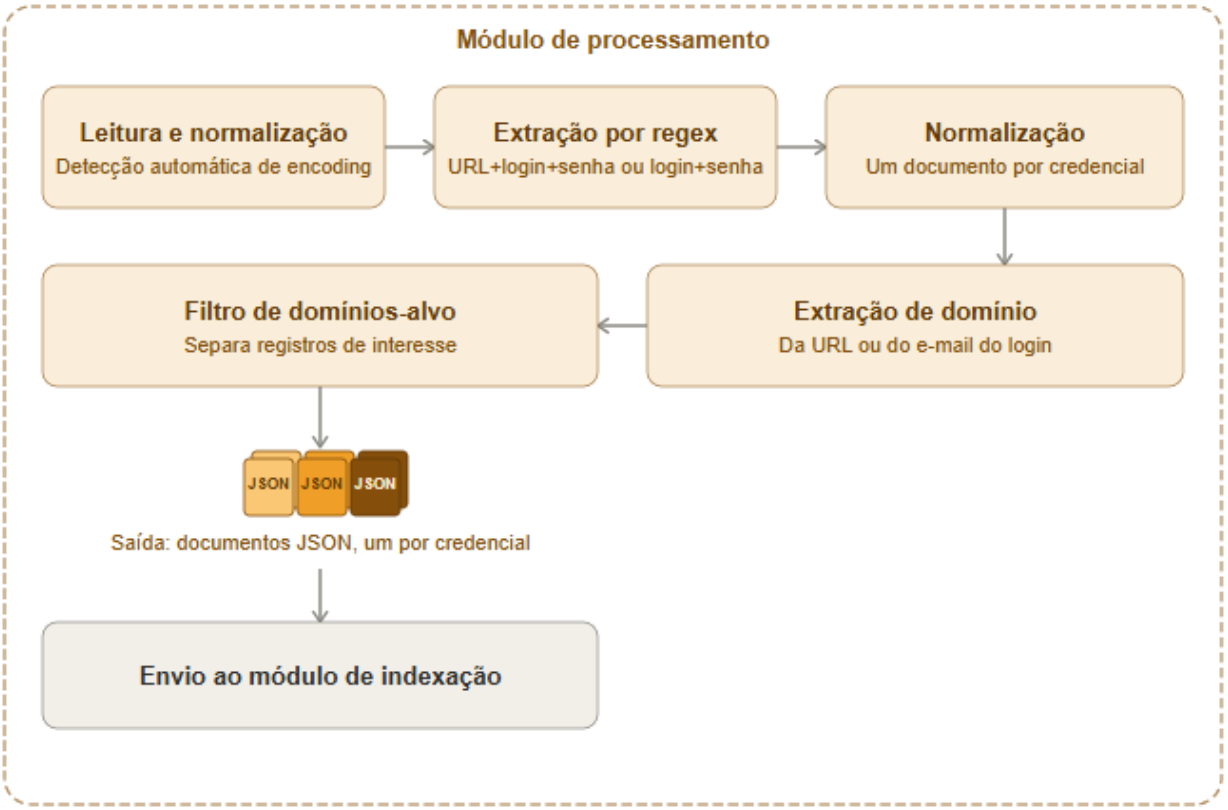


Figura 4.2: Fluxo de execução do módulo de processamento proposta nesta pesquisa.
Fonte: Elaboração própria.

formatos de arquivos e estruturas de publicação, em informações estruturadas e padronizadas. Como resultado, as credenciais comprometidas passaram a ser representadas por documentos enriquecidos com contexto e rastreabilidade, fornecendo uma base consistente para as atividades de análise e produção de Inteligência de Ameaças Cibernéticas realizadas pelos módulos subsequentes da arquitetura.

Diferentemente de bases estruturadas produzidas especificamente para compartilhamento automatizado, os conteúdos observados em ambientes monitorados frequentemente apresentam inconsistências de formatação, múltiplos esquemas de codificação, ausência de padronização e diferentes formas de representação dos pares usuário-senha. Como consequência, a simples coleta dos arquivos não é suficiente para viabilizar atividades de monitoramento ou análise. Torna-se necessário um processo intermediário capaz de converter essas informações em registros estruturados e passíveis de correlação.

Nesse contexto, a etapa de leitura e normalização busca reduzir problemas relacionados à diversidade de formatos observados. A utilização de mecanismos automáticos de detecção de codificação textual permite tratar arquivos produzidos em diferentes ambientes, minimizando perdas de informação decorrentes de incompatibilidades de *encoding*. Em seguida, são aplicadas expressões regulares desenvolvidas para identificar padrões recorrentes de representação de credenciais, contemplando tanto registros compostos por URL, login e senha quanto estruturas contendo apenas identificadores de usuário e respectivas senhas.

Após a identificação das credenciais, cada ocorrência é convertida em um documento independente. Essa decisão arquitetural possui papel relevante na proposta, pois permite que cada credencial seja tratada como uma unidade individual de análise. Dessa forma, consultas, correlações, agregações e mecanismos

de alerta podem atuar diretamente sobre eventos específicos, sem necessidade de reprocessar os arquivos originais.

A extração do domínio associado a cada credencial constitui uma etapa adicional de contextualização. Ao relacionar as credenciais identificadas aos domínios monitorados, a solução reduz significativamente o volume de dados que necessitam de análise manual, direcionando a atenção dos analistas para registros potencialmente associados aos ativos de interesse. Como resultado, o módulo de processamento atua como elemento de transição entre a coleta de dados brutos e a produção de inteligência, convertendo informações dispersas em registros estruturados e contextualizados.

4.2.3 Implementação do Módulo de Indexação

Após a extração e estruturação das credenciais comprometidas, os documentos produzidos pelo módulo de processamento são encaminhados ao módulo de indexação, responsável pelo armazenamento persistente das informações e sua disponibilização para consulta pelas etapas de análise e disseminação da inteligência. Essa etapa desempenha papel fundamental na arquitetura proposta, pois estabelece um repositório central capaz de organizar grandes volumes de registros e permitir sua recuperação de forma eficiente.

A indexação foi implementada utilizando o *Elasticsearch* versão 8.15.3, escolhido por oferecer mecanismos de indexação e consulta otimizados para documentos semiestruturados. Diferentemente dos bancos de dados relacionais, o Elasticsearch permite armazenar documentos contendo diferentes atributos sem a necessidade de esquemas rígidos, característica particularmente adequada ao contexto desta pesquisa, no qual as credenciais comprometidas apresentam diferentes estruturas e quantidades de informações associadas.

Cada credencial identificada durante o processamento é convertida em um documento independente e armazenada individualmente no índice da aplicação. Essa estratégia permite que cada ocorrência seja consultada, correlacionada e analisada de forma isolada ou em conjunto com outros registros, ampliando as possibilidades de exploração analítica dos dados produzidos durante o monitoramento.

Além dos atributos extraídos das credenciais, cada documento preserva os metadados obtidos durante a coleta e o processamento, incluindo informações como domínio identificado, URL associada, login, senha, protocolo de acesso, data e horário da publicação, grupo monitorado, identificador da mensagem, usuário responsável pela postagem, arquivo de origem e data de coleta. A manutenção dessas informações permite preservar a rastreabilidade das evidências e possibilita análises que vão além da simples identificação de credenciais comprometidas.

A Tabela 4.4 apresenta os principais atributos armazenados para cada documento indexado.

Conforme apresentado na Tabela 4.4, a estrutura de indexação foi projetada para armazenar não apenas os elementos que compõem a credencial comprometida, mas também os metadados necessários para sua contextualização. Essa organização permite realizar consultas utilizando diferentes critérios, como domínio, período de coleta, grupo monitorado, arquivo de origem ou usuário responsável pela publicação, ampliando significativamente o potencial analítico da solução.

A comunicação entre o módulo de processamento e o Elasticsearch foi implementada utilizando a

Tabela 4.4: Principais campos armazenados para cada documento indexado.

Campo	Descrição
login	Nome de usuário ou endereço eletrônico identificado.
senha	Senha associada à credencial comprometida.
url	Endereço associado à credencial, quando disponível.
dominio	Domínio extraído da URL ou do endereço eletrônico.
grupo	Grupo ou canal do Telegram onde a informação foi publicada.
remetente	Identificador do usuário responsável pela publicação.
id_mensagem	Identificador único da mensagem no Telegram.
arquivo_origem	Arquivo no qual a credencial foi encontrada.
data_utc	Data e horário da publicação em UTC.
data_coleta	Data e horário da execução da coleta.

biblioteca oficial disponibilizada para a linguagem Python. Após a geração dos documentos em formato JSON, cada registro é enviado automaticamente ao índice da aplicação, onde passa a integrar a base de dados utilizada pelos módulos subsequentes. Durante esse processo, os documentos são indexados de forma incremental, preservando o histórico das credenciais identificadas ao longo da execução da prova de conceito.

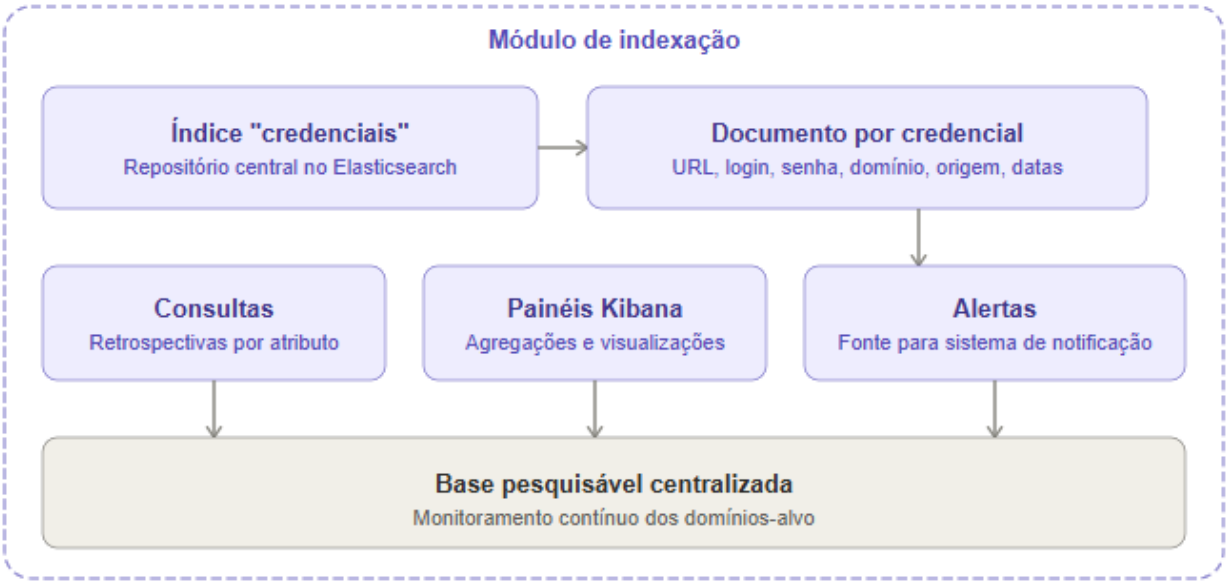


Figura 4.3: Fluxo de execução do módulo de indexação proposta nesta pesquisa.
Fonte: Elaboração própria.

Conforme ilustrado na Figura 4.3, os documentos estruturados produzidos pelo módulo de processamento são recebidos pelo indexador, convertidos para o formato esperado pelo Elasticsearch e armazenados no índice da aplicação. A partir desse momento, as informações tornam-se imediatamente disponíveis para consultas, construção de visualizações, correlações e geração de alertas, caracterizando a indexação como o elemento integrador entre o processamento dos dados e a produção de inteligência.

A implementação desse módulo permitiu centralizar todas as informações produzidas pela arquitetura em um único repositório, preservando a integridade dos registros e oferecendo mecanismos eficientes para

recuperação e exploração analítica dos dados. Como consequência, as etapas posteriores deixam de depender do processamento direto dos arquivos coletados e passam a operar sobre um conjunto estruturado de documentos, favorecendo consultas rápidas, correlação de informações e produção contínua de Inteligência de Ameaças Cibernéticas.

4.2.4 Implementação do Módulo de Análise

Concluída a etapa de indexação, os documentos produzidos pela arquitetura passam a compor uma base estruturada de informações que pode ser explorada pelo módulo de análise. Diferentemente das etapas anteriores, cujo objetivo consiste na obtenção, processamento e organização dos dados coletados, esta etapa concentra-se na produção de conhecimento a partir das informações armazenadas, permitindo identificar padrões, acompanhar tendências temporais, correlacionar evidências e apoiar o processo de tomada de decisão.

Para essa finalidade, foi utilizada a plataforma *Kibana*, integrada ao *Elasticsearch*, possibilitando consultas diretamente sobre os documentos indexados sem necessidade de novo processamento dos arquivos coletados. Essa integração permite que as informações produzidas ao longo da arquitetura sejam exploradas de maneira dinâmica, preservando tanto as credenciais identificadas quanto os metadados associados a cada evidência.

Com o objetivo de apoiar as atividades de monitoramento e investigação, foi desenvolvido um painel analítico que reúne, em uma única interface, as principais informações produzidas durante a execução da prova de conceito. O painel foi concebido para permitir que o analista visualize simultaneamente indicadores quantitativos, consultas detalhadas e gráficos temporais, reduzindo o tempo necessário para obtenção de informações relevantes durante uma investigação.

A Figura 4.4 apresenta a interface principal desenvolvida para exploração das credenciais comprometidas identificadas durante a pesquisa.

Conforme observado na Figura 4.4, o painel principal reúne diferentes componentes destinados à exploração das informações armazenadas. A interface integra consultas às credenciais indexadas, indicadores quantitativos e visualizações gráficas que permitem acompanhar a evolução das ocorrências ao longo do tempo. Essa organização permite que o analista obtenha rapidamente uma visão geral do ambiente monitorado, identificando tanto o volume de informações disponíveis quanto possíveis alterações no comportamento das fontes monitoradas.

Entretanto, atividades de *Cyber Threat Intelligence* normalmente exigem investigações direcionadas, nas quais apenas parte das informações armazenadas é relevante para responder a um determinado requisito de inteligência. Considerando essa necessidade, foram implementados mecanismos de filtragem capazes de restringir dinamicamente os resultados apresentados pelo painel utilizando diferentes atributos preservados durante as etapas anteriores da arquitetura. A Figura 4.5 apresenta os mecanismos de filtragem incorporados ao painel analítico.

Os filtros destacados na Figura 4.5 podem ser utilizados individualmente ou de forma combinada, permitindo ao analista restringir progressivamente o conjunto de registros recuperados. Essa funcionali-

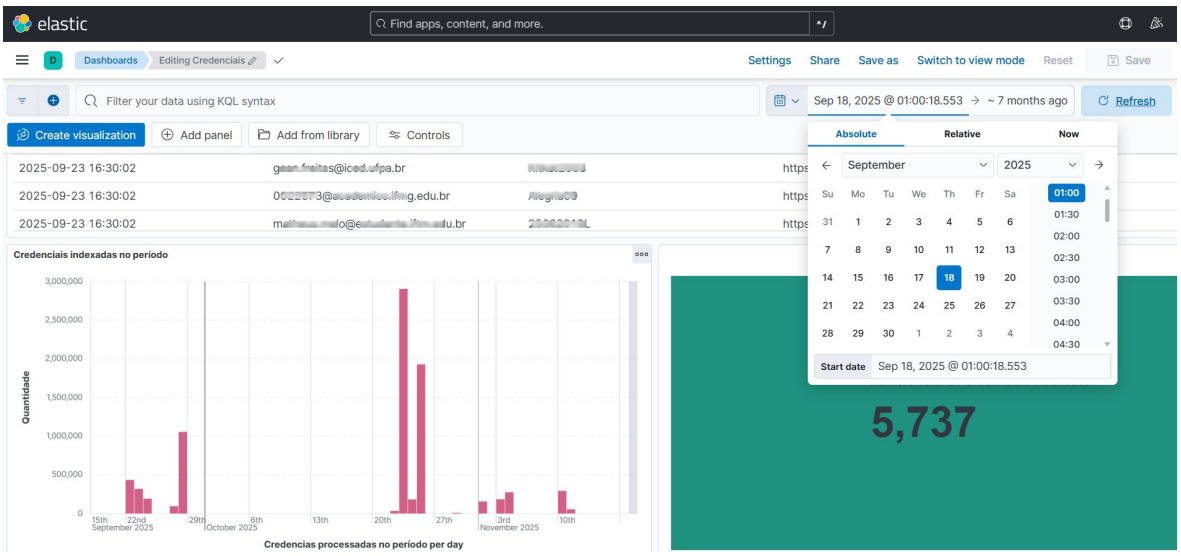


Figura 4.4: Painel principal desenvolvido para exploração das credenciais comprometidas. Os dados apresentados foram descaracterizados para preservar a confidencialidade das informações coletadas.
Fonte: Elaboração própria.

dade possibilita localizar rapidamente credenciais pertencentes a um usuário específico, analisar apenas mensagens provenientes de determinado grupo do Telegram ou concentrar a investigação em um intervalo temporal de interesse. Como consequência, a arquitetura deixa de atuar apenas como um repositório de dados e passa a oferecer mecanismos capazes de apoiar atividades de investigação e correlação de eventos.

Além das consultas direcionadas, o módulo disponibiliza recursos para análise agregada das informações coletadas. Entre esses recursos destaca-se a visualização da distribuição temporal das credenciais identificadas durante o monitoramento, permitindo acompanhar a evolução das ocorrências ao longo do período analisado. A Figura 4.6 apresenta a distribuição temporal das credenciais indexadas durante a execução da prova de conceito.

Observa-se, na Figura 4.6, que a quantidade de credenciais identificadas variou ao longo do período monitorado, evidenciando momentos de maior concentração de publicações nas fontes acompanhadas. Esse tipo de visualização permite identificar períodos com comportamento atípico, acompanhar tendências e direcionar investigações para intervalos específicos, contribuindo para a identificação de possíveis campanhas de divulgação de credenciais comprometidas.

Embora a distribuição temporal seja importante para compreender o comportamento das fontes monitoradas, a caracterização do ambiente também depende de indicadores quantitativos que sintetizem o volume de informações processadas pela arquitetura. Para essa finalidade foi implementado um indicador responsável por apresentar, em tempo real, a quantidade total de credenciais indexadas durante a execução da prova de conceito.A Figura 4.7 apresenta o indicador desenvolvido para esse propósito.

Durante o período de monitoramento foram indexadas 9.947 credenciais pertencentes aos domínios monitorados, resultado que evidencia a capacidade da arquitetura em processar continuamente grandes volumes de informações provenientes de fontes abertas. Entretanto, a simples contabilização das credenciais não é suficiente para apoiar atividades de Inteligência de Ameaças Cibernéticas. É necessário preservar o contexto em que cada evidência foi identificada, permitindo sua posterior investigação.



Figura 4.5: Mecanismos de filtragem implementados no painel analítico. (1) filtro por endereço de e-mail; (2) filtro por nome de usuário; (3) filtro por grupo monitorado; (4) filtro temporal.
Fonte: Elaboração própria.

Com esse objetivo, cada documento armazenado no Elasticsearch mantém não apenas os atributos associados à credencial comprometida, mas também informações relacionadas à sua origem, incluindo data da publicação, URL identificada, identificador da mensagem, grupo monitorado e demais metadados produzidos durante o processamento.

A Figura 4.8 apresenta um exemplo da estrutura disponibilizada ao analista para exploração dessas informações.

Conforme ilustrado na Figura 4.8, cada registro preserva informações suficientes para reconstrução do contexto em que a credencial foi identificada. Além do endereço eletrônico e da senha comprometida, permanecem disponíveis informações referentes à data da publicação, URL associada ao serviço comprometido e identificador da mensagem original. A preservação desses atributos amplia significativamente o potencial analítico da arquitetura, permitindo rastrear a origem das evidências, correlacionar diferentes ocorrências e reproduzir o contexto completo de cada registro durante atividades de investigação. As principais funcionalidades disponibilizadas pelo módulo de análise são resumidas na Tabela 4.5.

Conforme apresentado na Tabela 4.5, o módulo de análise vai além da simples visualização das credenciais comprometidas. A integração entre mecanismos de consulta, filtros, indicadores quantitativos, visualizações temporais e preservação de metadados permite transformar os documentos armazenados em informações contextualizadas, apoiando atividades de monitoramento, investigação e produção de Inteligência de Ameaças Cibernéticas. Dessa forma, o módulo consolida as informações produzidas nas etapas anteriores da arquitetura e fornece ao analista os recursos necessários para explorar, correlacionar e interpretar as evidências obtidas durante o monitoramento das fontes abertas.

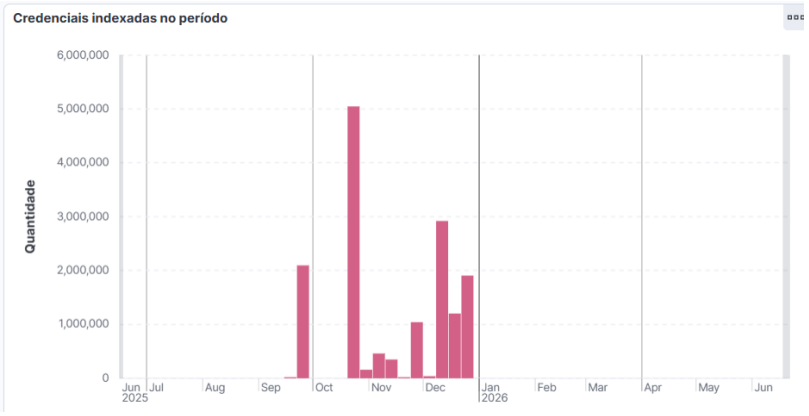


Figura 4.6: Distribuição temporal das credenciais indexadas durante a execução da prova de conceito.
Fonte: Elaboração própria.



Figura 4.7: Indicador contendo o número total de credenciais indexadas durante a execução da prova de conceito.
Fonte: Elaboração própria.

4.2.5 Implementação do Módulo de Alertas

A etapa final da arquitetura corresponde ao módulo de disseminação da inteligência, responsável por transformar as informações produzidas durante as etapas anteriores em notificações direcionadas aos responsáveis pelos domínios monitorados. No contexto desta pesquisa, a disseminação representa a entrega do produto de Inteligência de Ameaças Cibernéticas aos consumidores da informação, permitindo reduzir o intervalo entre a identificação de uma credencial comprometida e a adoção de medidas de resposta.

Conforme ilustrado na Figura 4.9, o processo inicia com a consulta ao índice de credenciais utilizando uma janela temporal configurável. Em seguida, os registros recuperados são agrupados por domínio e organizado para cada organização monitorada. Por fim, as notificações são enviadas automaticamente aos destinatários cadastrados, encerrando o ciclo operacional da arquitetura proposta.

O módulo foi implementado em Python e executado periodicamente após a conclusão do processo

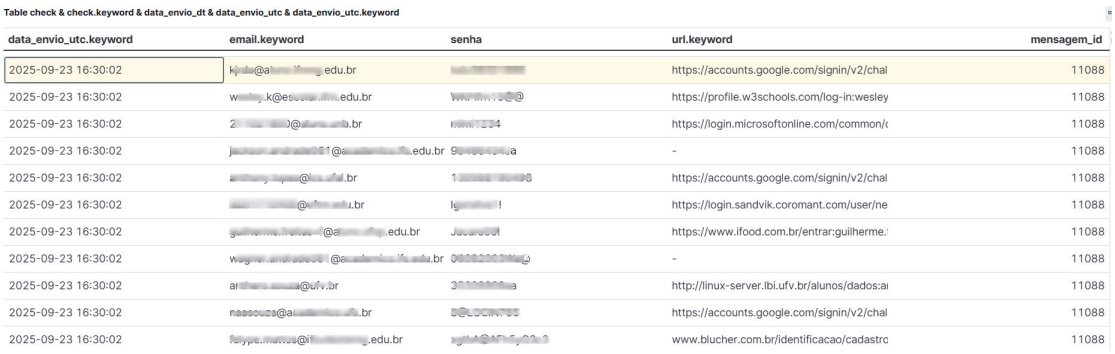


Table check & check.keyword & data_envio_dt & data_envio_utc & data_envio_utc.keyword

data_envio_utc.keyword	email.keyword	senha	url.keyword	mensagem_id
2025-09-23 16:30:02	[redacted]	[redacted]	https://accounts.google.com/signin/v2/chal	11088
2025-09-23 16:30:02	[redacted]	[redacted]	https://profile.w3schools.com/log-in:wesley	11088
2025-09-23 16:30:02	[redacted]	[redacted]	https://login.microsoftonline.com/common/(	11088
2025-09-23 16:30:02	[redacted]	[redacted]	-	11088
2025-09-23 16:30:02	[redacted]	[redacted]	https://accounts.google.com/signin/v2/chal	11088
2025-09-23 16:30:02	[redacted]	[redacted]	https://login.sandvik.coromant.com/user/ne	11088
2025-09-23 16:30:02	[redacted]	[redacted]	https://www.ifood.com.br/entrar:guilherme.:	11088
2025-09-23 16:30:02	[redacted]	[redacted]	-	11088
2025-09-23 16:30:02	[redacted]	[redacted]	http://linux-server.lbi.ufv.br/alunos/dados:a	11088
2025-09-23 16:30:02	[redacted]	[redacted]	https://accounts.google.com/signin/v2/chal	11088
2025-09-23 16:30:02	[redacted]	[redacted]	www.blucher.com.br/identificacao/cadastro	11088

Figura 4.8: Consulta detalhada das credenciais indexadas e respectivos metadados.
Fonte: Elaboração própria.

Tabela 4.5: Principais análises disponibilizadas pelo módulo de análise.

Análise	**Objetivo**
Consulta de credenciais	Localizar registros específicos utilizando qualquer atributo indexado.
Distribuição temporal	Acompanhar a evolução das ocorrências ao longo do período monitorado.
Credenciais por domínio	Identificar organizações com maior número de credenciais expostas.
Credenciais por grupo	Verificar quais grupos apresentam maior volume de publicações.
Filtros por período	Restringir as análises a intervalos específicos de tempo.
Consulta por arquivo	Identificar a origem de cada credencial processada.
Rastreabilidade	Recuperar os metadados associados a cada evidência coletada.

de indexação. A rotina consulta o índice armazenado no Elasticsearch utilizando uma janela temporal configurável, recuperando apenas as credenciais identificadas desde a última execução do sistema. Essa estratégia evita o envio repetitivo das mesmas ocorrências e garante que apenas novas evidências sejam consideradas durante a geração dos alertas.

Após a recuperação dos documentos, os registros são agrupados de acordo com o domínio ao qual pertencem. Para cada domínio monitorado, o sistema contabiliza a quantidade de novas credenciais identificadas durante a janela temporal configurada e prepara automaticamente uma notificação eletrônica. Além do domínio afetado e da quantidade de ocorrências, o alerta inclui informações que auxiliam na localização das evidências, como o endereço eletrônico comprometido, o identificador da mensagem de origem, o grupo monitorado e a URL associada quando disponível. Entretanto, informações sensíveis, como as senhas identificadas durante o processamento, não são incluídas nas notificações.

Conforme observado na Figura 4.10, o módulo consulta automaticamente o índice de credenciais considerando a janela temporal configurada, identifica novas ocorrências para cada domínio monitorado, contabiliza a quantidade de credenciais encontradas e inicia o processo de envio das notificações. Durante a execução também são registrados eventos relacionados à busca das informações, ao agrupamento dos resultados e ao status de envio das mensagens eletrônicas, permitindo acompanhar todo o funcionamento do módulo.

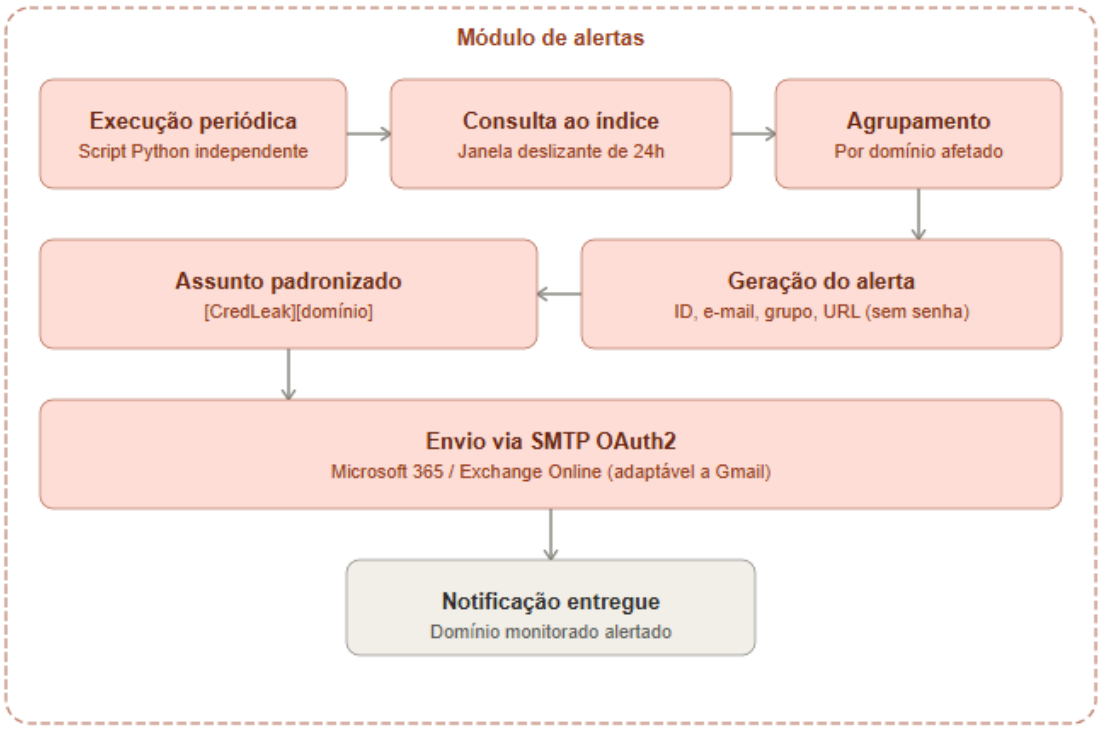


Figura 4.9: Fluxo de execução do módulo de alerta proposta nesta pesquisa.
Fonte: Elaboração própria.

Após a consolidação das informações, o sistema gera automaticamente uma mensagem eletrônica destinada aos responsáveis pelo domínio afetado.

A Figura 4.11 apresenta um exemplo do alerta produzido pela arquitetura.

Conforme ilustrado na Figura 4.11, a mensagem apresenta ao destinatário o domínio monitorado, a quantidade de novas credenciais identificadas durante o intervalo analisado e informações suficientes para localização das evidências correspondentes. A organização das informações permite que os responsáveis identifiquem rapidamente a existência de novas ocorrências e iniciem os procedimentos de verificação e resposta.

Embora o correio eletrônico seja utilizado como mecanismo de disseminação da inteligência, a arquitetura foi desenvolvida de forma a preservar a confidencialidade das informações monitoradas. Os detalhes completos das credenciais permanecem armazenados no Elasticsearch e podem ser consultados apenas por meio do ambiente analítico implementado no Kibana, permitindo que mecanismos de autenticação e controle de acesso sejam aplicados antes da visualização das evidências. Dessa forma, a disseminação da inteligência fornece informações suficientes para notificação dos responsáveis sem ampliar desnecessariamente a exposição de dados sensíveis

A implementação desse módulo conclui o fluxo operacional da arquitetura proposta, convertendo os resultados produzidos pelas etapas de coleta, processamento, indexação e análise em produtos de inteligência direcionados aos responsáveis pelos ativos monitorados. Dessa forma, a arquitetura implementa todas as fases previstas para a produção de Inteligência de Ameaças Cibernéticas, desde a aquisição das informações em fontes abertas até sua disseminação de forma estruturada e acionável, permitindo reduzir

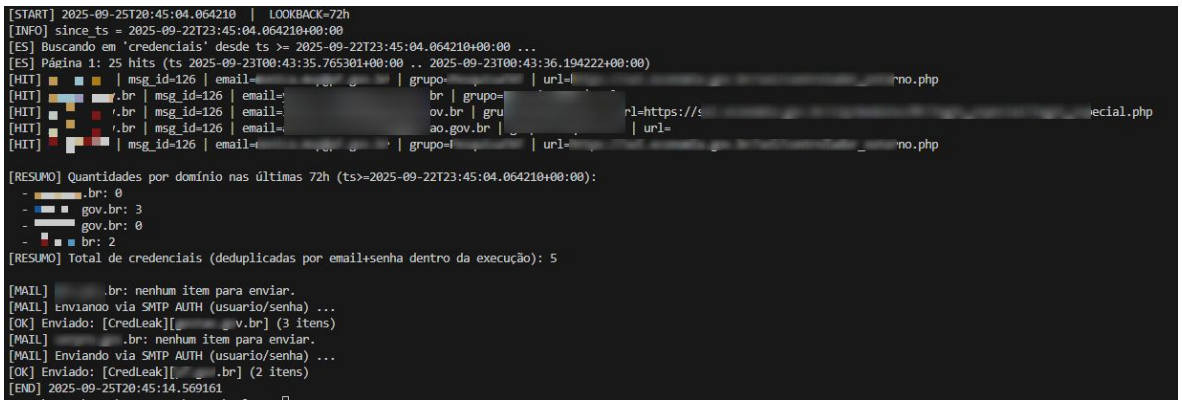


Figura 4.10: Execução do módulo de disseminação da inteligência.
Fonte: Elaboração própria.



Figura 4.11: Exemplo de notificação gerada automaticamente pelo módulo de disseminação da inteligência.
Fonte: Elaboração própria.

o tempo entre a identificação de uma credencial comprometida e a adoção de medidas de mitigação pelas organizações monitoradas.

4.3 RESULTADOS DA PROVA DE CONCEITO

A prova de conceito foi conduzida com o objetivo de validar a arquitetura proposta para monitoramento automatizado de credenciais comprometidas divulgadas em grupos públicos do Telegram. Durante o período de monitoramento, todos os módulos da arquitetura permaneceram em operação de forma contínua e integrada, executando automaticamente as etapas de coleta, processamento, indexação, análise e disseminação da inteligência.

A validação buscou verificar não apenas o funcionamento individual de cada módulo, mas principalmente a integração entre todas as etapas da arquitetura. Para isso, foram avaliadas a capacidade de identificar credenciais pertencentes aos domínios monitorados, preservar os metadados associados às evidências coletadas, disponibilizar mecanismos para exploração analítica das informações e gerar notificações automáticas destinadas aos responsáveis pelos domínios afetados.

Durante aproximadamente três meses foram monitorados dois grupos públicos do Telegram previamente selecionados em função da recorrente divulgação de credenciais comprometidas. Nesse período,

cerca de 100 arquivos foram coletados e processados automaticamente pela arquitetura, contemplando diferentes formatos de armazenamento das informações, incluindo arquivos TXT, CSV, XML, ZIP e RAR. A arquitetura foi configurada para monitorar 239 domínios de interesse pertencentes às organizações participantes da pesquisa, restringindo o processamento às credenciais relacionadas ao escopo definido para a prova de conceito.

Como resultado, foram indexadas 9.947 credenciais pertencentes aos domínios monitorados. Os documentos produzidos permaneceram disponíveis para consulta no Elasticsearch, permitindo sua exploração por meio dos painéis analíticos implementados no Kibana e a geração automatizada de notificações sempre que novas ocorrências eram identificadas para os domínios acompanhados.A Tabela 4.6 apresenta um resumo dos principais resultados obtidos durante a execução da prova de conceito.

Tabela 4.6: Resumo dos resultados obtidos durante a prova de conceito.

Indicador	**Resultado**
Período de monitoramento	3 meses
Grupos públicos monitorados	2
Domínios monitorados	239
Arquivos processados	Aproximadamente 100
Credenciais indexadas	9.947
Frequência da coleta	A cada 6 horas
Frequência da geração de alertas	A cada 6 horas
Formatos suportados	TXT, CSV, XML, ZIP e RAR
Plataformas utilizadas	Elasticsearch e Kibana

Conforme apresentado na Tabela 4.6, a arquitetura operou continuamente durante todo o período de monitoramento, automatizando integralmente o fluxo de obtenção, processamento e disseminação das informações. O volume de credenciais identificadas evidencia a capacidade da solução em processar dados provenientes de fontes abertas e demonstra que a combinação entre coleta automatizada, processamento estruturado, indexação e mecanismos de exploração analítica permite produzir informações relevantes para atividades de Cyber Threat Intelligence.

Conforme observado na Figura 4.4, o ambiente analítico reúne em uma única interface consultas às credenciais indexadas, indicadores quantitativos e visualizações temporais, permitindo acompanhar continuamente a evolução das informações produzidas durante o monitoramento. Essa integração possibilita que o analista obtenha rapidamente uma visão geral do ambiente monitorado e identifique alterações relevantes no comportamento das fontes acompanhadas.

4.3.1 Validação da Arquitetura

A validação da arquitetura foi conduzida com o objetivo de verificar sua capacidade de executar, de forma integrada e automatizada, as etapas definidas na metodologia proposta. Mais do que avaliar individualmente cada módulo, buscou-se verificar a operacionalização do fluxo completo, desde a aquisição dos dados provenientes dos grupos públicos monitorados até a disponibilização das ocorrências identificadas para análise e disseminação.

A Prova de Conceito foi executada durante aproximadamente três meses, com ciclos de coleta realizados em intervalos de seis horas. Nesse período, foram processados aproximadamente 100 arquivos provenientes de dois canais ou grupos públicos do Telegram e identificadas e indexadas 9.947 ocorrências de credenciais associadas aos 239 domínios monitorados. A execução do fluxo permitiu verificar a integração entre os módulos de coleta, processamento, indexação, análise e disseminação, fornecendo evidências da viabilidade operacional da arquitetura no cenário experimental avaliado.

As evidências apresentadas ao longo deste capítulo corroboram essa integração. As Figuras 4.4, 4.5, 4.6 e 4.8 demonstram que os registros produzidos durante o processamento e indexados no Elasticsearch permaneceram disponíveis para exploração analítica, preservando os atributos das credenciais e os metadados associados às ocorrências. A realização de consultas, a aplicação de filtros e a análise da distribuição temporal dos registros permitiram explorar as informações sob diferentes perspectivas e recuperar o contexto necessário à análise das evidências identificadas.

A etapa de disseminação também foi validada durante a execução da Prova de Conceito. Conforme apresentado nas Figuras 4.10 e 4.11, o módulo de notificação consultou periodicamente os registros indexados, identificou novas ocorrências relacionadas aos domínios monitorados e gerou automaticamente as notificações correspondentes. Os alertas foram estruturados de modo a fornecer informações para localização e análise inicial das ocorrências, mantendo as senhas identificadas restritas ao ambiente analítico.

Dessa forma, a validação demonstrou que os componentes implementados puderam operar de maneira integrada e recorrente durante o período experimental, transformando dados provenientes das fontes monitoradas em registros estruturados, contextualizados e disponíveis para análise e disseminação. Os resultados obtidos sustentam, portanto, a viabilidade operacional da arquitetura no escopo avaliado, sem implicar generalização para outras fontes, volumes de dados ou condições operacionais não contempladas pela Prova de Conceito.

4.3.2 Discussão dos Resultados

Os resultados obtidos durante a Prova de Conceito demonstraram a viabilidade da integração das etapas de coleta, processamento, indexação, análise e disseminação previstas na arquitetura proposta. A execução integrada desses módulos permitiu transformar dados não estruturados provenientes das fontes monitoradas em registros estruturados e contextualizados, automatizando atividades que, de outra forma, demandariam intervenção recorrente durante o processo de monitoramento.

Durante aproximadamente três meses de execução, foram identificadas e indexadas 9.947 ocorrências de credenciais associadas aos 239 domínios monitorados. Considerando que a validação foi realizada a partir de apenas dois canais ou grupos públicos do Telegram, esses resultados não permitem generalizações sobre a plataforma como um todo. Entretanto, evidenciam o potencial das fontes selecionadas para a identificação de credenciais expostas relacionadas aos ativos de interesse e demonstram a aplicabilidade do Telegram, no contexto avaliado, como fonte para atividades de monitoramento e produção de CTI.

Outro aspecto observado durante a validação foi a heterogeneidade dos dados disponibilizados pelas fontes monitoradas. Foram processados aproximadamente 100 arquivos em formatos como TXT, CSV, XML, ZIP e RAR, contendo diferentes formas de representação das credenciais. Essa diversidade reforça

a importância da etapa de processamento da arquitetura, responsável por identificar, normalizar e estruturar informações provenientes de conteúdos com diferentes formatos e padrões de organização.

A preservação dos metadados associados às ocorrências também se mostrou relevante para sua contextualização. Além dos atributos das credenciais identificadas, foram mantidas informações relacionadas à origem, ao grupo ou canal monitorado, à mensagem, à URL associada e à temporalidade da ocorrência. Esses elementos permitem recuperar o contexto dos registros e fornecem informações adicionais para consultas, análises e atividades posteriores de investigação. Dessa forma, o resultado do processamento não se restringe à extração de credenciais, mas inclui elementos necessários à sua utilização no processo de produção de CTI.

Na etapa de disseminação, a geração automatizada de notificações permitiu comunicar novas ocorrências relacionadas aos domínios monitorados sem expor as senhas identificadas no conteúdo dos alertas. As informações necessárias à consulta e localização das evidências são disponibilizadas aos responsáveis, enquanto os atributos sensíveis permanecem restritos ao ambiente analítico. Essa separação permite disseminar a ocorrência identificada preservando o acesso controlado às informações mais sensíveis.

De forma geral, os resultados demonstraram a viabilidade operacional da arquitetura no cenário avaliado e a capacidade de integração dos módulos implementados em ciclos periódicos de monitoramento. A Prova de Conceito não teve como objetivo avaliar a totalidade das fontes disponíveis no Telegram, validar a atividade das credenciais identificadas ou mensurar comparativamente o desempenho da solução em relação a procedimentos manuais. Dessa forma, os resultados devem ser interpretados dentro do escopo experimental definido, como evidência da viabilidade da arquitetura para automatizar o monitoramento de credenciais expostas associadas a ativos de interesse e apoiar a produção de *Cyber Threat Intelligence*.

4.3.3 Contribuições Alcançadas

Os resultados obtidos por meio da Prova de Conceito permitem retomar as contribuições apresentadas no início desta dissertação e discutir sua materialização no contexto da validação realizada. Nesse sentido, a principal contribuição alcançada está relacionada à integração das diferentes etapas da produção de Cyber Threat Intelligence em um fluxo automatizado e orientado ao monitoramento de credenciais expostas associadas a ativos de interesse.

Do ponto de vista metodológico, os resultados demonstraram a possibilidade de articular, em uma mesma arquitetura, a aquisição de dados provenientes de fontes abertas, a identificação e estruturação de credenciais, sua associação aos domínios monitorados, a preservação dos metadados de origem, a indexação para exploração analítica e a disseminação das ocorrências identificadas. Essa integração constitui o principal diferencial em relação aos trabalhos correlatos analisados, que apresentam contribuições relevantes para etapas específicas da produção de CTI, mas, no conjunto de estudos considerado nesta pesquisa, não contemplam esse fluxo integrado especificamente direcionado ao monitoramento contínuo de credenciais expostas associadas a ativos previamente definidos.

A execução da Prova de Conceito forneceu evidências experimentais da viabilidade operacional dessa integração. Durante aproximadamente três meses, foram monitorados dois canais ou grupos públicos do Telegram e 239 domínios de interesse, resultando na identificação e indexação de 9.947 ocorrências de cre-

denciais. A execução automática em intervalos de seis horas correspondeu a aproximadamente 360 ciclos de monitoramento durante o período experimental, demonstrando que as etapas implementadas puderam ser executadas de maneira recorrente sem a necessidade de acionamento manual de cada componente do fluxo.

Os resultados também evidenciaram a importância do direcionamento da produção de inteligência aos requisitos previamente definidos. A utilização dos domínios de interesse como critério de seleção permitiu restringir o conjunto analisado às ocorrências relacionadas aos ativos monitorados, enquanto a preservação de informações sobre origem, fonte e temporalidade forneceu contexto adicional para sua posterior recuperação e análise. Dessa forma, a contribuição da arquitetura não se limita à identificação de padrões de credenciais, mas compreende sua inserção em um processo orientado à produção de informações contextualizadas para apoio às atividades de segurança cibernética.

Em relação ao impacto da automação, os resultados permitem quantificar o volume e a frequência das atividades realizadas automaticamente, mas não permitem determinar um percentual de redução de tempo em comparação com procedimentos manuais. Embora aproximadamente 360 ciclos tenham sido executados automaticamente durante o período experimental, não foi estabelecido um *baseline* com o tempo necessário para que um analista realizasse manualmente as mesmas atividades. Essa limitação impede uma comparação quantitativa direta de eficiência temporal, embora os resultados demonstrem a automatização das atividades repetitivas contempladas pela arquitetura.

Por fim, a pesquisa resultou também em produção científica diretamente relacionada à arquitetura desenvolvida. O trabalho *Proposal of an OSINT Pipeline for Monitoring Exposed Credentials in Underground Telegram Channels* foi apresentado na *Second Summer School on Artificial Intelligence in Cybersecurity (CYBER-AI 2026)*, com publicação prevista como *Proceeding Paper* no periódico *Engineering Proceedings* [18].

5 CONCLUSÃO E TRABALHOS FUTUROS

O crescimento do número de credenciais comprometidas disponíveis em ambientes digitais, aliado à velocidade com que essas informações são disseminadas em plataformas de mensageria e outras fontes abertas, evidencia a necessidade de mecanismos capazes de apoiar continuamente a produção de Cyber Threat Intelligence. Nesse contexto, esta dissertação apresentou uma arquitetura para monitoramento automatizado de credenciais expostas em canais públicos do Telegram, integrando as etapas de coleta, processamento, indexação, análise e disponibilização das informações em um fluxo contínuo de produção de Inteligência.

A arquitetura proposta foi desenvolvida com base nos princípios do ciclo de Inteligência e nas boas práticas observadas na literatura sobre Cyber Threat Intelligence, incorporando mecanismos automatizados para aquisição de mensagens, identificação de arquivos contendo credenciais, extração de informações relevantes, normalização dos dados e indexação em uma plataforma de busca e análise. A utilização do Elasticsearch como mecanismo de armazenamento e indexação, associada ao Kibana para construção de painéis analíticos, possibilitou a organização e visualização das informações coletadas, permitindo acompanhar indicadores relacionados às credenciais monitoradas e apoiar atividades de análise e resposta.

A avaliação da solução demonstrou a viabilidade da utilização de plataformas de mensageria como fontes de Cyber Threat Intelligence para identificação de credenciais comprometidas pertencentes a domínios de interesse. Os resultados obtidos evidenciaram que a automação do processo de monitoramento reduz significativamente o esforço necessário para aquisição e tratamento das informações, além de contribuir para disponibilizar evidências de comprometimento em menor intervalo de tempo quando comparado às atividades realizadas manualmente. Dessa forma, a arquitetura proposta demonstra potencial para apoiar organizações na ampliação da consciência situacional e na adoção de medidas preventivas relacionadas ao comprometimento de credenciais.

Do ponto de vista científico, esta pesquisa contribui ao integrar, em uma única arquitetura, diferentes etapas do processo de produção de Cyber Threat Intelligence aplicadas ao monitoramento de credenciais expostas em plataformas de mensageria. Além de consolidar conceitos provenientes das áreas de Inteligência, Open Source Intelligence e Cyber Threat Intelligence, a pesquisa apresenta uma implementação prática capaz de transformar informações provenientes de fontes abertas em produtos de Inteligência destinados ao apoio à tomada de decisão. Espera-se que os resultados obtidos possam servir como referência para pesquisas futuras voltadas ao desenvolvimento de arquiteturas automatizadas de monitoramento e análise de ameaças cibernéticas.

5.1 LIMITAÇÕES E OPORTUNIDADES DE EVOLUÇÃO

Embora os resultados obtidos tenham demonstrado a viabilidade da arquitetura proposta, algumas limitações devem ser consideradas quanto ao alcance da validação realizada por meio da Prova de Conceito. Essas limitações estão relacionadas principalmente ao escopo das fontes monitoradas, às capacidades analíticas implementadas, à infraestrutura experimental e às métricas utilizadas na avaliação da solução.

A primeira limitação refere-se ao escopo das fontes monitoradas. A validação foi conduzida a partir de dois canais ou grupos públicos do Telegram previamente selecionados por apresentarem divulgação de credenciais expostas. Dessa forma, os resultados representam o comportamento da arquitetura nas fontes selecionadas e não devem ser generalizados para todo o ecossistema do Telegram ou para outras fontes utilizadas na disseminação desse tipo de informação. Além disso, a Prova de Conceito restringiu-se a fontes públicas acessíveis por meio da API da plataforma, não contemplando canais privados, fóruns, repositórios de compartilhamento de arquivos ou outras fontes abertas potencialmente relevantes.

Outra limitação está relacionada às capacidades analíticas implementadas. Embora a arquitetura permita relacionar as credenciais identificadas aos domínios de interesse e preservar metadados que possibilitam consultas sobre as ocorrências, a avaliação de sua criticidade permanece dependente da atuação do analista. Não foram implementados mecanismos automatizados para classificação de risco, priorização das ocorrências ou estimativa de impacto. Da mesma forma, apesar de os registros armazenados permitirem identificar recorrências e reconstruir o histórico das ocorrências por meio de consultas, não foram desenvolvidos indicadores específicos para mensurar automaticamente a persistência temporal das credenciais expostas.

A infraestrutura empregada foi dimensionada para a validação da arquitetura em escala experimental. Nesse contexto, o processamento foi direcionado aos 239 domínios previamente definidos como de interesse, sendo descartadas, durante o processamento, as credenciais que não apresentavam associação com esses domínios. Essa decisão permitiu concentrar o processamento e o armazenamento no objeto de interesse da pesquisa, mas impossibilita análises retrospectivas sobre as credenciais descartadas e limita a avaliação da arquitetura sobre a totalidade dos dados disponibilizados pelas fontes monitoradas.

Também deve ser considerada como limitação a ausência de uma avaliação experimental comparativa entre o tempo necessário para execução manual das atividades de monitoramento e o tempo de processamento da arquitetura automatizada. Durante aproximadamente três meses de execução, a coleta foi realizada automaticamente em intervalos de seis horas, correspondendo a cerca de quatro execuções diárias e aproximadamente 360 ciclos de monitoramento. Nesse período, foram identificadas e indexadas 9.947 ocorrências associadas aos domínios de interesse, correspondendo a aproximadamente 110 ocorrências por dia e 28 ocorrências por ciclo. Assim, os resultados permitem quantificar o volume de atividades executadas automaticamente, mas não determinar um percentual de redução de tempo em relação a um procedimento manual, uma vez que não foi estabelecido um *baseline* experimental para essa comparação.

As limitações identificadas indicam diferentes possibilidades de evolução da arquitetura. Em relação às fontes de dados, trabalhos futuros podem ampliar o número de canais e grupos monitorados e incorporar outras fontes abertas relevantes para a produção de CTI. A inclusão de mecanismos para descoberta automatizada de novas fontes também pode ampliar a cobertura do monitoramento, reduzindo a dependência

da seleção prévia dos canais de interesse.

No âmbito analítico, a arquitetura pode ser ampliada com mecanismos de classificação e priorização das ocorrências, enriquecimento com fontes externas e indicadores capazes de caracterizar recorrência, persistência e histórico de redistribuição das credenciais. A incorporação desses recursos permitiria aumentar o nível de contextualização das informações produzidas e fornecer elementos adicionais para apoiar a avaliação de risco e a tomada de decisão pelos analistas.

Como evolução da avaliação experimental, recomenda-se realizar estudos comparativos entre procedimentos manuais e automatizados, considerando métricas como tempo de processamento, volume de dados processados por unidade de tempo, necessidade de intervenção humana e escalabilidade. A realização desses experimentos permitiria mensurar quantitativamente o ganho de eficiência proporcionado pela automação, complementando os resultados obtidos nesta pesquisa.

Por fim, os mecanismos de disseminação podem ser ampliados por meio da integração com plataformas de gerenciamento de incidentes e de CTI. Também podem ser investigados mecanismos de notificação com menor latência, adequados a cenários que demandem respostas mais rápidas. Essas evoluções podem ampliar a aplicabilidade da arquitetura em ambientes operacionais e fortalecer sua integração com processos de prevenção, detecção e resposta a incidentes.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] KENT, S. *Strategic Intelligence for American World Policy*. Princeton University Press, 2025. (Princeton Legacy Library). ISBN 9780691273754. Disponível em: <https://books.google.com/books?id=7eooEQAAQBAJ>.

[2] CLARK, R. M. *Intelligence Analysis: A Target-Centric Approach*. 2. ed. CQ Press, 2006. ISBN 9781933116938. Disponível em: <https://books.google.com/books?id=KTK_PwAACAAJ>.

[3] LOWENTHAL, M. *Intelligence: From Secrets to Policy*. SAGE Publications, 2012. ISBN 9781608716753. Disponível em: <https://books.google.com.br/books?id=xNBbYNt3JJ0C>.

[4] SANTOS, P.; ABREU, R.; REIS, M. J. C. S.; SERóDIO, C.; BRANCO, F. A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors*, v. 25, n. 14, p. 4272, 2025.

[5] SAEED, S.; SUAYYID, S. A.; AL-GHAMDI, M. S.; AL-MUHAISEN, H.; ALMUHAIDEB, A. M. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, MDPI, v. 23, n. 16, p. 7273, 2023. Disponível em: <https://www.mdpi.com/1424-8220/23/16/7273>.

[6] CHATZIAMANETOGLOU, D.; RANTOS, K. Cyber threat intelligence on blockchain: A systematic literature review. *Computers*, MDPI, v. 13, n. 3, p. 60, 2024. Disponível em: <https://www.mdpi.com/2073-431X/13/3/60>.

[7] Verizon Business. *2025 Data Breach Investigations Report (DBIR)*. New York, NY, USA, 2025. Disponível em: <https://www.verizon.com/business/resources/reports/dbir/>.

[8] RABZELJ, M.; SEDLAR, U. Beyond the leak: Analyzing the real-world exploitation of stolen credentials using honeypots. *Sensors*, MDPI, v. 25, n. 12, p. 3676, 2025.

[9] HAYS, S.; SANDBORN, M.; WHITE, J. Reducing usefulness of stolen credentials in sso contexts. *arXiv preprint arXiv:2401.11599*, 2024.

[10] THOMAS, K.; LI, F.; ZAND, A.; BARRETT, J.; RANIERI, J.; INVERNIZZI, L.; MARKOV, Y.; COMANESCU, O.; ERANTI, V.; MOSCICKI, A. et al. Data breaches, phishing, or malware? understanding the risks of stolen credentials. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. [S.l.]: ACM, 2017. p. 1421–1434.

[11] MADARIE, R.; POOT, C. de; KRANENBARG, M. W. Criminal clickbait: A panel data analysis on the attractiveness of online advertisements offering stolen data. *Frontiers in Big Data*, v. 6, p. 1320569, 2023.

[12] CAMPOBASSO, M.; ALLODI, L. Know your cybercriminal: Evaluating attacker preferences by measuring profile sales on an active, leading criminal market for user impersonation at scale. *arXiv preprint arXiv:2303.03249*, 2023.

[13] PATSAKIS, C.; ARROYO, D.; CASINO, F. The malware as a service ecosystem. In: *Malware: Handbook of Prevention and Detection*. [S.l.]: Springer, 2024. p. 371–394.

[14] ETYANG, F.; PAVITHRAN, P.; MANDELA, N.; MWENDWA, G. The evolution and impact of malware-as-a-service (maas) in the dark web: Systematic review. In: IEEE. *2025 12th International Conference on Computing for Sustainable Global Development (INDIACom)*. [S.l.], 2025. p. 1–7.

[15] SHI, Y.; YANG, Z.; ZHONG, K.; YANG, G.; YANG, Y.; ZHANG, X.; YANG, M. The skeleton keys: A large scale analysis of credential leakage in mini-apps. In: *NDSS*. [S.l.: s.n.], 2025.

[16] HOLTHOUSE, R.; OWENS, S.; BHUNIA, S. The 23andme data breach: Analyzing credential stuffing attacks, security vulnerabilities, and mitigation strategies. *arXiv preprint arXiv:2502.04303*, 2025.

[17] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*. [S.l.], 2024. Disponível em: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.

[18] MARQUES, N.; AUGUSTINHO, B. M.; NZE, G. D.; MENDONçA, F. L.; ALBUQUERQUE, R. Proposal of an osint pipeline for monitoring exposed credentials in underground telegram channels. Proceeding Paper accepted for publication in Engineering Proceedings. Presented at the Second Summer School on Artificial Intelligence in Cybersecurity (CYBER-AI 2026), Universidad Complutense de Madrid. 2026.

[19] PHYTHIAN, M. (Ed.). *Understanding the Intelligence Cycle*. Routledge, 2022. Disponível em: <https://doi.org/10.4324/9781003031475>.

[20] BARRIOS-GONZáLEZ, M.; AGUIAR-PéREZ, J. M.; PéREZ-JUáREZ, M. ; BENITO, E. Castañeda-de. Redefining cyber threat intelligence with artificial intelligence: From data processing to predictive insights and human–ai collaboration. *Applied Sciences*, MDPI, v. 16, n. 3, p. 1668, 2026. Disponível em: <https://www.mdpi.com/2076-3417/16/3/1668>.

[21] ALBARRAK, M.; SALONITIS, K.; JAGTAP, S. Natural language processing (nlp)-based frameworks for cyber threat intelligence and early prediction of cyberattacks in industry 4.0: A systematic literature review. *Applied Sciences*, MDPI, v. 16, n. 2, p. 619, 2026. Disponível em: <https://www.mdpi.com/2076-3417/16/2/619>.

[22] GUO, Y.; LIU, Z.; HUANG, C.; WANG, N.; MIN, H.; GUO, W.; LIU, J. A framework for threat intelligence extraction and fusion. *Computers & Security*, Elsevier, v. 132, p. 103371, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S016740482300281X>.

[23] LIN, P.-C.; HSU, W.-H.; LIN, Y.-D.; HWANG, R.-H.; WU, H.-K.; LAI, Y.-C.; CHEN, C.-K. Correlation of cyber threat intelligence with sightings for intelligence assessment and augmentation. *Computer Networks*, Elsevier, v. 228, p. 109736, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128623001810>.

[24] HAN, Y.; HAN, W.; LI, A.; LI, S. Cyberattack event and arguments extraction based on feature interaction and few-shot learning. *Scientific Reports*, Nature Publishing Group, v. 15, n. 1, p. 31808, 2025. Disponível em: <https://doi.org/10.1038/s41598-025-15138-x>.

[25] ALAEIFAR, P.; PAL, S.; JADIDI, Z.; HUSSAIN, M.; FOO, E. Current approaches and future directions for cyber threat intelligence sharing: A survey. *Journal of Information Security and Applications*, Elsevier, v. 83, p. 103786, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214212624000899>.

[26] REITTINGER, T.; GRILL, J.; PERNUL, G. Share and benefit: Incentives for cyber threat intelligence sharing. *International Journal of Information Security*, v. 25, n. 1, p. 37, 2026. ISSN 1615-5270. Disponível em: <https://doi.org/10.1007/s10207-025-01165-2>.

[27] AVRAHAMI, Z.; ZWILLING, M.; HAJAJ, C. Leveraging osint for advanced proactive cybersecurity: Strategies and solutions. *IEEE Access*, v. 13, p. 154229–154250, 2025. Disponível em: <https://doi.org/10.1109/ACCESS.2025.3603868>.

[28] ALI, A.; HWANG, R.-H.; LIN, Y.-D. Evaluating cyber threat intelligence: Accuracy, completeness, relevance, and freshness. *IEEE Access*, v. 13, p. 157863–157876, 2025.

[29] MAHBOUBI, A.; LUONG, K.; ABOUTORAB, H.; BUI, H. T.; JARRAD, G.; BAHUTAIR, M.; CAMTEPE, S.; POGREBNA, G.; AHMED, E.; BARRY, B.; GATELY, H. Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, Academic Press (Elsevier), v. 232, p. 1–34, 2024. Disponível em: <https://doi.org/10.1016/j.jnca.2024.104004>.

[30] GARKAVA, T.; MONEVA, A.; LEUKFELDT, R. E. Stolen data markets on telegram: A crime script analysis and situational crime prevention measures. *Trends in Organized Crime*, Springer Nature, 2024.

[31] PUYVELDE, D. V.; RIENZI, F. T. The rise of open-source intelligence. *European Journal of International Security*, v. 10, n. 4, p. 530–544, 2025. Disponível em: <https://doi.org/10.1017/eis.2024.61>.

[32] SZYMONIAK, S.; FOKS, K. Open source intelligence opportunities and challenges: A review. *Advances in Science and Technology Research Journal*, v. 18, n. 3, p. 123–139, 2024. Disponível em: <https://doi.org/10.12913/22998624/186036>.

[33] BROWNE, T. O.; ABEDIN, M.; CHOWDHURY, M. J. M. A systematic review on research utilising artificial intelligence for open source intelligence (osint) applications. *International Journal of Information Security*, v. 23, p. 2911–2938, 2024. Disponível em: <https://doi.org/10.1007/s10207-024-00868-2>.

[34] BALASUBRAMANIAN, P.; NAZARI, S.; KHOLGH, D. K.; MAHMOODI, A.; SEBY, J.; KOSTAKOS, P. *TSTEM: A Cognitive Platform for Collecting Cyber Threat Intelligence in the Wild*. 2024. Disponível em: <https://arxiv.org/abs/2402.09973>.

[35] BAUMGARTNER, J.; ZANNETTOU, S.; SQUIRE, M.; BLACKBURN, J. *The Pushshift Telegram Dataset*. 2020. Disponível em: <https://arxiv.org/abs/2001.08438>.

[36] MORGIA, M. L.; MEI, A.; MONGARDINI, A. M. *TGDataset: Collecting and Exploring the Largest Telegram Channels Dataset*. 2025. Disponível em: <https://arxiv.org/abs/2303.05345>.

[37] SILVA, A. de Melo e; GONDIM, J. J. C.; ALBUQUERQUE, R. de O.; VILLALBA, L. J. G. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet*, MDPI, v. 12, n. 6, p. 108, 2020.

[38] ARIKKAT, D. R.; T., S. B.; NICOLAZZO, S.; NOCERA, A.; P., V.; A., R. R. K.; R, K. *CTI Dataset Construction from Telegram*. 2025. Disponível em: <https://arxiv.org/abs/2509.20943>.

[39] RASTOGI, N.; DUTTA, S.; ZAKI, M. J.; GITTENS, A.; AGGARWAL, C. *TINKER: A framework for Open source Cyberthreat Intelligence*. 2023. Disponível em: <https://arxiv.org/abs/2102.05571>.

[40] MARCHIORI, F.; CONTI, M.; VERDE, N. V. Stixnet: A novel and modular solution for extracting all stix objects in cti reports. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security*. ACM, 2023. (ARES 2023), p. 1–11. Disponível em: <http://dx.doi.org/10.1145/3600160.3600182>.

[41] IACOVAZZI, A.; WANG, H.; BUTUN, I.; RAZA, S. Towards cyber threat intelligence for the iot. In: *Proceedings of the 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*. Pafos, Cyprus: IEEE, 2023. p. 483–490. ISBN 979-8-3503-1734-3. Disponível em: <https://doi.org/10.1109/DCOSS-IoT58021.2023.00081>.

[42] AL-MOHANNADI, H.; AWAN, I.; HAMAR, J. A.; CULLEN, A.; DISSO, J.; ARMITAGE, L. Cyber threat intelligence from honeypot data using elasticsearch. In: *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. [s.n.], 2018. p. 900–906. Disponível em: <https://doi.org/10.1109/AINA.2018.00132>.

[43] OSINGA, F. P. B. *Science, Strategy and War: The Strategic Theory of John Boyd*. London: Routledge, 2006. ISBN 9780415409690.

[44] ALAEIFAR, P.; PAL, S.; JADIDI, Z.; HUSSAIN, M. et al. Current approaches and future directions for cyber threat intelligence sharing: A survey. *Journal of Information Security and Applications*, v. 83, p. 103786, 2024.