DISSERTAÇÃO DE MESTRADO PROFISSIONAL

# PROPOSTA DE UM FRAMEWORK PARA MELHORIA DA QUALIDADE NA PRODUÇÃO DE INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA

**Rogerio Machado da Silva**

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

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

# PROPOSTA DE UM FRAMEWORK PARA MELHORIA DA QUALIDADE NA PRODUÇÃO DE INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA

**Rogerio Machado da Silva**

**Orientador: Prof. João José Costa Gondim, Dr., PPEE/CIC-UnB**

**Coorientador: Prof. Robson de Oliveira Albuquerque, Dr., FT/UnB**

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM ENGENHARIA ELÉTRICA

PPEE.MP.047
BRASÍLIA/DF JUNHO - 2023

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

# PROPOSTA DE UM FRAMEWORK PARA MELHORIA DA QUALIDADE NA PRODUÇÃO DE INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA

**Rogerio Machado da Silva**

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

Banca Examinadora

Prof. João José Costa Gondim, Dr., PPEE/CIC-UnB _____
*Orientador*

Prof. Robson de Oliveira Albuquerque, Dr., FT/UnB _____
*Coorientador*

Prof. Dino Macedo Amaral, Dr., Banco do Brasil _____
*Examinador Externo*

Prof. Rafael Rabelo Nunes, Dr., PPEE/ADM-UnB _____
*Examinador interno*

Prof. Georges Daniel Amvame Nzé, Dr., PPEE/ENE-UnB _____
*Examinador Suplente*

**FICHA CATALOGRÁFICA**

SILVA, ROGERIO MACHADO
PROPOSTA DE UM FRAMEWORK PARA MELHORIA DA QUALIDADE NA PRODUÇÃO DE INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA [Distrito Federal] 2023.
xvi, 68 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

| | |
|---|---|
| 1. Inteligência de Ameaças | 2. Ciclo de Inteligência |
| 3. Análise Metodológica | 4. Cyber Threat Intelligence |
| I. ENE/FT/UnB | II. Título (série) |

**REFERÊNCIA BIBLIOGRÁFICA**

SILVA, R. M. (2023). *PROPOSTA DE UM FRAMEWORK PARA MELHORIA DA QUALIDADE NA PRODUÇÃO DE INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA*. Dissertação de Mestrado Profissional, Publicação PPEE.MP.047, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 68 p.

**CESSÃO DE DIREITOS**

AUTOR: Rogerio Machado da Silva
TÍTULO: PROPOSTA DE UM FRAMEWORK PARA MELHORIA DA QUALIDADE NA PRODUÇÃO DE INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA.
GRAU: Mestre em Engenharia Elétrica ANO: 2023



---

Rogerio Machado da Silva
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

## DEDICATÓRIA

Dedico essa conquista a meus pais, exemplos de integridade, dedicação e esforço. A determinação com que vocês enfrentam os desafios, moldou meu caráter e me inspirou a ser quem sou. Vocês me ensinaram o valor do trabalho, da persistência e da busca constante pelo conhecimento. Vocês são a fonte do meu sucesso.

## AGRADECIMENTOS

A ABIN pelo fomento à formação acadêmica dos profissionais de inteligência.

Aos Professores, todos foram excelentes, sintam-se representados na figuras dos meus orientadores, com os quais tive maior contato, Professores João José Costa Gondim e Robson de Oliveira Albuquerque, pelos ensinamentos, dedicação, paciência e experiências compartilhadas no decorrer dessa jornada.

Aos colegas de turma e colaboradores do PPEE, em especial à Tayná Gabriela Araújo Albuquerque e Cristiana Rosa da Costa que estiveram presentes nos momentos certos, sempre atentas aos prazos, nos ajudando incondicionalmente e a qualquer hora, literalmente, sempre com comunicação clara, muita paciência e precisas nas nossas necessidades.

Minha gratidão especial à minha grande família, os de longe e os de perto, os de sangue e os de coração, todos foram importantes de alguma forma, todos me apoiaram e incentivaram durante esse período de estudo e pesquisa, seja em pensamento, em oração, suportando a ausência, enfim, mesmo que pela mais singela forma.

Aos colegas de trabalho que torceram por mim e sempre me apoiaram e suportaram minha ausência, a compreensão de vocês contribuiu bastante para o meu sucesso.

Essa conquista é nossa, cada um de vocês é um pilar na construção desse conhecimento.

## RESUMO

No espaço cibernético, os limites estão constantemente sendo ultrapassados em nome do progresso e comodidade, invariavelmente abrindo caminho para novas vulnerabilidades e ataques em potencial. As abordagens tradicionais de segurança não são capazes de conter a natureza dinâmica das novas técnicas e ameaças, cada vez mais adaptativas e complexas. Nesse cenário, o compartilhamento de inteligência de ameaça vem crescendo. Contudo, a heterogeneidade e o grande volume de dados de ameaças dificultam a identificação dos dados relevantes, o que impõe grande limitação aos analistas de segurança. Dentre os fatores que contribuem para a baixa qualidade da *Cyber Threat Intelligence* (CTI), destaca-se a falta de direção e planejamento, cuja consequência é a produção de informações imprecisas, incompletas ou desatualizadas, que tornam as ações reativas. Porém, inteligência de ameaça de qualidade tem impacto positivo no tempo de resposta a um incidente. A proposta para contornar essa limitação é a adoção de um processo de produção de conhecimento baseado no ciclo de inteligência, apoiado pela consciência situacional e o modelo 5W3H para criação de contexto. A fase de direção e planejamento é a fase menos abordada nas pesquisas científicas, mas, quando bem executada tem relação direta para que a inteligência produzida seja relevante, precisa e oportuna, pois define o propósito e o escopo das etapas seguintes. As próximas fases do processo visam o refinamento progressivo de dados, que iniciam com grande volume e baixa relevância e por meio de avaliação, busca por correlações, análises, formação de contexto e interpretações terminam com baixo volume, porém capazes de serem empregados para tomada de decisões.



## ABSTRACT

In cyberspace, boundaries are constantly being crossed in the name of progress and convenience, invariably paving the way for new vulnerabilities and potential attacks. Traditional security approaches are not able to contain the dynamic nature of new techniques and threats, which are increasingly adaptive and complex. In this scenario, threat intelligence sharing is growing. However, the heterogeneity and the large volume of threat data make it difficult to identify the relevant data, imposing significant limitations on security analysts. Among the factors contributing to the low quality of Cyber Threat Intelligence (CTI), the lack of direction and planning stands out, resulting in the production of inaccurate, incomplete, or outdated information that leads to reactive actions. However, quality threat intelligence has a positive impact on the response time to an incident. The proposed solution to overcome this limitation is the adoption of a knowledge production process based on the intelligence cycle, supported by situational awareness and the 5W3H model for context creation. The direction and planning phase is the least addressed phase in scientific research, but when executed properly it directly contributes to the relevance, accuracy and timeliness of the intelligence produced, as it defines the purpose and scope of the subsequent steps. The next phases of the process aims at the progressive refinement of data, which starts with a large volume

and low relevance and, by means of evaluation, search for correlations, analysis, context formation, and interpretation, ends up with a low volume, but capable of being used for decision making.

# SUMÁRIO

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE SÍMBOLOS

## Siglas

| | |
|---|---|
| APT | *Advanced Persistent Threat* (Ameaça Persistente Avançada) |
| CCL | *Conscious Competence Learning* (Aprendizagem por Competência Consciente) |
| CTI | *Cyber Threat Intelligence* (Inteligência de Ameaça Cibernéticas) |
| ENISA | *European Union Agency for Network and Information Security* (Agência da União Europeia para Segurança de Redes e Informações) |
| DNS | *Domain Name System* (Sistema de Nomes de Domínio) |
| IDS | *Intrusion Detection System* (Sistema de Detecção de Intrusão) |
| Ioa | *Indicator Of Attack* (Indicador de Ataque) |
| IoC | *Indicator Of Compromise* (Indicador de Comprometimento) |
| IP | *Internet Protocol Version 4* |
| IPS | *Intrusion Protection System* (Sistema de Proteção de Intrusão) |
| JDL | *Joint Directors of Laboratories* |
| MISP | *Malware Information Sharing Platform* |
| ML | *Machine Learning* (Aprendizado de Máquina) |
| NIST | *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia) |
| NLP | *Natural Language Processing* (Processamento de Linguagem Natural) |
| PoP | *Pyramid of Pain* (Pirâmide da Dor) |
| SIEM | *Security Information and Event Management* (Gerenciamento de Informações e Eventos de Segurança) |
| TIC | Tecnologia da Informação e Comunicação |
| TIP | *Threat Intelligence Platform* (Plataforma de Inteligência de Ameaça) |
| TTP | *Tactics, Techniques and Procedures* |

# 1 INTRODUÇÃO

O avanço da tecnologia popularizou o uso da internet e introduziu facilidades significativas que nos induzem a permanecer conectados continuamente, consequentemente, também são incorporadas novas vulnerabilidades [8]. No mesmo sentido, as ameaças cibernéticas crescem em volume e sofisticação [9, 10, 11, 12, 13, 14, 15], e constituem complicadores para os profissionais de segurança cibernética [16, 13, 17, 18]. Além disso, os atacantes se organizam e evoluem rapidamente, compartilhando ferramentas e serviços para aumentar a eficácia de seus ataques [19].

As instituições têm adotado mecanismos de defesa pró-ativas na tentativa de mitigar ataques cibernéticos [20, 21]. A Inteligência de Ameaça Cibernética (CTI - *Cyber Threat Intelligence*) é uma das medidas empregadas e abrange a coleta de informações sobre ameaças cibernéticas que são armazenadas e organizadas. A análise dessas informações possibilita prever, prevenir ou defender ataques cibernéticos [20, 22].

Com o advento da CTI, se consolida o emprego de Plataformas de Inteligência de Ameaças (TIP - *threat intelligence platform*), que em grande parte não abordam o processo completo de produção de inteligência [17, 15]. Isso impacta diretamente na qualidade da CTI gerada.

Nesse contexto foram identificados, por meio de revisão da literatura, os fatores que influenciam na qualidade da CTI. Os principais desafios observados são a heterogeneidade e a gestão do alto volume de dados [20, 23, 9], a falta de mecanismos para avaliação das fontes [19], a baixa capacidade de análise dos dados e pouca ou nenhuma relevância da informação gerada para o contexto da organização, o compartilhamento de inteligência de pouca qualidade [9], além da falta de um processo definido [24].

Por outro lado, inteligência de ameaça cibernética de qualidade contribui para que organizações obtenham uma visão abrangente do cenário de ameaças em que estão inseridas, assim podem avaliar melhor os riscos, priorizar recursos e tomar decisões mais assertivas, além de identificar lacunas de segurança e implementar medidas de mitigação apropriadas para reduzir a superfície de ataque.

## 1.1 MOTIVAÇÃO

Os modelos tradicionais de segurança não são suficientes para conter a rápida evolução de novos métodos de ataque [15, 25, 26]. Nesse sentido houve um aumento significativo dos estudos científicos sobre o tema Inteligência de Ameaças Cibernéticas, à medida que a conscientização sobre a importância dessa disciplina continua a crescer.
A inteligência de ameaças cibernéticas desempenha um papel fundamental na defesa e segurança cibernética, fornecendo informações valiosas sobre ameaças em evolução, vulnerabilidades, táticas e técnicas empregadas, e tentando identificar atores maliciosos. Nos níveis técnico, tático e operacional ajudam as organizações a detectar ameaças precocemente e a responder incidentes de forma mais eficaz. No nível estratégico fornece percepção e compreensão de ameaças relevantes para os tomadores de decisão.

Além disso, a qualidade da inteligência produzida influencia a tomada de decisões estratégicas re-

lacionadas à segurança cibernética, permitindo avaliar riscos, priorizar recursos e implementar medidas adequadas.

Embora a CTI tenha evoluído e se tornado uma parte essencial da segurança cibernética, existem lacunas na produção de inteligência de ameaças de qualidade.

A qualidade da CTI depende da coleta adequada de dados relevantes, no entanto, muitas vezes há falta de acesso a fontes de dados relevantes ou a coleta de dados é limitada, dificultando a produção de inteligência abrangente e precisa.

A falta de contexto adequado é outro desafio da CTI. A análise de contexto é essencial para identificar as ameaças que podem afetar os processos de negócio de uma organização. Sem contexto não será possível produzir inteligência acionável.

Estudos mostram que a colaboração e o compartilhamento de informações entre organizações são fundamentais para uma inteligência de ameaças eficaz. Contudo, há relutância em compartilhar informações devido à preocupações de privacidade, segurança ou competição comercial, o que limita a disponibilidade de informações relevantes e oportunas.

A análise de ameaças requer habilidades especializadas e conhecimento avançado para identificar padrões e correlações e fazer avaliações significativas. A falta desses especialistas pode levar a uma análise limitada e menos abrangente das informações disponíveis e, dessa forma, resultar em inteligência superficial que não fornece compreensão aprofundada das ameaças.

A qualidade da CTI também depende da validação e verificação adequadas dos dados e das fontes sob os aspectos de autenticidade, confiança e competência. Por falta de processos para avaliação das fontes e julgamento do dado, informações imprecisas, desatualizadas ou falsas podem ser consideradas na produção de inteligência, comprometendo a confiabilidade.

A maioria das análises de CTI está baseada na coleta indiscriminada de relatórios, alertas e dados brutos, ao invés de orientada por questões de inteligência predeterminadas. O alto volume de novos dados diários [20, 23, 9] necessitam de mais triangulação para avaliar sua relevância para um contexto de ameaça específico, dessa forma, a ausência de uma metodologia pode induzir à paralisia da análise, principalmente em equipes menores. Além de produzir grande quantidade de informações irrelevantes para a organização.

Da analise desse contexto, observa-se que todas as lacunas tem impacto relevante sobre a qualidade da CTI gerada, então surge a seguinte questão: Como melhorar a qualidade da Inteligência de Ameaça Cibernética?

## 1.2 OBJETIVO

A pesquisa realizada para confecção deste trabalho aborda a melhoria da qualidade na produção de inteligência de ameaças. O desafio principal diz respeito a falta de metodologia para produção de CTI, poucos autores abordam o ciclo de inteligência, ou algum processo de produção do conhecimento, e mesmo os que realizam estudos nesse sentido, evidenciam sua importância, mas não propõem formas de resolver essa questão.

### 1.2.1 Objetivo geral

Essa pesquisa tem por objetivo propor um *framework* baseado no ciclo de inteligência que possibilite uma visão clara dos passos para produção de inteligência de ameaças cibernéticas que atenda aos requisitos de oportunidade, relevância, precisão e completude.

### 1.2.2 Objetivo específico

Compreender a abrangência de pesquisas relacionadas à inteligência de ameaças cibernéticas que façam referência ao ciclo de inteligência.

Promover a conscientização sobre a importância da fase de direção e planejamento e fornecer diretrizes claras para o estabelecimento de objetivos, identificação de fontes de dados relevantes e análise do contexto da organização.

Promover o uso complementar de métodos e processos que sirvam como referência para a aplicação de boas práticas, garantindo o emprego de técnicas adequadas para as informações necessárias para a produção de CTI de qualidade.

### 1.2.3 Contribuições

Os estudos realizados no decorrer dessa pesquisa contribuíram para a confecção de um artigo científico que contempla parte do *framework* proposto nesse trabalho, porém com maior ênfase no emprego do método 5W3H, utilizado para diretriz na construção do contexto da ameaça, e na fase de processamento, em especial o processo de enriquecimento e posterior verificação de completude das informações originadas do enriquecimento de dados.

- R. Machado da Silva, J. J. Costa Gondim, and R. de Oliveira Albuquerque, "Methodology to Improve the Quality of Cyber Threat Intelligence Production Through Open Source Platforms," in CSEI: International Conference on Computer Science, Electronics and Industrial Engineering (CSEI), M. V Garcia and C. Gordón-Gallegos, Eds. Cham: Springer Nature Switzerland, 2023, pp. 86–98.

As contribuições decorrentes do presente trabalho abrangem a proposta de um *framework* para produção de inteligência de ameaça, cuja a inovação está no emprego de métodos complementares que apoiam tanto na construção da consciência situacional, quanto na verificação da completude da inteligência produzida, além da percepção de como a produção científica com o tema Inteligência de Ameaça Cibernética abordam o ciclo de Inteligência.

### 1.2.4 Organização do trabalho

O restante do trabalho está estruturado em quatro capítulos, sendo que no capítulo 2 são apresentados os conceitos necessários para compreensão da solução proposta, além da metodologia de seleção do referencial teórico, metodologia de pesquisa, e os trabalhos correlatos. No capítulo 3 são discutidas características que permitam a integração dos métodos selecionados. No capítulo 4 são relatados aspectos da

construção do *framework* proposto, assim como, considerações baseadas no desenvolvimento da solução e finalmente no capítulo 5 estão as conclusões acerca do *framework* desenvolvido e propostas de trabalhos futuros.

# 2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os principais conceitos abordados nesta pesquisa e os trabalhos relacionados, a fim de fornecer uma base sólida de conhecimentos e conceitos essências para a compreensão da solução proposta, assim como sustentar as discussões e conclusões dessa pesquisa.

## 2.1 CONCEITOS RELACIONADOS

### 2.1.1 Ameaça, vulnerabilidade e ataque

A segurança cibernética desempenha um papel crucial na proteção dos ativos de uma organização, envolvendo a preservação da confidencialidade, integridade e disponibilidade desses ativos [1, 27]. Os ativos abrangem uma ampla gama de elementos que tem valor para a organização como informações, processos de negócios, dispositivos, sistemas e redes [28]. Além disso, a segurança cibernética também se estende à proteção da identidade e autenticação dos usuários, das comunicações seguras, à prevenção e detecção de ameaças, bem como à resposta a incidentes de segurança [29, 30].

No entanto, o espaço cibernético apresenta uma complexa integração de pessoas, *software* e serviços disponíveis na *internet*, mediada por dispositivos físicos de tecnologia da informação e comunicação (TIC) [1]. Essa integração, embora traga benefícios e oportunidades, também introduz desafios significativos, uma vez que os diversos dispositivos e redes interconectados que compõem o espaço cibernético estão distribuídos entre diferentes proprietários, cada um com suas próprias preocupações comerciais, operacionais e regulatórias. Essa dispersão resulta em lacunas de segurança que podem ser exploradas por agentes maliciosos [1].

A segurança busca proteger ativos contra ameaças com potencial para violação. Nesse contexto as partes interessadas atribuem valor a seus ativos e implementam medidas de salvaguarda, como controles de segurança, baseados em avaliações de risco, a fim de reduzir as vulnerabilidades e mitigar os impactos das ameaças [1]. No entanto, os agentes da ameaça também atribuem valor aos ativos de interesse e procuram explorar as vulnerabilidades residuais, ou seja, aquelas que não foram adequadamente protegidas pelos controles implementados [1]. Essa relações podem ser observadas na Figura 2.1.

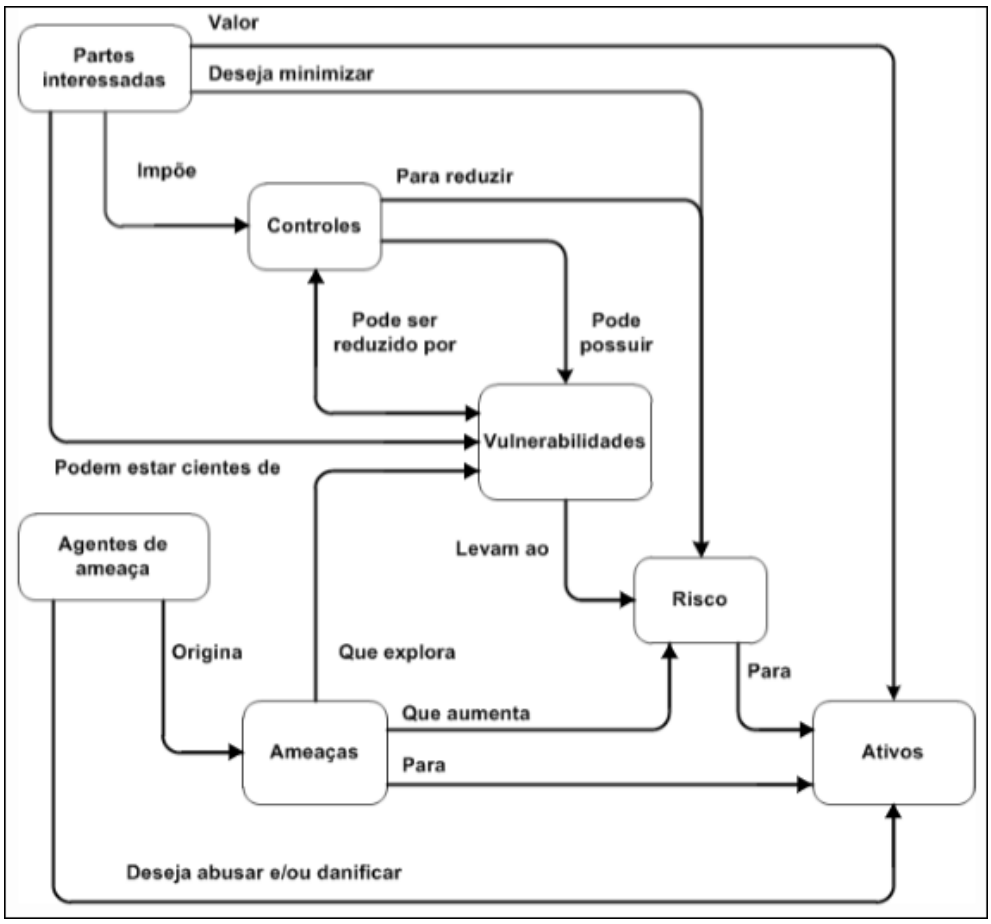


Figura 2.1: Relações de segurança [1]

Agente de ameaça é um indivíduo, grupo ou entidade que realiza ações maliciosas ou prejudiciais com objetivo de comprometer a segurança dos ativos de uma organização [1]. Esses agentes podem ter diferentes motivações, conhecimentos técnicos e níveis de sofisticação.

Ameaça é qualquer evento, indivíduo, entidade ou ação com potencial de interferir e causar danos à integridade, à confidencialidade, à autenticidade e a disponibilidade de dados e informações de uma organização [24]. Tem conexão com ações intencionais ou acidentais que visam explorar vulnerabilidades, incluem as ações de um agente malicioso [9], que compreendem as táticas, técnicas e procedimentos empregados.

A vulnerabilidade está relacionada com situações que colocam a organização em risco, ou seja, suscetível a ações maliciosas (mal-intencionadas) [28]. Enquanto ataque é uma ação não autorizada com intenção de violar a integridade, confidencialidade, autenticidade e disponibilidade [28].

A identificação e avaliação dos riscos cibernéticos são fundamentais para o desenvolvimento de estratégias eficazes de segurança da informação. Os riscos cibernéticos referem-se às ameaças e vulnerabilidades que podem impactar negativamente a confidencialidade, integridade e disponibilidade dos ativos de uma organização [29]. A identificação de riscos envolve a análise detalhada dos ativos, sistemas, redes e processos existentes, bem como a identificação das ameaças potenciais e das vulnerabilidades subjacentes. Já a avaliação de riscos visa determinar a probabilidade e o impacto desses riscos, permitindo a priorização e

implementação de controles adequados para mitigar os riscos identificados [29, 1].

O desenvolvimento de controles cibernéticos é essencial para proteger os ativos de uma organização contra ameaças cibernéticas. Esses controles são medidas técnicas, administrativas e físicas implementadas para mitigar os riscos identificados. Os controles cibernéticos podem incluir *firewalls*, sistemas de detecção e prevenção de intrusões, autenticação de usuários, criptografia, políticas de segurança, treinamento de conscientização, gestão de *patches* e atualizações, backups regulares, entre outros. É importante que esses controles sejam adaptados às necessidades e características específicas da organização, levando em consideração os ativos, ameaças e vulnerabilidades identificados durante a análise de riscos [1].

Através da identificação e avaliação de riscos cibernéticos, do estabelecimento de um Sistema de Gestão da Segurança da Informação e do desenvolvimento de controles cibernéticos apropriados, as organizações podem fortalecer sua postura de segurança e mitigar os riscos associados às ameaças e vulnerabilidades presentes no ambiente cibernético [1].

Incidente são ocorrências, que indicam comprometimento de segurança ou falha de controles, relacionadas e identificadas que possam prejudicar ativos ou comprometer as operações de uma organização [28].

Conclui-se que ameaça é o potencial de realizar uma ação maliciosa, vulnerabilidade, nesse escopo, é o meio pelo qual a ameaça alcança seu objetivo, o ataque é a ação de explorar uma vulnerabilidade, e a evolução do ataque ou seus vestígios são considerados incidentes.

### 2.1.2 Modelo tradicional de segurança cibernética

Devido à natureza dinâmica do espaço cibernético, a segurança é um estado que não pode ser alcançado, o que os especialistas fazem é seguir em sua direção, mas sabendo que não é possível alcançar o objetivo, o que se pode fazer é gerenciar um nível de risco aceitável [31].

Dessa forma, segurança é um processo que deve ser aplicado continuamente, se esse processo for interrompido a segurança piora a medida que novas ameaças e técnicas surgem [31].

O modelo tradicional de segurança abrange a segurança de infraestrutura, segurança de perímetro, segurança ativa e consciência de situação. Normalmente baseado na detecção de anomalias, uso indevido dos recursos de tecnologia da informação e na alteração comportamento [32].

Os sistemas são norteados por políticas, regras, processos, procedimentos, estruturas organizacionais e funções de hardware e software para evitar que o ataque não ocorram [28]. São utilizados sistemas de proteção de perímetro e de detecção de intrusão, para identificar ataques e mitigar seus efeitos, além do emprego de análise ativa da rede para verificar tendências e agir preventivamente antes da ocorrência de um ataque [32].

Esse modelo tem como principais desafios a resposta passiva, a elevada taxa de alarme falso e a baixa capacidade para detecção de ameaças avançadas persistentes, cujo grau de sofisticação permite passar despercebido pelas barreiras de segurança tradicionais [32].

Os adversários não se limitam mais a atores individuais, surge um novo cenário em que organizações

altamente sofisticadas exploram vulnerabilidades de segurança desconhecidas publicamente (*zero day*) e empregam táticas avançadas para passarem despercebidos por sistemas tradicionais de segurança cibernética [15, 33]. Atacam pequenas, médias e grandes empresas, além de governos municipais, estaduais e federais, consequentemente, controles cibernéticos avançados ficam obsoletos rapidamente [33].

Como exemplo, a campanha lançada pelo grupo RedEcho, ligado a China, visando o setor de energia Indiano para cópia não autorizada de dados, cuja detecção, análise, correlação de dados, detecção dos padrões de ataque e medidas de mitigação duraram um período de dois anos [34].

Nesse contexto torna-se essencial o conhecimento das táticas e técnicas empregados pelos atores da ameaça. Assim surge a inteligência de ameaça cibernética para abordar esses desafios, principalmente os relacionados a resposta passiva e detecção de ameaças emergentes. A inteligência de ameaça cibernética, em conjunto com as técnicas tradicionais, além de produzir conhecimento sobre determinadas ameaças ganha força também através do compartilhamento dessas informações, dessa forma as organizações tendem a obter resultados mais imediatos.

### 2.1.3 Cenário de ameaças avançadas

A crescente dependência da tecnologia da informação mudou o cenário de ameaças enfrentado pelas empresas, pois atualmente seus ativos mais valiosos existem na forma de bits dentro de sua rede. Essa realidade leva ao desenvolvimento de novos termos e conceitos para definir as ameaças que são enfrentadas e como elas operam.

Os vetores de ataque também mudaram com foco no uso de ameaças polimórficas (software capaz de ocultar sua assinatura) e compostas, que exploram ataques sintáticos e semânticos contra vulnerabilidades técnicas e sociais, permitindo a execução de novos e sofisticados ataques.

#### 2.1.3.1 Ameaças polimórficas

São *malwares* com capacidade de mudar constantemente dificultando as defesas baseadas em assinaturas [35]. Apesar da mudança, a função essencial do código permanece a mesma. O polimorfismo é utilizado para dificultar a detecção por meio de defesas baseadas em assinaturas, forçando uma constante implantação de novas assinaturas nos dispositivos e sensores de detecção. Esse ciclo favorece o atacante, que está sempre um passo à frente [15].

#### 2.1.3.2 Ameaças de dia zero

São ameaças que exploram vulnerabilidades de sistemas operacionais ou aplicações desconhecidas publicamente. Esses ataques podem passar despercebidos por longos períodos de tempo até que a vulnerabilidade seja identificada publicamente e corrigida [35]. Normalmente os desenvolvedores tomam conhecimento da existência de vulnerabilidades após a ocorrência de um ataque.

#### 2.1.3.3 Ameaças compostas

Os ataques podem ser classificados em sintáticos ou semânticos [35]. Ataques sintáticos exploram vulnerabilidades técnicas de software ou hardware, enquanto os ataques semânticos exploram vulnerabilidades sociais para obter informações pessoais [35].

Ameaças que empregam técnicas tanto de ataque sintático quanto semântico são classificadas como compostas ou combinadas, exploram vulnerabilidades técnicas e sociais.

#### 2.1.3.4 Ameaças Persistentes Avançadas (*Advanced Persistent Threats* - APT)

Ameaça persistente avançada (ATP) é um ator de ameaça com grande especialização e altos recursos, que por meio de diversas ferramentas estabelece presença na infraestrutura de organizações alvo [36]. A principal característica do APT é a persistência para manter-se na infraestrutura atacada, buscando alternativas frente aos recursos de segurança existentes [37]. São capazes de promover ataques sofisticados baseados em ameaças multivetoriais e multiestágios, com finalidade principal de manter comunicação com o meio externo e se manter oculto aos dispositivos de segurança [35, 38].

APTs empregam técnicas variadas para que o ataque passe despercebido, embora, exista uma sequência de etapas bem definidas, as estratégias em cada etapa são constantemente alteradas, assim como adotam campanhas de longa duração, dessa forma as etapas não ficam evidentes diminuindo a capacidade de detecção [39, 40, 41, 42].

Sob o patrocínio de um Estado ou entidade privada, utilizam recursos diversos e significativos para atacar um alvo estrategicamente valioso. Esse novo ator pode ser diferenciado de outros empreendimentos criminosos por quatro características principais: objetivos específicos e claros; alta organização e altos recursos; maior duração dos ataques; e alto grau de furtividade [20].

Nas ameaças tradicionais os ataques ocorrem por curto período de tempo, não possuem alvos específicos e tem abordagem simples, com poucas tentativas para burlar barreiras de segurança, são executados, majoritariamente, por indivíduos e não por grupos e contra sistemas individuais [43]. Enquanto, ameaças avançadas tem características distintas, como emprego de diversos meios de propagação, uso técnicas de evasão e ofuscação e divisão em vários estágios e vetores.

As ameaças avançadas são realizadas por grupos altamente organizados e a incidência têm aumentado ao longo dos anos [44], contudo, as estratégias de defesa tradicionais não são suficientes para conter esse avanço, por isso a importância de conhecer as táticas e técnicas envolvidas nesse processo, a fim de criar alternativas que sejam capazes de contornar esse cenário.

### 2.1.4 Inteligência

Inteligência: do latim *"intelligentia"*, de *"intelligere"*, que significa: entender, proveniente de *"inter"* (entre) + *"legere"* (escolher). Indica a capacidade de aprender, entender, raciocinar, interpretar e pensar de forma lógica [45, 46]. Essa capacidade resulta de elementos constitutivos que se relacionam na forma de processo, no qual, a partir de dados brutos obtém-se informação, que serve de base para o conhecimento

e por fim inteligência. Porém Inteligência também pode representar o produto resultante do processo de construção do conhecimento [47, 48], o qual se refere ao valor agregado pela análise e interpretação das informações dentro de contextos específicos, gerando oportunidades que se traduzem em ações estratégicas, operacionais ou técnicas [49].

Contudo, existem outras definições, dependendo do contexto onde o termo inteligência é aplicado seja no escopo acadêmico, psicológico, governamental ou militar [50].

A inteligência como produto refere-se ao resultado final do processo de produção do conhecimento que resulta em informações relevantes para a tomada de decisões estratégicas [51]. É o conhecimento obtido a partir da análise de dados, que é transformado em informações significativas e úteis para apoiar ações e decisões informadas. O produto de inteligência geralmente é apresentado em relatórios, *briefings*, *dashboards* ou outras formas de comunicação que apresentam as descobertas, análises e recomendações para os tomadores de decisão [51].

A inteligência como organização refere-se a uma estrutura ou entidade dedicada à produção contínua de inteligência [51]. Pode ser uma unidade dentro de uma empresa, um departamento de inteligência governamental, uma agência de segurança ou qualquer outra entidade que tenha a finalidade de processar informações relevantes para um determinado objetivo [51]. Essas organizações geralmente possuem especialistas, analistas e sistemas específicos para coleta, análise e disseminação de inteligência [51].

A inteligência como processo refere-se à sequência sistemática de atividades e etapas realizadas para transformar dados brutos em informações valiosas e acionáveis [51]. Esse processo envolve a identificação de requisitos de inteligência, coleta de dados relevantes de diversas fontes, análise e interpretação desses dados, produção de conhecimento e, finalmente, a disseminação desse conhecimento para os destinatários adequados [51]. O processo de inteligência segue metodologias e técnicas específicas para garantir a precisão, relevância e confiabilidade das informações produzidas [51].

Essas definições estão interligadas e se complementam. A inteligência como produto é o resultado do processo de inteligência realizado por uma organização especializada nessa área. A organização de inteligência emprega o processo para produzir o produto final, que é utilizado para apoiar a tomada de decisões estratégicas.

O produto da inteligência tem como principal função a tomada de decisão, dessa forma, a análise de informações deve fornecer base útil para criação de estimativas e previsões [52], normalmente sobre um fator outrora desconhecido capaz de causar danos, cuja gravidade depende do grau e da probabilidade da ameaça, que pode ser reduzida ou eliminada pela aquisição do conhecimento. Assim, a existência de ameaça é requisito importante na definição de inteligência, dado que sem ameaça, ou possibilidade de sua existência, não haveria necessidade dos processos de produção de inteligência [53].

### 2.1.5 Ciclo de Inteligência

O ciclo de inteligência é uma definição comumente empregada para o processo sistemático de obtenção do conhecimento [54], no qual várias partes são encadeadas sequencialmente numa ordem predefinida [55]. Suas fases e nomenclatura podem variar conforme a proposta do fluxo dos dados até o produto final

e da organização que o emprega. Processos que envolvem coleta, análise e uso de informações existem desde tempos muito antigos. Sun Tzu, na China, Chanakya, também conhecido como Kautilya, na Índia, ambos do século IV Antes de Cristo, o rei Davic IV, da Geórgia, no século 12, Francis Walsingham, na Inglaterra e George Washington, nos Estados Unidos, ambos no século 18, dentre outros, adotaram metodologias próprias para coleta, processamento e consumo de informações como meio para manter e expandir a segurança e o poder do Estado [52].

Embora metodologias peculiares sejam empregadas desde muito tempo, o ciclo de inteligência ganhou notoriedade após a segunda guerra mundial, quando evolui o conceito de atividade de inteligência, o modelo base e os aspectos relevantes da coleta e análise de informações [52].

Contudo, grande parte dos estudos nessa área consideram Kent e Platt (1967) os pioneiros para tornar a produção de inteligência mais técnica, com adoção de procedimentos comuns [49], a fim de proporcionar maior confiança no compartilhamento de conhecimento entre organizações.

Neste trabalho [56] foi adotado o ciclo de inteligência de cinco fases:

- **Direção e Planejamento** envolve determinar o que deve ser monitorado e analisado, assim como a lista de requisitos e preparação do plano de coleta. Envolve estabelecer objetivos e metas, identificar as necessidades e definir as fontes de dados. Passando por identificação de áreas de interesse estratégico e das fontes de informação relevantes.
- **Coleta:** obtenção de informações brutas com emprego de diversas fontes e vários tipos de coleta, que sejam relevantes para responder ou complementar os aspectos essências a conhecer.
- **Processamento:** refinamento e uso primário das informações. Os dados e informações são organizados, triados e tratados para torná-los úteis e fáceis de serem compreendidos. A fim de verificar a credibilidade do dado, realiza-se a avaliação da fonte, quanto a autenticidade, confiança e competência, e dos dados, quanto semelhança, coerência e compatibilidade.
- **Análise:** os dados processados são traduzidos em produto informacional acabado na forma de resumos, previsões e resultados de medidas informativas específicas. Ocorre a interpretação das informações coletadas, a busca de relações e padrões, e a produção de conclusão e recomendações.
- **Implantação e disseminação:** a inteligência gerada é compartilhada com as partes interessadas de forma clara e precisa. O produto acabado é fornecido aos consumidores dos níveis estratégico, operacional, tático e técnico com detalhamento compatível com suas funções.

### 2.1.6 Dado, Informação, Conhecimento e Inteligência

A inteligência é resultado do processo de obtenção do conhecimento, que tem como insumo básico o dado. É importante conhecer as conexões de cada passo até alcançar a inteligência.

Os dados são símbolos que isoladamente não tem significado, dessa forma se não puderem ser relacionados, não terão propósito específico. O dado por si só não consegue explicar um evento, contudo, são importantes para criar informações [57, 58].

A informação surge de relações obtidas entre os dados coletados, normalmente se traduzem na forma de respostas para perguntas como “Quem?”, “O quê?”, “Onde?” e “Quando?” [57]. A busca por informações visa explorar um contexto específico.

O conhecimento é resultado da interpretação de informações, e pode ser empregado para decisão e reação em determinadas situações. O conhecimento tem natureza dinâmica, uma vez que pode variar em função do conjunto de informações disponíveis, ao passo que a natureza da informação é estática. A interpretação de informações é uma prerrogativa de analistas humanos [59, 52], embora, o emprego crescente de aprendizado de máquina (*Machine Learnig* - ML), esse método tende a muitos falsos positivos [59].

Softwares podem coletar, cruzar, comparar e selecionar dados, mas não produzem inteligência, pois são desprovidos de intuição, bom censo e experiência, além da dificuldade de interpretação [60]. Ademais, um software não gera relatórios não estruturados com apontamentos precisos para tomada de decisão.

A inteligência, como produto, pode ser descrita como o uso do conhecimento para compreender, prever, prosperar e reconhecer ameaças e dessa forma reduzir as incertezas e fazer planos para o futuro. Enquanto o conhecimento tem relação com o tempo atual, por meio da compreensão de eventos passados e presentes, a inteligência procura antecipar eventos futuros, estando também ligada a redução de risco, é o cerne do processo de tomada de decisão.

O refinamento progressivo de dados e informações tem impacto no volume de dados ao longo do processo, que inicia com grande volume e baixa relevância e ao longo do processo por meio de avaliação, busca por correlações, análises e interpretações, termina com baixo volume, porém capaz de ser empregado para tomada de decisões, conforme Figura 2.2.

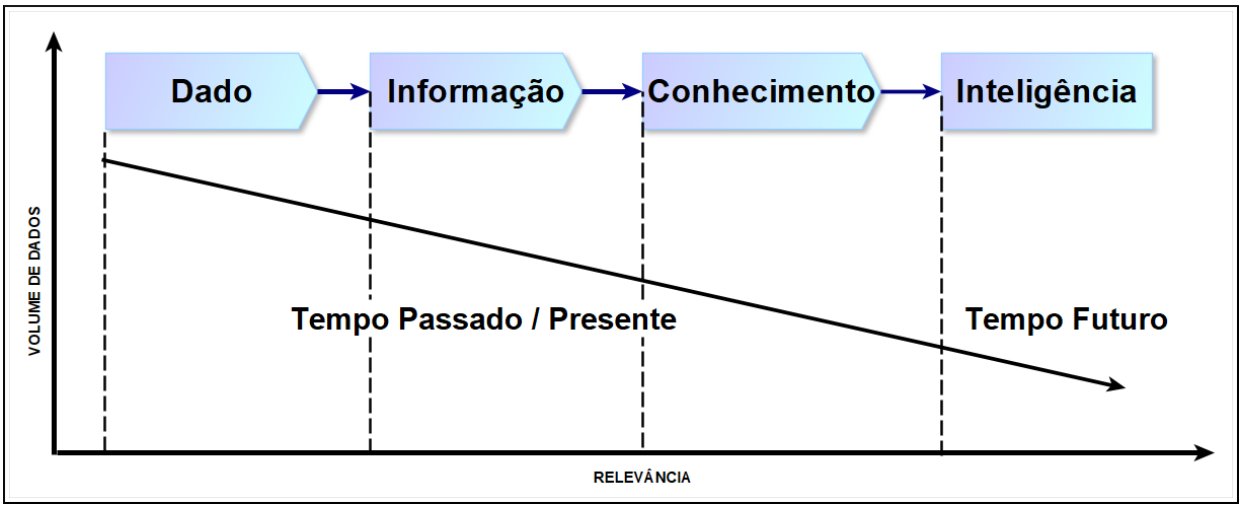


Figura 2.2: Do Dado à Inteligência - Relação com o tempo, Volume e Relevância

Ao longo do ciclo de inteligência é possível estabelecer claramente a relação entre dados brutos, informação, conhecimento e inteligência. Dados brutos é uma massa de registros que quando analisados isoladamente são limitados e não agregam valor capaz de subsidiar processos de tomada de decisão. Entretanto, essa massa de dados brutos, quando coletados e processados de forma adequada se tornam informações e tem maior probabilidade de se tornarem uteis. Informações relacionadas com outras informações

ou analisadas à luz da experiência passada de analistas geram compreensão da informação, conhecimento. Inteligência é a forma como o conhecimento é empregado no formato de avaliações que permitem a antecipação ou previsão de situações ou circunstâncias futuras.

### 2.1.7 Inteligência de Ameaça Cibernética

A inteligência de ameaça cibernética faz parte do domínio da segurança cibernética, que se concentra no campo geral relacionado a proteger sistemas e dados, enquanto inteligência cibernética e inteligência de ameaça cibernética são domínios mais específicos destinados a fornecer informações sobre ameaças emergentes.

Segurança cibernética, cibersegurança, ou do inglês, *cybersecurity*, refere-se às ações de segurança ou medidas para garantir um estado de inviolabilidade, confidencialidade, integridade e disponibilidade de recursos computacionais [1]. É um conjunto de controles que integra tecnologias, pessoas e processos [61] para proteger sistemas, redes, dispositivos e informações digitais, além de assegurar a continuidade dos serviços em caso de incidentes.

Inteligência Cibernética (*Cyber intelligence*) compreende ações de aquisição, processamento, análise e disseminação de informações que identifiquem, rastreiem (técnicas, táticas e procedimentos) e prevejam ameaças, riscos e oportunidades no domínio cibernético para oferecer cursos de ação que aprimorem os caminhos para tomada de decisões [48]. A Inteligência cibernética fornece um compreensão ampla do cenário cibernético de ameaças de uma organização [13]. Lee [62] divide a inteligência cibernética nas seguintes subdisciplinas: inteligência de ameaça cibernética, operações de coleta de inteligência cibernética e contra inteligência cibernética. Portanto Inteligência Cibernética é mais abrangente que Inteligência de Ameaça cibernética.

Quanto à Inteligência de Ameaça Cibernética (*Cyber Threat Intelligence*), existem algumas variações para sua definição, todas giram em torno do conhecimento sobre ameaça e as ações derivadas desse conhecimento [63, 64, 35]. Wiem Tounsi et al. [35], por exemplo, define Inteligência de Ameaça Cibernética (CTI) como o conhecimento baseado na análise de rastros que representam a ameaça, capaz de se traduzir em tomada de decisão. Enquanto Zibak et al. [65] afirma que em diversas pesquisas científicas a definição de inteligência de ameaça cibernética e outros termos relacionados ao assunto são usados de forma inconsistente.

Inteligência de ameaças é uma avaliação prospectiva baseada em evidências, incluindo contexto, implicações e conselhos orientados para a ação sobre uma ameaça ou vulnerabilidade de um sistema ou rede. Essa inteligência é produzida por meio da aplicação de métodos cognitivos individuais ou coletivos, e pode ser usada para informar decisões sobre a resposta a essa ameaça ou vulnerabilidade [65].

O analista exerce papel fundamental na verificação, análise, interpretação e definição de hipóteses, uma vez que a qualidade da Inteligência é influenciada pelo processo de produção, embora as pesquisas apontem para falta de implementação de um processo formal [24].

Entre os desafios enfrentados estão a heterogeneidade e o grande volume de dados de ameaças, que dificultam a identificação dos dados realmente relevantes [66, 15]. Assim originou-se um problema de

quantidade sobre qualidade [35]. Outro desafio é a limitação da plataformas de inteligência de ameaças, (*Threat Intelligence Platform* - TIP) [20], tais como gerenciamento ineficaz de informações de ameaça, compartilhamento de grande volume de informações com baixa qualidade, falta de transparência na informação das fontes e capacidade analítica avançada limitada [67, 24, 23].

Diversos trabalhos dividem a Inteligência de Ameaça Cibernética nos domínios técnico, tático, operacional e estratégico [68, 69, 62, 61, 35, 15]. Esses domínios na sequencia apresentada compreendem níveis de inteligência diretamente proporcionais ao emprego ao longo do tempo, quanto mais próximo do nível estratégico, maior a validade da informação a longo prazo.

- *Inteligência de ameaças técnica:* suportam atividades de segurança que podem ser automatizadas em infraestruturas de defesa. Normalmente as informações empregadas tem origem em Indicadores de comprometimento, (*Indicators of Compromisse* - IoC) [61]. É a mais abordada nos diversos estudos, sendo consumida por infraestruturas de segurança cibernética, alimenta dispositivos como firewalls, sistema de detecção de intrusão (*intrusion detection system* - IDS), sistema de prevenção de intrusão (*intrisuon prevention system* - IPS) ou dispositivos de filtragem de e-mail. Normalmente é baseada em indicadores de comprometimento observados em eventos passados.
- **Inteligência de ameaças tática:** Compreende o estudo das táticas, técnicas e procedimentos associados aos atores das ameaças. São detalhes sobre o modus operandi, ferramentas e capacidades.
- **Inteligência de ameaças operacional:** São informações sobre ataques eminentes, envolve conhecimento sobre identificação dos atores da ameaça e suas capacidades, além de como e quando irão atacar. Esse tipo de inteligência é o mais complexo de adquirido, uma vez que a coleta de dados para responder essas questões costumam estar disponíveis em fóruns privados.
- **Inteligência de ameaças estratégica:** Informações de caráter executivo, como situação geopolítica e atividades dos atores da ameaça, análise do risco, impacto financeiro e tendências de ataque. Geralmente na forma de relatórios próprios para humanos [13, 61]. Lida com conceitos como risco e probabilidade

A inteligência de ameaça cibernética visa reduzir a incerteza, seu principal objetivo é determinar fatos e formar conclusões e previsões confiáveis para auxiliar na tomada de decisões, além de amparar processos operacionais de detecção, prevenção e resposta a incidentes [70].

### 2.1.8 Plataforma de Inteligência de Ameaça

Com a evolução da internet a capacidade de coleta de dados teve impacto importante nas etapas de processamento e análise do ciclo de inteligência. Com a expansão do volume de dados e a diversificação das fontes aumenta o desafio de separar dados que podem ser uteis, isoladamente ou através de correlações com outros dados, daqueles que não agregam valor ao contexto em que estão inseridos. Esses fluxos de dados constituem recursos valiosos para obter vantagens operacionais, desde que o armazenamento e gerenciamento sejam adequados. O desafio está na estruturação, processamento e análise desse volume massivo de dados a fim de obter inteligência significativa para atender aos requisitos de precisão, clareza,

oportunidade, relevância e acionabilidade [57, 59], além da falta de mecanismos para avaliação das fontes e dados.

Para contornar esses desafios as organizações têm adotado ferramentas, conhecidas como Plataforma de Inteligência de Ameaças, que gerenciam o fluxo de informações, as convertem em conhecimento [15] e facilitam o compartilhamento [71]. Contudo, a maioria das plataformas não contemplam o ciclo completo de inteligência e servem como agregadores de conteúdo com recursos de análise limitado [72].

Silva et al. [6] propõe uma metodologia para avaliação de TIP de código aberto. O resultado aponta algumas TIP satisfatórias com capacidade de otimizar o processo de CTI. A seleção varia em função do contexto e objetivos pretendidos. Considerando os objetivos distintos de cada plataforma, é possível concluir que não existe uma solução completa. Neste contexto, as TIP de código aberto mais completas e flexíveis foram MISP e OpenCTI [6].

Diante disso surge a hipótese de que grande parte dos desafios observados decorrem da inexistência de uma metodologia que direcione para adoção de requisitos mínimos. Ainda que diversos autores estejam pesquisando o tema, não há consenso sobre os requisitos, tampouco, aderência ao ciclo de inteligência.

### 2.1.9 Consciência Situacional

Consciência situacional é um campo muito vasto, estudos sobre o tema surgiram na década de 1980 inicialmente focados para situações militares e de aviação, mas podem ser aplicados em qualquer área de conhecimento, incluindo segurança cibernética. Um dos desafios identificados a partir de trabalhos correlatos diz respeito a ontologia que varia conforme as particularidades de cada situação [73].

Uma ontologia determina as classes envolvidas em situações e suas dependências lógicas. É a representação explícita e formal do conhecimento sobre um domínio [74] e engloba: Tipos de entidades existentes no domínio; Propriedade das entidades; Relações entre entidades; Processos e eventos nos quais as entidades estão envolvidas; e Regularidades estatísticas que caracterizam o domínio. A ontologia de um determinado domínio está sujeita a desafios como: Conhecimento inconclusivo, ambíguo, incompleto, não confiável e dissonante; e Incerteza sobre quaisquer dos conhecimentos contidos no domínio.

Com relação à ontologia, entidade é qualquer conceito que pode ser descrito e fundamentado dentro do domínio de aplicação. No domínio de segurança cibernética, entidade engloba o conjunto de ativos, eventos, ameaças, vulnerabilidades, gestão de identidades e autenticação, criptografia, políticas de segurança, gestão de incidentes, gestão de risco, dentre outros fatores que afetam de forma positiva ou negativa os processos de negócio da organização.

Pesquisas sobre consciência situacional apresentam diversas definições. Para Devlin é uma parte estruturada da realidade que é discriminada por algum agente. No modelo JDL é a estimativa e previsão de estruturas de partes da realidade, envolve agregação de relacionamentos entre entidades e as mudanças de estados decorrentes destes relacionamentos [74]. A definição mais habitual refere-se a proposta de Endsley, “Consciência situacional é a percepção dos elementos dentro de um volume de tempo e espaço, a compreensão do seu significado e a projeção de seu estado em um futuro próximo” [75, 76].

Estudos indicam que o modelo de consciência situacional mais aceito é o de Endsley [77], o qual

é adotado nessa pesquisa. Outros modelos menos abordados nas pesquisas cientificas são: Modelo de Beringer e Hancok; Modelo Carroll, Modelo JDL Data Fusion; Teoria da Situação e Lógica de Barwise, Perry e Devlin; Modelo de Smith e Hancock; Modelo de Bedny e Meister; Iniciativa Fusion for Situation Awareness da Organização Australiana de Ciência e Tecnologia de Defesa (DSTO), liderada por Lampert.

A consciência situacional, segundo Endsley, divide-se em níveis progressivos que variam da percepção básica de dados importantes, interpretação e combinação de dados para gerar conhecimento, e capacidade de prever eventos futuros e suas implicações. Envolve desafios técnicos e cognitivos [78], estudos indicam que a consciência situacional é um atributo direcionado para humanos, tem natureza complexa e multifacetada e surge de processos cognitivos que são renovados continuamente [75].

Primeiro nível: Percepção dos elementos, concerne perceber elementos relevantes do ambiente, seus atributos e estados, ou seja, registro da presença, características e atividades dos objetos que compõem o cenário que se deseja tomar consciência. No campo da cibernética, envolve o emprego de sensores para coleta de dados.

Segundo nível: Compreensão da situação atual, refere-se a compreender o significado dos elementos percebidos, implica entender as relações entre si e com a situação observada. Abrange o armazenamento, a interpretação e a produção de informações e combinação de informações para formação de conhecimento.

Terceiro nível: projeção de estados dos elementos em futuro próximo. Com base no conhecimento produzido e no entendimento do impacto de cada elemento frente a situação observada, poder prever estados futuros e suas consequências. Requer que os níveis anteriores sejam bem executados, além de experiência no domínio. Os níveis um e dois podem ser automatizados, porém o terceiro nível sugere o emprego de modelos mentais do analista humano. Em outros modelos, como o JDL, existe uma fase relacionada a decisão e tomada de ações decorrentes da avaliação da situação, porém no modelo proposto por Endsley a consciência da situação é subsídio para decisão e ações futuras, mas estes não fazem parte do processo de conscientização da situação.

A consciência situacional pode ser empregada como ponto de partida para segurança cibernética, pois envolve a compreensão abrangente do ambiente operacional, incluindo as ameaças, vulnerabilidades, ativos de informação e atividades maliciosas. Contribui para identificar possíveis ameaças, vulnerabilidades e incidentes de segurança, além de identificar padrões, correlações e tendências que possam indicar uma violação de segurança. Contudo os analistas de segurança devem empregar ferramentas complementares, uma vez que a consciência situacional sofre forte influência de fatores individuais, relacionados à experiência do analista, e também de fatores dos sistemas envolvidos, esses aspectos podem ser observados na Figura 2.3.

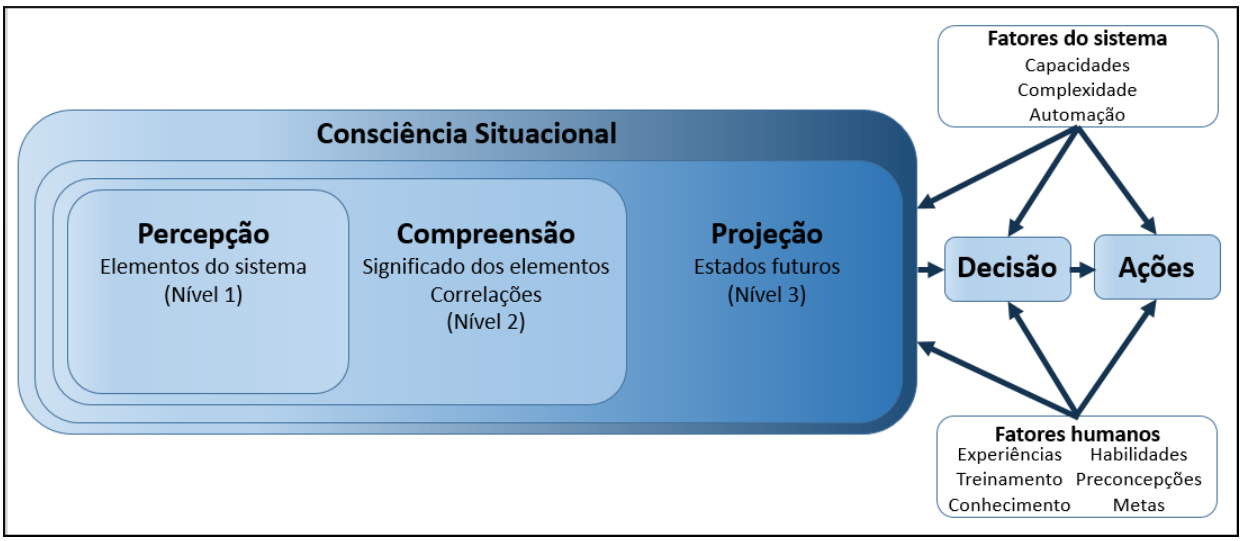


Figura 2.3: Modelo de Consciência Situacional - Adaptado [2]

### 2.1.10 Estrutura Analítica do Ataque

O principal propósito de um APT é obter acesso não detectado na infraestrutura de uma organização por um período prolongado de tempo. Os ataques são planejados com alto grau de personalização e sofisticação para alvos específicos e envolvem vários estágios e diferentes técnicas, para isso empregam tempo e recursos significativos pesquisando e identificando vulnerabilidades da organização.

O estudo da estrutura analítica do APT contribui para a consciência situacional por meio da percepção de elementos que possam indicar a fase na qual um ataque de encontra, através das características desses elementos é possível revelar as táticas e compreender as técnicas e procedimentos empregados pelos atacantes e dessa forma decidir sobre ações de defesa mais eficazes [26, 71]. Também permite que o analista investigue a progressão do invasor, interrompa ou atrase seu avanço.

Existem diversos estudos que abordam diferentes estruturas dos ataques APT, com modelos que caracterizam as fases do ataque [15, 35, 79, 80, 43]. Os modelos dividem o ataque em fases que compreendem objetivos intermediários, tais como: reconhecimento, infiltração, armamento, entrega, expansão, exploração, instalação, comando e controle, ação em objetivos e extração. *Kill Chain* é um modelo desenvolvido pela Lockheed Martin em 2011, empregado para dividir um ataque complexo em fases consecutivas, conforme Figura 2.4, permitindo que o analista aborde cada fase separadamente, é o *framework* mais conhecido e contempla as seguintes fases:

1. **Reconhecimento:** Coleta e compilação de informações, que pode ser ativa ou passiva. No reconhecimento passivo não há interação com o alvo, enquanto no reconhecimento ativo o atacante interage com o alvo para obtenção de dados.

2. **Armamento:** Etapa de criação do ataque, com base nas informações do reconhecimento o atacante seleciona, customiza ou cria vetores, códigos maliciosos, que serão utilizados para obter acesso não autorizado à infraestrutura do alvo.

3. **Entrega ou transporte:** Ainda com base nas informações do reconhecimento, o atacante elabora estratégia para infiltrar o vetor na infraestrutura do alvo. As formas mais comuns de entrega são e-mail, acesso web e *pendrive*, ou via cadeia de suprimento.

4. **Exploração:** Acionamento do vetor para execução do código malicioso que explora vulnerabilidades identificadas na fase de reconhecimento.

5. **Implantação ou instalação:** O *malware* é instalado no alvo, são explorados mecanismos de persistência.

6. **Comando e controle:** O *malware* estabelece um canal de comunicação com servidores remotos, assim o invasor tem capacidade de executar comandos diretamente no dispositivo comprometido.

7. **Ações finais:** O controle do dispositivo comprometido permite que o atacante atinja seus objetivos, por exemplo, extração de dados. Nessa etapa também pode ocorrer o movimento lateral e execução de técnicas de evasão, a fim de permanecer o maior tempo possível indetectável.

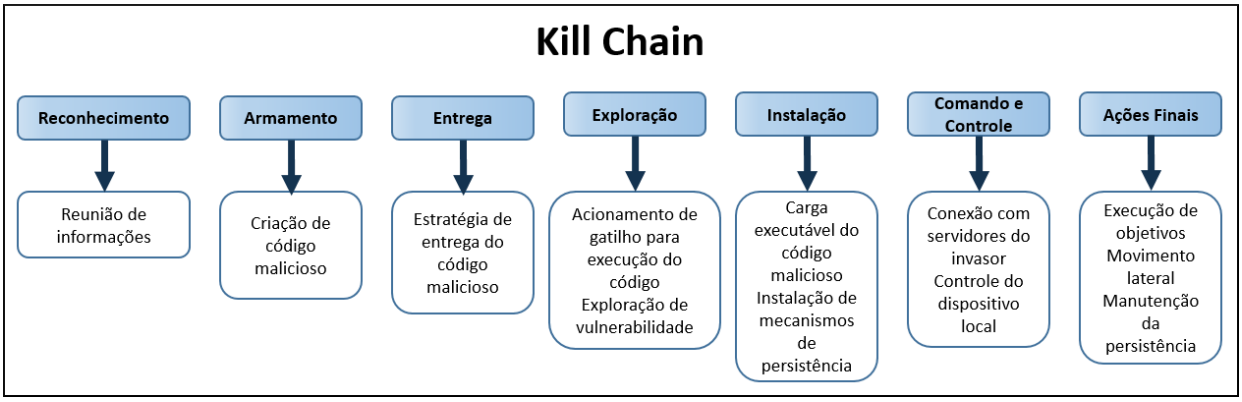


Figura 2.4: Kill Chain

No mesmo contexto o *framework Mitre Att&ck (Adversarial Tactics, Techniques, and Common Knowledge)* complementa o estudo da estrutura analítica dos ataques APT por meio do mapeamento do comportamento adversário, que é apresentado no formato de matriz contendo as táticas e técnicas empregadas ao longo do ciclo de vida do ataque, como apresentado na Figura 2.5. O emprego da matriz *Att&ck* é relevante, tendo em vista que descreve detalhadamente padrões de comportamento conhecidos dos atores da ameaça por meio das seguintes técnicas: reconhecimento, desenvolvimento de recursos, acesso inicial, execução, persistência, escalação de privilégio, evasão de defesa, acesso a credenciais, descoberta, movimento lateral, coleta, comando e controle, cópia de dados não autorizada e impacto. Cada tática abrange um conjunto de técnicas que somadas totalizam 227, essa quantidade de técnicas corresponde a versão 13, lançada em abril de 2023, eventualmente surgem novas técnicas no lançamento de nova versão da matriz *Att&ck*.

O primeiro modelo *Att&ck* foi criado em 2013 focado no ambiente Windows, em 2015, a matriz original foi expandida e passou a ter 96 técnicas distribuídas em 9 táticas. Em 2017, foram contempladas outras plataformas, como macOS, Linux, Azure AD, Office 365, Containers, entre outras [81].

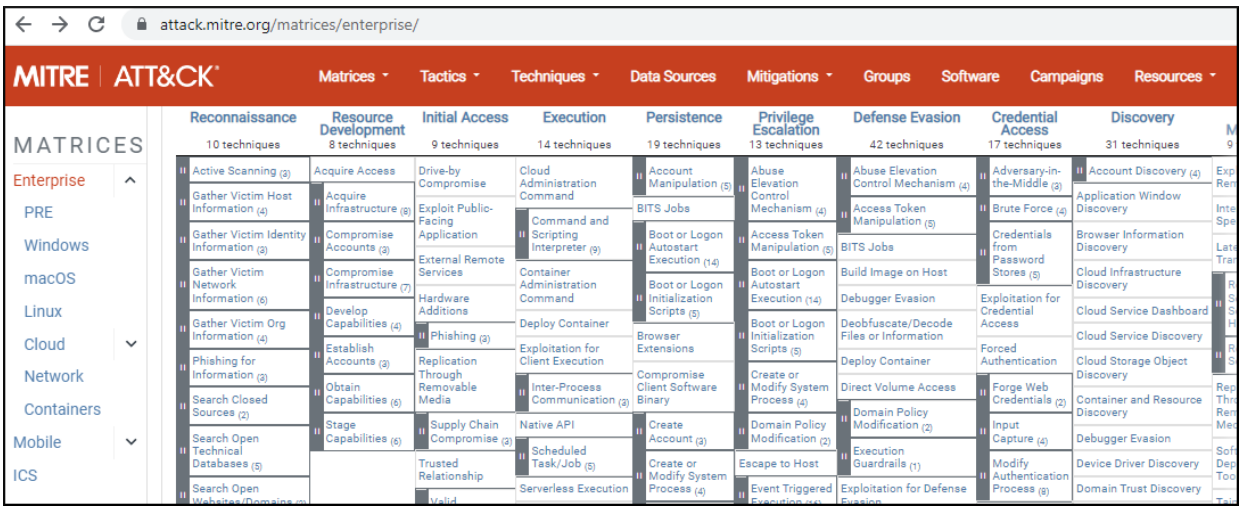


Figura 2.5: Framework Att&ck [3]

### 2.1.11 Enriquecimento

Grande parte da inteligência cibernética permanece restrita à organização que a produziu, e a maioria das informações compartilhadas é na forma não estruturada [24, 34]. O principal desafio é lidar com o volume diário de novos dados, cuja forma mais comum é o Indicador de Comprometimento (IoC), que frequentemente não indica um comprometimento real devido à sua volatilidade [24, 34]. Além disso, um IoC isoladamente não possui valor significativo e, portanto, não pode ser considerado como Inteligência de Ameaça Cibernética (CTI), requerendo avaliação para verificar possíveis relacionamentos [24].

A Pirâmide da Dor (Pyramid of Pain - PoP), que foi introduzida por Bianco em 2013 [4], fornece uma melhor compreensão dos níveis técnico, tático, operacional e estratégico da Inteligência de Ameaça Cibernética. As informações no nível inferior pertencem ao nível técnico e são compostas principalmente por IoCs, Indicadores de Ataque (IoA), evidências forenses e descrições técnicas [82]. Já as informações nos níveis superiores da pirâmide são mais difíceis de obter e estão relacionadas ao nível tático, descrevendo ferramentas e Táticas, Técnicas e Procedimentos (TTP) que oferecem contexto para a análise do ataque, bem como informações sobre os atores envolvidos, contribuindo para a completude da CTI [82].

As informações nos níveis operacional e estratégico resultam da análise de dados de alto nível, que têm o potencial de prever ataques iminentes e fornecer a capacidade de análise de cenários de ameaças prováveis [82].

A representação da PoP é ilustrada na Figura 2. Na base da pirâmide estão os dados mais facilmente obtidos e que têm menor impacto nas operações adversas. Conforme se avança em direção ao topo, a dificuldade e a complexidade de obtenção dos dados aumentam, porém a quantidade de informações de alto nível também cresce, resultando em maior completude das informações sobre uma determinada ameaça ou incidente. Vale ressaltar que os valores de *hash*, presentes na base da pirâmide, são considerados dados menos significativos [4]. Apesar de serem IoCs muito precisos, alterações irrelevantes em um arquivo podem resultar em um valor de *hash* completamente diferente [4].

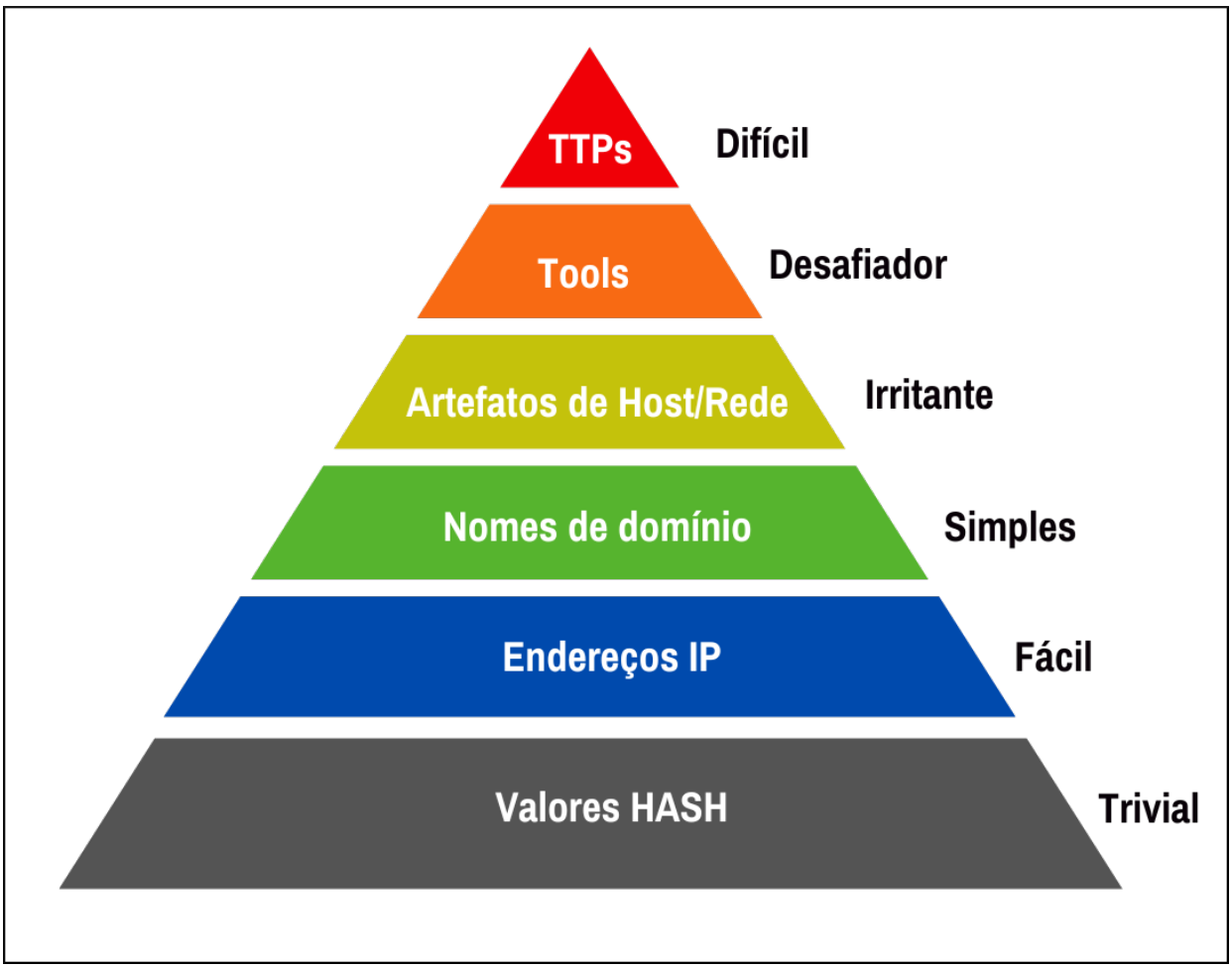


Figura 2.6: Pirâmide da Dor - Adaptado de [4]

Os endereços IP desempenham um papel fundamental nas conexões de rede, pois são facilmente identificáveis, embora também demandem pouco esforço para serem alterados. Quando o tráfego de um endereço IP associado a atividades maliciosas é bloqueado, um adversário avançado pode se recuperar facilmente, com pouco ou nenhum impacto em suas ações [4]. Na parte inferior da pirâmide, próxima à linha central, encontram-se os nomes de domínio, que são registrados em provedores de Sistema de Nomes de Domínio (Domain Name System - DNS) e geralmente são pagos [4]. No entanto, existem provedores de DNS com padrões negligentes de registro, e novos registros podem levar de uma a quarenta e oito horas para serem propagados por toda a internet, tornando-os um pouco mais difíceis de serem alterados do que os endereços IP [4].

Mais acima na pirâmide, ainda tocando a linha central, estão os artefatos de rede e host. Nesse nível, se uma organização detecta e responde adequadamente, o impacto negativo para o adversário é maior, pois isso força a adaptação do ataque [4]. O próximo nível, mais próximo do topo, é representado pelas ferramentas. A detecção das ferramentas utilizadas causa um impacto significativo nas ações do adversário, pois o obriga a gastar tempo desenvolvendo uma nova ferramenta [4]. No topo da pirâmide estão as TTP, que são os indicadores mais valiosos, mas também os mais complexos de serem identificados [4].

A utilização de processos adequados, aliada ao poder de automatização das Plataformas de Inteligência

de Ameaça (TIP), aumenta a capacidade de produção de CTI e contribui para aliviar a carga de trabalho dos analistas de segurança [83]. Dentre esses processos, o enriquecimento de dados tem como objetivo obter informações de contexto a partir de um conjunto de dados brutos aparentemente não relacionados, aumentando o valor da informação e transformando-a em conhecimento [84].

O método mais comum para obter conhecimento a partir de um dado específico é por meio do cruzamento de IoCs provenientes de diferentes fontes externas [20, 85, 86, 13], aproveitando a capacidade de enriquecimento das diversas comunidades que disponibilizam esses dados [20].

Algumas TIPs possuem a facilidade de integrar serviços de terceiros para agregar valor aos dados coletados. Um exemplo é a plataforma MISP, uma das mais completas entre as soluções de código aberto, que possui integração com diversas ferramentas de enriquecimento, incluindo aquelas que não são de código aberto ou cujas versões gratuitas impõem limitações que inviabilizam o uso em larga escala.

Além disso, é possível melhorar a correlação de dados provenientes de várias fontes, incluindo dados coletados internamente pela própria organização [87, 88]. Esse cruzamento permite identificar a relevância e prioridade dos dados resultantes na forma de IoCs, além de proporcionar uma conscientização situacional por meio de contextos adicionais [87, 88, 89].

Através do enriquecimento de dados, é possível contribuir com três aspectos que influenciam a qualidade da CTI:

- **Relevância:** à medida que aumenta a relação entre eventos externos e internos, maior é a relevância das informações que fazem sentido para a organização;
- **Precisão:** quando os analistas de segurança adquirem conscientização situacional por meio do entendimento dos contextos, suportados pelo enriquecimento dos dados, a resposta a um incidente pode ser aprimorada;
- **Completude:** o enriquecimento de dados produz informações mais abrangentes, aumentando a capacidade de descrever um incidente de forma abrangente.

No entanto, é importante ressaltar que muitas abordagens esperam encontrar contexto a partir de dados brutos [20, 65]. Contudo, do ponto de vista do ciclo de inteligência, os dados precisam ser organizados de forma a fornecer respostas que complementem um contexto predefinido [87, 88]. Sem contexto, não existem elementos necessários para apoiar a tomada de decisão. Sem ação, a CTI não tem impacto e se mostra inútil, sobrecarregando ainda mais os analistas de segurança sem agregar inteligência acionável.

Os dados que podem servir como fontes potenciais de CTI vêm em diversas variedades, sendo os Indicadores de Comprometimento a forma mais comum [24]. Esses IoCs são artefatos, como endereços IP, nomes de domínio ou *hashes* de arquivo, que estão relacionados a atividades maliciosas. Os IoCs coletados são comparados com os dados da organização e, se houver correspondência, indicam um possível comprometimento. No entanto, é importante ressaltar que os IoCs não indicam um comprometimento real, pois podem gerar falsos positivos [24]. Por exemplo, um endereço IP pertencente à infraestrutura de nuvem, anteriormente utilizado por um agente malicioso, pode estar sendo utilizado posteriormente para fins benignos por outra entidade [4]. Em essência, os IoCs não possuem valor de inteligência por si só, pois precisam ser correlacionados com os logs da infraestrutura de rede. Portanto, não devem ser considerados

CTI, uma vez que não representam um produto de inteligência acabado [24]. Embora muitos autores se refiram aos IoCs como CTI, é necessário avaliá-los de forma adequada [24].

## 2.2 TRABALHOS CORRELATOS

### 2.2.1 Referencial Teórico

A base de pesquisa resultou de fontes acadêmicas como google scholar (https://scholar.google.com.br), portal de periódicos da CAPES (https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br), IEEE Xplore (https://ieeexplore-ieee-org.ez54.periodicos.capes.gov.br/Xplore/guesthome.jsp), Springer Link - (https://link-springer-com.ez54.periodicos.capes.gov.br) e ACM Digital Library (https://dl-acm-org.ez54.periodicos.capes.gov.br/) por meio de palavras chaves como *"cyber security", "threat intelligence platform", "cyber threat intelligence", "advanced persistente threat", "cyber intelligence quality", "APT", "kill chain", "situational awareness", "intelligence cycle"*, "inteligência de ameaça cibernética", "cadeia da morte", "consciência situacional", "ameaça persistente avançada", "ciclo de inteligência", "segurança cibernética", "plataforma de inteligência de ameaça" e "qualidade da inteligência cibernética". Por meio da base de periódicos da CAPES foi possível obter acesso a bases com conteúdo ofertado para venda. Assim, exceto o conteúdo dessas bases, todo o restante foi *Opensource*.

Inicialmente, priorizou-se trabalhos publicados nos últimos cinco anos, mas alguns trabalhos altamente referenciados, embora não atendessem a esse critério, foram incluídos quando estavam disponíveis gratuitamente. Como a busca específica sobre o tema "ciclo de inteligência"resultou em poucos estudos recentes, o filtro de data foi expandido. Além disso, foram considerados trabalhos com alto índice de citações.

Em seguida, realizou-se a avaliação dos resumos dos trabalhos pré-selecionados para verificar sua relevância ao contexto de inteligência de ameaça cibernética, especialmente em relação à qualidade. Essa análise resultou na seleção de 144 trabalhos científicos e 40 relatórios e pesquisas de instituições conceituadas na área de segurança cibernética. Alguns trabalhos de maior interesse foram identificados empiricamente e, para aprofundar a pesquisa, foram revisadas suas citações, o que ocasionalmente levou a incluir mais trabalhos relevantes.

Adicionalmente, buscas foram realizadas em momentos oportunos para complementar os conceitos relacionados. Cabe destacar que nem todos os trabalhos selecionados foram efetivamente utilizados, pois foram evitados aqueles que não apresentavam evidências de revisão acadêmica ou que não contribuíram para a questão central da pesquisa.

### 2.2.2 Metodologia

A fim de obter respostas e resultados relacionados à pergunta central deste estudo, "Como melhorar a qualidade da Inteligência de Ameaça Cibernética, foi adotada a abordagem qualitativa. Essa abordagem busca compreender os motivos e interpretar a relação dos elementos relevantes que afetam a qualidade da Inteligência de Ameaça Cibernética. A natureza aplicada do estudo visa gerar novos conhecimentos focados na mitigação do problema da baixa qualidade da CTI produzida, explorando os fatores que contribuem

para solução do problema por meio de pesquisa bibliográfica.

Após identificar a literatura relevante nos principais periódicos e anais de conferências, foi realizada uma revisão manual para abordar deficiências identificadas na literatura em relação aos atributos que mais impactam a qualidade da CTI. Estudos com propostas de *frameworks* e metodologias foram explorados para verificar o estado da arte. Essa etapa revelou detalhes importantes e validou a hipótese de que a qualidade da inteligência de ameaça cibernética está fortemente relacionada à sua relevância, precisão, completude e oportunidade. Também foi constatado que muitos *frameworks* e metodologias disponíveis são baseados nos processos das Plataformas de Compartilhamento de Inteligência e tendem a negligenciar a fase de direção e planejamento.

Na primeira fase deste estudo [56], foi apresentado um caso de uso com foco na fase de análise da CTI. Essa análise abordou principalmente a completude, que foi mensurada utilizando o modelo 5W3H, embora os requisitos de inteligência tenham sido estabelecidos de forma hipotética.

Uma vez que as questões de inteligência foram definidas hipoteticamente, o próximo passo foi uma tentativa de simular a coleta de dados internos de uma organização, essa abordagem não obteve sucesso. O objetivo era simular um ambiente de infraestrutura de rede de uma organização, envolvendo alertas e *logs* de dispositivos como IDS, *firewall*, concentradores de *logs*, entre outros. No entanto, os dados encontrados se limitaram principalmente a fluxos de rede contendo amostras de *malware*, não representando adequadamente o cenário desejado.

Diante dessa situação, a alternativa adotada foi iniciar um exercício de implementação de inteligência de ameaça em uma organização real. Nesse momento, ficou evidente a falta de uma metodologia consolidada para guiar as atividades. Portanto, optou-se por um realinhamento da pesquisa, visando explorar de forma mais detalhada as atividades da fase de direção e planejamento do ciclo de inteligência de ameaças cibernéticas.

Não há consenso sobre as características que indicam a qualidade da informação no âmbito da CTI, no entanto, quatro características estão entre as mais citadas [20, 65, 90]:

- **Oportunidade:** está relacionada com a origem de um evento e o tempo de reação ou uso de determinada informação;
- **Relevância:** indica a relação da informação com os ativos de serviços e de rede da organização;
- **Precisão:** mede o quanto a informação permite melhorar a resposta a um incidente e;
- **Completude:** indica a capacidade de a informação descrever um incidente.

Há evidências conclusivas que informações sobre ameaças imprecisas, incompletas ou desatualizadas são um desafio importante [20, 85, 15]. Garantir a qualidade do CTI em todo o processo de colaboração é crucial para seu sucesso. A troca e a utilização de informações significativas sobre ameaças dependem da medição e garantia de sua qualidade. Esta necessidade é reforçada ao verificar que a qualidade da informação compartilhada tem um impacto no tempo necessário para responder a um incidente [91].

Estudos apontam a falta de um processo definido, além de não considerar o ciclo de inteligência [17, 15], entretanto, há estudos que apontam a necessidade da implementação do ciclo de inteligência

no processo de obtenção de CTI [6], porém não foram identificados estudos que incorporem em seu escopo o ciclo de inteligência [17]. Uma metodologia bem definida ajuda a estabelecer a credibilidade e confiança nas análises de ameaças cibernéticas à medida que padroniza processos e táticas.

Embora, o esforço para empregar o ciclo de produção de inteligência, poucas fases são suportadas pelas TIP [92], especialmente a fase de planejamento [17]. Os poucos estudos que abordam o ciclo de inteligência em CTI, indicam a fase de planejamento como a etapa de seleção das fontes de dados [90, 84]. Entretanto, as contribuições da fase de planejamento vão muito além. Nessa fase se estabelece o escopo, os objetivos e prazos, além de parâmetros e técnicas que serão empregadas [49], além dos recursos que poderão ser utilizados. Com base nos aspectos conhecidos são verificadas as questões que necessitam de respostas [49], essa fase é determinante para a qualidade da CTI [93].

O ciclo de inteligência é um processo sistemático e iterativo com várias fases, amplamente adotado em diversas áreas de Inteligência, promove a consistência e a qualidade do conhecimento produzido, apoiando a tomada de decisão. Entretanto, poucas publicações específicas da CTI tratam o ciclo de Inteligência, e dessas não há consenso sobre qual a melhor estrutura de fases a ser adotada. Existem autores que propõem um ciclo de inteligência compreendendo as fases de requisitos, coleta, análise, produção e avaliação e outros cujo estudo está baseado nas fases, planejamento e direção, coleta, processamento e exploração, análise e produção, disseminação e integração [94].

As informações de fontes externas tem naturalmente ampla abrangência, assim é necessária a intervenção de um profissional para determinar a relevância para a organização [9, 20]. É importante que os profissionais de segurança identifiquem métricas e indicadores específicos para o domínio no qual a informação será usada. Daniel Schelette et al. [91], observa que a detecção e defesa contra ataques cibernéticos ocorre de maneira eficaz somente com CTI de alta qualidade. Primeiramente são propostas métricas para avaliar as dimensões de qualidade relevantes, em seguida cria uma extensão para uma ferramenta de CTI existente a fim de prover exibição visual da qualidade de um objeto. Em [87] é proposta uma pontuação para as informações de ameaças recebidas a fim de mensurar a pertinência da ameaça com relação aos ativos de rede e serviços da organização, dessa forma é possível avaliar o quanto é relevante. Entretanto, assim como a proposta de Daniel Schelette, a pontuação é atribuída baseada no conhecimento de um especialista, o que pode se tornar inviável para grande volume de dados.

Outro fator impactante é a eficácia duvidosa das Plataformas de Inteligência de Ameaça, tendo em vista limitações como baixa acurácia na extração de indicadores de comprometimento, dificuldade de em descrever o cenário completo de um evento e as relações entre IoC heterogêneos não são explorados [25, 23]. Para contornar esse desafio, analistas de CTI não devem apoiar todo o processo de produção de inteligência apenas nas TIPs. A chave é usar ferramentas complementares [6, 7], além de compor a base para análise com dados oriundos de sensores internos, isso demanda profissionais com conhecimento especializado e interdisciplinar.

Grande parte do compartilhamento de dados são IoC, que não são considerados inteligência, mas dados brutos que carecem de processamento e análise [24]. Além disso não há como garantir que os dados recebidos foram adequadamente analisados, também não há mecanismos para rastrear cominho do dado compartilhado, de forma que um conteúdo semelhante recebido de duas fontes distintas, na verdade pode ter a mesma origem, o que degrada a avaliação do dado. Nesse sentido uma metodologia compartilhada

permite que todos adotem uma abordagem consistente, facilitando a colaboração e estabelecendo credibilidade e confiança nas análises de ameaças cibernéticas.

Em síntese, a falta de uma metodologia adequada para a produção de conhecimento sobre ameaças cibernéticas pode levar a uma qualidade inferior do conhecimento, ineficiência operacional, falta de padronização, dificuldades na colaboração, falta de previsibilidade, falta de credibilidade e confiança. Dessa forma, é essencial adotar uma abordagem estruturada e sistemática para enfrentar os desafios elencados.

# 3 DISCUSSÃO DO PROBLEMA

A produção de uma inteligência de ameaça cibernética eficaz enfrenta diversos desafios que podem comprometer a qualidade e utilidade das informações geradas. Esses desafios abrangem desde a falta de contexto adequado e compartilhamento limitado de inteligência até a escassez de especialistas qualificados e a falta de adoção de uma metodologia estruturada. A superação desses desafios é crucial para garantir a relevância, precisão e atualidade da inteligência produzida, bem como promover a colaboração e a confiança entre as organizações. Nesse sentido, a implementação de um ciclo de inteligência se mostra como uma abordagem sistemática e abrangente para a produção de conhecimento que visa mitigar esses desafios e promover uma melhor segurança cibernética.

Um dos principais desafios enfrentados na produção de inteligência de ameaça cibernética é a falta de contexto adequado. A ausência de informações relevantes e detalhadas sobre as ameaças em questão compromete a compreensão do cenário em que elas estão inseridas. A falta de contexto dificulta a identificação de possíveis conexões entre diferentes eventos e a avaliação correta do impacto e da relevância das informações. Além disso, o compartilhamento limitado de inteligência entre as organizações também contribui para a falta de contexto, uma vez que a troca de informações e experiências é essencial para obter uma visão mais abrangente das ameaças em um nível global.

Outro desafio importante é a escassez de especialistas com habilidades adequadas para analisar e interpretar as informações coletadas. A complexidade crescente das ameaças cibernéticas exige profissionais altamente qualificados e atualizados, capazes de identificar padrões, tendências e comportamentos suspeitos nos dados. A falta de especialistas compromete a capacidade de análise e o resultado das investigações, levando a informações imprecisas e incompletas. Além disso, a falta de padronização nas habilidades e conhecimentos dos analistas dificulta a colaboração e o compartilhamento eficiente de inteligência entre as equipes.

Para garantir a qualidade da inteligência de ameaça cibernética, é essencial superar os desafios enfrentados ao longo do processo de produção. A avaliação rigorosa das fontes e dos dados, o compartilhamento confiável e seguro de informações, o investimento na capacitação de especialistas e a adoção de uma metodologia estruturada são aspectos-chave a serem considerados. A implementação de um ciclo de inteligência, que engloba etapas como direção e planejamento, coleta, análise, implantação e disseminação, aliado ao emprego de métodos complementares, a fim de fornecer diretrizes mais completas, oferece uma abordagem sistemática para enfrentar esses desafios. Essa abordagem proporciona diretrizes claras, procedimentos comuns e boas práticas, promovendo a confiabilidade, a eficácia e a colaboração entre as organizações na produção e compartilhamento de inteligência de ameaça cibernética.

## 3.1 QUALIDADE

A avaliação da qualidade na inteligência de ameaças cibernéticas pode ser subjetiva e variar dependendo do contexto e dos requisitos específicos de cada organização [95]. Diversos pesquisadores têm se dedicado a identificar métricas que proporcionem uma avaliação mais objetiva nesse sentido. No entanto, essa é uma tarefa desafiadora, considerando a multiplicidade de fatores que podem influenciar em diferentes graus, como acessibilidade, quantidade de dados, credibilidade, integridade, representação concisa, facilidade de manipulação, quantidade de erros, facilidade de interpretação, objetividade, relevância, reputação, oportunidade, compreensão, completude, pontualidade, entre outros [95].

Wang at al. [95] concluem que entre as múltiplas dimensões a completude, precisão, oportunidade, consistência e relevância são as cinco principais dimensões de qualidade, além disso, eles observaram que a sobrecarga de informações, o nível de experiência do analista e as restrições de tempo afetam a qualidade dos dados e influenciam a tomada de decisões.

Qiang at al. [96] conduziu uma pesquisa avaliando trabalhos relacionados à qualidade, baseados em dados provenientes de fontes de listas negras e *feeds* de inteligência de ameaças. Os critérios de relevância, pontualidade, precisão e integridade foram avaliados, porém, concluiu-se que esse método não é capaz de refletir a realidade, uma vez que as amostras representam apenas uma fração das informações de inteligência de ameaças.

Outra abordagem para a avaliação quantitativa da qualidade das fontes visa aprimorar ferramentas automatizadas por meio da priorização do nível de confiança durante a coleta [19]. Essa abordagem é estruturada em cinco critérios de avaliação: precisão sintática, completude, pontualidade, certeza da situação, consistência e relevância. A avaliação é baseada na média ponderada das fontes selecionadas, em que médias maiores correspondem a fontes mais confiáveis [19].

Estudos baseados em questionários respondidos por especialistas com experiência em segurança da informação e segurança cibernética de empresas de diferentes portes também têm sido realizados. Esses questionários têm proporcionado descobertas importantes, como a amplificação de problemas de qualidade de dados preexistentes ao integrar dados de diversas fontes, a dificuldade de encontrar inteligência acionável no meio de uma grande quantidade de dados de curta duração e a baixa acessibilidade e visualização dos dados, dificultando a produção de inteligência de ameaças [97].

Outro desafio identificado é que um padrão de compartilhamento, não garante a qualidade dos dados compartilhados. Tendo em vista que existem campos de livre preenchimento sem definição de uma linguagem comum, o que dificulta a interpretação, além disso, há falta de sinalização quanto a classificação de risco [97].

Segundo [65], a qualidade é definida como a adequação ao uso ou conformidade aos requisitos, e não pode ser determinada independentemente dos consumidores. Não há consenso sobre o conjunto preciso de dimensões que definem a qualidade dos dados ou informações. Identificar dimensões e métricas de dados fornece às organizações uma estrutura de referência para facilitar a comparação entre os dados coletados e os valores de referência. Essas observações foram resultado de uma pesquisa que entrevistou 30 especialistas com experiência em inteligência de ameaças cibernéticas, distribuídos em diferentes níveis de experiência [65].

Além disso, [20] afirma que a qualidade baseia-se em quatro características: pontualidade, relevância, precisão e completude. A pontualidade pode ser facilmente quantificada, a relevância depende do contexto do consumidor, a precisão e completude só podem ser avaliadas após um fato e são sempre estimativas. O autor também defende o aprimoramento da qualidade por meio do enriquecimento dos dados (IoC), mas não define uma metodologia de mensuração. Nesse contexto, não há uma forma definitiva de mensurar a qualidade da inteligência de ameaças, pois esse valor depende da percepção do analista que a recebe.

Dessa forma, não é possível garantir que as organizações tenham percepções idênticas sobre a qualidade diante de uma mesma informação. A diferença de contexto entre as organizações, que é dinâmico e distintivo, tem sido apontada como o principal fator para essa disparidade de percepção, conforme evidenciado em pesquisa conduzida por Sillaber at al. [97].

Por outro lado, a Agência da União Europeia para Segurança de Redes e Informações (ENISA) estabelece critérios para que uma informação seja considerada acionável e apoie tomadores de decisão. Esses critérios incluem relevância, oportunidade, precisão, abrangência (integralidade) e capacidade de assimilação (ingestibilidade) [98]. Enquanto o Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology* - NIST) recomenda que a inteligência deve ser oportuna, relevante, precisa e acionável [99].

Considerando que uma das premissas da inteligência como produto é a capacidade de ser empregada para a tomada de decisões, e considerando também o objetivo desta dissertação de aprimorar a qualidade ao longo do processo de produção de inteligência de ameaças, foram adotadas para o presente estudo quatro dimensões existentes tanto nas propriedades das informações acionáveis segundo a ENISA e o NIST, quanto nas pesquisas relacionadas à qualidade na CTI, quais sejam: relevância, completude, precisão e oportunidade. Esses aspectos são continuamente aprimorados ao longo do ciclo de inteligência por meio de procedimentos e métodos complementares entre si.

O critério de relevância é alcançado quando a inteligência é aplicável na área de responsabilidade da organização, incluindo redes, versões de software e plataformas de hardware [98]. A oportunidade está relacionada ao momento de emprego da inteligência, que deve estar disponível dentro do tempo necessário para gerar os efeitos desejados, caso contrário, torna-se irrelevante e não acionável [98]. A precisão refere-se ao nível de assertividade da inteligência, sendo que um maior nível de assertividade em relação aos requisitos previamente definidos resulta em menor incidência de falsos positivos e, portanto, maior precisão [65]. A completude envolve o fornecimento de uma visão abrangente da ameaça, incluindo a contextualização das informações sobre a ameaça, bem como as técnicas, táticas e procedimentos empregados [65, 98].

## 3.2 PLATAFORMA DE INTELIGÊNCIA DE AMEAÇA

As plataformas de inteligência de ameaça desempenham um papel fundamental na segurança cibernética, fornecendo recursos e ferramentas para coleta, análise e compartilhamento de informações relevantes sobre ameaças em tempo real [100]. Com a crescente sofisticação e volume de ataques cibernéticos, torna-se essencial adotar abordagens proativas para identificar e mitigar essas ameaças. Nesse contexto, as

plataformas de inteligência de ameaça desempenham um papel crucial ao fornecer uma visão abrangente das tendências, táticas e técnicas utilizadas pelos adversários, permitindo que as organizações fortaleçam suas defesas e tomem medidas preventivas adequadas.

No entanto, o uso efetivo de uma plataforma de inteligência de ameaça enfrenta desafios significativos. As principais expectativas na adoção de uma TIP envolvem a gestão do fluxo de informação, a conversão dos dados em conhecimento e a gestão do compartilhamento. Alguns fatores contribuem para que essa expectativa não seja alcançada, como a negligência em relação à fase de direção e planejamento, assim o restante do processo não segue uma diretriz. O poder de análise limitado é outro fator importante que aliado à enorme quantidade de dados que precisam ser coletados, processados e analisados, influenciam na qualidade da inteligência produzida.

Existem diversos estudos focados em modelos para o desenvolvimento de TIP [94, 69, 101, 13, 34], mas esses esforços não tem sido suficientes para contornar os desafios existentes. É importante compreender que a CTI não é integralmente produzida nos processos internos da plataforma de inteligência de ameaça. Além disso, é desejável que o analista esteja consciente do estado do ambiente cibernético da organização para definir corretamente os objetivos, além de ter experiência suficiente para visualizar, interpretar e interagir com a plataforma no processo de análise. Nesse sentido, segundo a ENISA [100] os programas de inteligência contra ameaças são compostos por pessoas, processos e tecnologia, uma TIP é uma disciplina de tecnologia emergente que oferece suporte aos programas de inteligência de ameaças das organizações e as ajuda a melhorar seus recursos. A Figura 3.1 é uma representação simples da integração entre pessoas, processos e tecnologia.

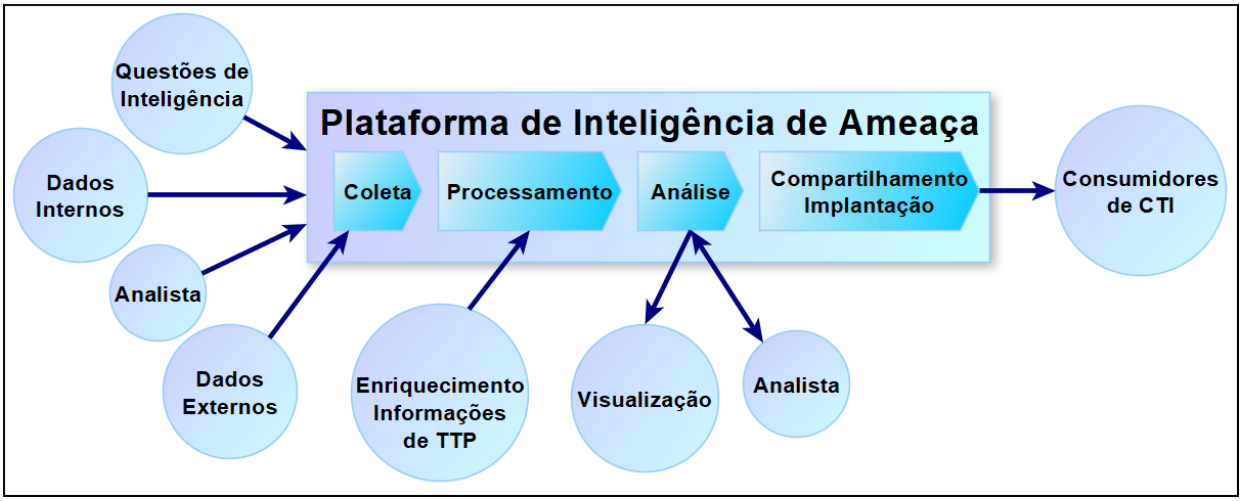


Figura 3.1: Programa de Inteligência contra Ameaça

Em suma, as plataformas de inteligência de ameaça devem proporcionar uma visão abrangente do cenário de ameaças, auxiliando na detecção precoce, na resposta eficiente a incidentes e na adoção de medidas preventivas. No entanto, para aproveitar ao máximo essas plataformas, é crucial superar os desafios relacionados à falta de metodologia, à coleta e análise de dados e à qualidade das informações. Ao enfrentar esses desafios de forma adequada, as organizações estarão melhor preparadas para lidar com as ameaças cibernéticas em constante evolução e proteger seus ativos e dados de maneira eficaz.

## 3.3 ENRIQUECIMENTO

O enriquecimento de dados desempenha um papel essencial na ampliação da completude das informações geradas no âmbito da inteligência de ameaça cibernética. No entanto, diversos desafios e considerações devem ser levados em conta nesse processo, como a validade dos indicadores de comprometimento (IoC), a confiabilidade das fontes e a necessidade de contextualização dos dados.

Um dos desafios encontrados no enriquecimento de dados diz respeito à validade dos IoC. Determinados tipos de IoC possuem uma relevância temporal limitada, que pode variar em função de diversos fatores [17]. Por exemplo, endereços IP maliciosos podem ser identificados como IoC, mas sua validade é restrita, uma vez que podem ser abandonados ou modificados pelo atacante. A organização DShield disponibiliza uma API que oferece diversas funcionalidades, incluindo uma lista de endereços IP com informações sobre o primeiro e o último avistamento conforme Figura 3.2 [5]. Com base na análise dos 1000 principais endereços, constatou-se que 73% deles permanecem na lista por até 7 dias [127]. Portanto, IoC contendo endereços IP com um *timestamp* superior a 7 dias em relação à data corrente podem ter valor apenas do ponto de vista histórico, não agregando necessariamente valor às ações de segurança.

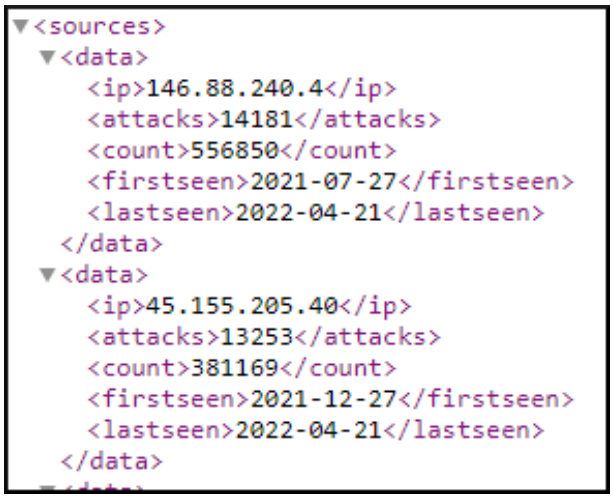


Figura 3.2: Extrato de consulta API Source [5]

Outro exemplo relacionado à validade dos IoC está relacionado ao uso de *hashes* de *malware*. Relatórios indicam que a maioria dos *hashes* de *malware* é observada por um período extremamente curto, com uma média de 58 segundos [102]. Isso significa que ferramentas baseadas em *hashes* podem se tornar ineficientes para a detecção de *malware*, uma vez que esses *hashes* deixam de ser avistados devido a alterações no objeto de origem. Além disso, estudos apontam que 60% dos domínios maliciosos possuem um período de vida de uma hora ou menos [103]. Esses exemplos reforçam a ideia de que nem todos os indicadores serão relevantes e úteis para as ações de segurança.

Além dos desafios relacionados à validade dos IoC, a identificação dos agentes de ameaça também apresenta controvérsias que podem comprometer a qualidade da geração de CTI. Diferentes organizações podem atribuir identificações distintas ao mesmo grupo de atacantes, o que interfere na identificação de relações entre os dados coletados. Nesse contexto, é importante destacar o trabalho de autores que propõem a criação de conexões entre gráficos por meio do enriquecimento de dados, permitindo encontrar informa-

ções relacionadas e fornecer um contexto mais abrangente [85]. No entanto, a falta de padronização pode prejudicar a identificação dessas relações e a compreensão completa das ameaças, como exemplificado pela identificação de um grupo de atacantes que recebe diferentes nomes, como APT28 (por Mandiant), Sofacy Group (por Kaspersky), Sednit, Tsar Team (por FireEye) e STRONTIUM (por Microsoft), FANCY BEAR [104, 105].

Os estudos realizados ao longo dessa pesquisa contribuíram para a elaboração de um artigo científico [56], que descreve uma experiência baseada em dados estruturados e não estruturados relacionados ao *spyware* Pegasus. Esses dados foram obtidos de fontes confiáveis, amplamente discutidos por empresas especializadas em segurança cibernética. Essas empresas apresentam recursos diferenciados em comparação a outras instituições, por exemplo, a vantagem de receber inúmeros *feedbacks* de aplicativos instalados na infraestrutura de seus clientes. O *spyware* Pegasus, desenvolvido pelo Grupo NOS de Israel, tem sido amplamente utilizado como uma ferramenta de vigilância contra funcionários do governo, ativistas de direitos humanos, jornalistas e chefes de Estado [106].

Ao coletar informações de diversas fontes, é fundamental observar a credibilidade dos dados e a idoneidade da fonte, levando em consideração aspectos como autenticidade, confiança e competência. As informações apresentadas foram extraídas de oito relatórios selecionados, listados na Tabela 3.1.

Tabela 3.1: Relatórios *Spyware* Pegasus

| **Relatório** | **Fonte** | **Formato** | **Data** | **Quantidade de Objetos** |
|---|---|---|---|---|
| **The Million dollar dissident** | Citizen lab report / MISP DCIBER | STIX2 | 25/08/2016 | 37 |
| **The Million dollar dissident** | Citizen lab report | PDF | 25/08/2016 | 50 |
| **OSINT - An Investigation of Chrysaor Malware on Android** | Android Developers Blog – (Rich Cannings, Jason Woloz, Neel Mehta, Ken Bodzak, Wentao Chang, Megan Ruthven) / MISP DCIBER | STIX2 | 04/04/2017 | 7 |
| **OSINT - NSO related domains** | MISP DCIBER | STIX2 | 19/07/2021 | 1407 |

*Continua na próxima página*

Tabela 3.1 – *Continuação da tabela*

| **Relatório** | **Fonte** | **Formato** | **Data** | **Quantidade de Objetos** |
|---|---|---|---|---|
| **A wolf in sheep's clothing: Actors spread malware by leveraging trust in Amnesty International and fear of Pegasus** | MISP DCIBER | STIX2 | 04/04/2017 | 9 |
| **Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits** | MISP DCIBER | STIX2 | 01/09/2021 | 23 |
| **OSINT - Cytrox Spyware Indicators of Compromise** | MISP DCIBER | STIX2 | 03/02/2022 | 329 |
| **Technical Analysis of Pegasus Spyware – relatório para humanos abril 2017** | Lookout Security Intelligence | PDF | Abril 2017 | 13 |
| **AmnestyTech/investigations/blob/master/2021-12-16_cytrox/cytrox.stix2** | AmnestyTech / MISP DCIBER | STIX2 | 16/12/2021 | 330 |
| **OSINT - AmnestyTech/investigations/master/2021 - 07-18_nso/pegasus.stix2** | AmnestyTech / Github | STIX2 | 18/07/2021 | 1439 |
| **Twitter Feeds Today feed** | MISP DCIBER | Event MISP DCIBER | 04/04/2022 | 835 |
| **Twitter Feeds Today feed** | MISP DCIBER | Event MISP DCIBER | 04/04/2022 | 851 |
| **Import of CitizenLab public DB of malware indicators** | CitzenLab | List Feeds MISP Local | 20/11/2014 | 7440 |

*Fim da tabela*

A escolha da plataforma utilizada baseou-se em estudos recentes que indicam a *Malware Information Platform* (MISP) como a TIP de código aberto mais completa e flexível [6, 84, 87, 67, 92, 15]. Esses estudos levam em consideração aspectos como integração, capacidade, suporte para padrões consolidados, disponibilidade de documentação e capacidade de resposta da comunidade.

A MISP oferece integração com diversas ferramentas de enriquecimento, permitindo a incorporação de informações adicionais aos dados coletados. No entanto, é importante observar que algumas dessas ferramentas não são necessariamente de código aberto ou possuem versões gratuitas com limitações. Nesse estudo [56], optou-se por utilizar apenas *plugins* e integrações de código aberto conforme Tabela 3.2.

Tabela 3.2: *Plugins* empregados para enriquecimento

| ***Plugin*** | **Entrada** | **Saída** |
|---|---|---|
| **Bgpranking** | ASN | Posição de classificação e descrição |
| **Cve_advanced** | | Informações sobre vulnerabilidades |
| **DNS** | Domain, hostname | Endereço IP |
| **IPASN** | Endereço IP | Último ASN relacionado |
| **PassiveTotal** | hostname, domain, ip-src, ip-dst, x509, fingerprint-sha1, email-src, email-dst, target-mail, whois (dados do registrante e data de criação), text | Atributos adicionais presentes em sua base de dados |
| **Shodan** | Endereço IP | Atributos adicionais presentes em sua base de dados. |
| **Deverse_dns** | Endereço IP | Nome de host |
| **Threat_miner** | Hostname, domain, ip-src, ip-dst, md5, sha1, sha256, sha512 | Atributos adicionais relacionados: domínio, ip-src, ip-dst, texto, md5, sha1, sha256, sha512, ssdeep, authentihash, nome do arquivo, whois-registrant-email, url, link |

*Continua na próxima página*

Tabela 3.2 – *Continuação da tabela*

| ***Plugin*** | **Entrada** | **Saída** |
|---|---|---|
| **Rbl (Real-Time Blackhost List)** | Endereço IP | Resultado de consulta em blacklist conhecidas |
| **Urlhaus** | Domain, hostname, ipscr, md5, sha256, url | url, filename, md5, sha256 |
| **Dbl_spamhaus (Doamin Block List)** | Domain, hostname | Código de resposta correspondente a reputação do domínio. |
| **Malwarebazaar** | Hash: md5, sha1, sha256 | Objetos descrevendo o arquivo relacionado ao hash de entrada |
| **Pdf_enrich** | Arquivo pdf | Lista de possíveis IoC presentes no corpo do arquivo |

*Fim da tabela*

Durante a análise dos dados, verificou-se o impacto da questão da pontualidade. Considerando que os relatórios e dados utilizados no caso de uso abrangem o período entre 2016 e 2022, a maioria dos domínios não existe mais ou possui data de registro posterior à data do relatório. O número médio de domínios expirados, ou seja, disponíveis para novo registro, é de 68%, variando de 58% a 80% em cada relatório. Essas observações foram feitas a partir de relatórios de agosto de 2016, julho de 2021, setembro de 2021, dezembro de 2021, fevereiro de 2022, abril de 2022 e junho de 2022, confrontados com registros de domínio de julho de 2022. Esse dado é preocupante, uma vez que durante a pesquisa foram identificadas ferramentas para detecção do *spyware* Pegasus baseadas em conjuntos de IoC desses relatórios, o que pode resultar em falsos positivos.

Outra observação relevante está relacionada a relatórios idênticos que, ao serem analisados por organizações distintas, produzem resultados diferentes. Por exemplo, o relatório "*The Million Dollar Dissident - Citizen lab report*", disponível em formato PDF, foi analisado por mais de uma organização especializada em segurança. No entanto, cada organização gerou uma quantidade diferente de IoC a partir desse relatório. Ao importar e enriquecer esse relatório no MISP, constatou-se uma análise limitada devido à complexidade computacional inerente ao processamento de linguagem natural (*Natural Language Processing* - NLP). Consequentemente, informações relevantes contidas em relatórios disponíveis em linguagem natural não foram extraídas pelas ferramentas empregadas para a coleta.

Em resumo, o enriquecimento de dados desempenha um papel crucial na fase de processamento da

inteligência de ameaça cibernética. No entanto, é necessário enfrentar os desafios associados, como a validade dos IoC, a confiabilidade das fontes e a necessidade de contextualização dos dados. A escolha adequada de uma plataforma e a utilização de ferramentas de enriquecimento apropriadas podem contribuir para aumentar a qualidade e a utilidade das informações geradas, promovendo uma inteligência de ameaça cibernética mais eficaz e acionável.

## 3.4 CICLO DE INTELIGÊNCIA

O emprego do ciclo de inteligência, estabelece diretrizes e padrões para unificar os estudos, que atualmente estão fragmentados. Sua abrangência na CTI é importante para desenvolver metodologias apropriadas, estabelecer boas práticas, impulsionar a inovação e garantir uma abordagem sistemática e eficaz. A aplicação de uma metodologia comum para o domínio de CTI impulsiona a inovação, uma vez que os esforços serão concentrados.

Existem pesquisas relacionadas aos processos de produção de inteligência de ameaça cibernética, por exemplo, Sakellariou et al. [94] faz um breve estudo da abordagem do ciclo de inteligência, contudo, não esclarece as fontes, além de apresentar resultado conflitante com abordagens semelhantes [17], outras publicações também apresentam resultados distintos, contudo trazem apenas menções textuais sem apresentar números [9, 72]. Da mesma forma [94] identifica que a fase de direção e planejamento é implementada em todos os TIP existentes, além de não esclarecer quais as TIP avaliadas, esta informação conflita com diversos estudos que identificam a fase de direção e planejamento como a mais negligenciada [17].

A correta orientação sobre essa abrangência é importante pois serve como diretriz para identificar lacunas do processo de produção do conhecimento. A falta de uma diretriz sobre o cenário atual das pesquisas em torno da CTI, contribuem para o declínio na qualidade da inteligência produzida. Isso reforça a importância de avaliar, mesmo que brevemente, a abrangência do ciclo de inteligência nas publicações acadêmicas que tem como tema a inteligência de ameaça cibernética a fim de identificar as lacunas existentes.

Dessa forma os principais estudos que abordam a negligencia em relação ao ciclo de inteligência provem de autores que visam apresentar o estado da arte, contudo, não definem diretrizes para solução.

## 3.5 CONSCIÊNCIA SITUACIONAL

A consciência situacional é uma dinâmica para percepção, compreensão e projeção de cenários que visa a tomada de decisão e pode ser empregada em uma grande variedade de domínios do conhecimento [2]. Permite estabelecer análise e avaliação de situações presentes e criar projeções possíveis em curto prazo. Dessa forma, implementar a consciência situacional para a correta orientação sobre o estado atual do ambiente cibernético da organização é uma base importante para o gerenciamento da segurança de rede [107].

Nesse sentido foram identificados diversos trabalhos que aplicam a consciência situacional na segu-

rança de rede, normalmente relacionados a varredura do tráfego [77, 78, 108]. Assim como, uma aplicação de ferramentas de gerenciamento de informações e eventos de segurança (*Security Information and Event Management* - SIEM) para avaliar a consciência situacional no domínio cibernético [109]. Nesse trabalho os processos de um sistema SIEM são divididos em coleta e padronização, análise ou correlação e gestão de alertas, a fim de buscar relações com os níveis da consciência situacional.

Em outro trabalho a consciência situacional foi utilizada em conjunto com o ciclo de inteligência como referência para conduzir o desenvolvimento de um estudo de caso, da empresa de inteligência de segurança nacional dos EUA, que busca soluções para lacunas relacionadas à avaliação de riscos de segurança da informação [110].

Conclui-se que os modelos de consciência situacional já são amplamente empregados para buscar orientação sobre o estado geral do ambiente cibernético da organização, comprovando sua contribuição para a formação do contexto, contudo, seu emprego para produção de CTI precisa levar em conta todos os domínios da inteligência de ameaça, técnico, tático, operacional e estratégico, pois dada as características da consciência situacional, seria, em tese, complexo de produzir inteligência estratégica de longo prazo. Para contornar esse desafio a proposta é confrontar as características da consciência situacional com as fases do ciclo de inteligência para verificar a existência de semelhanças entre seus processos, semelhante ao adotado em [109] e dessa forma complementar o ciclo de inteligência com as contribuições da consciência situacional. A integração da consciência situacional com o ciclo de Inteligência pode contribuir para uma compreensão mais ampla do ambiente operacional, permitindo assim uma avaliação mais precisa das ameaças e uma resposta mais efetiva.

## 3.6 APRENDIZAGEM POR COMPETÊNCIA CONSCIENTE

A produção de inteligência de ameaça cibernética é uma atividade que apoia a proteção efetiva de sistemas e informações em um ambiente dinâmico e complexo. Nesse contexto, a aplicação dos estágios de competência, também conhecido como modelo de aprendizagem de competência consciente, pode fornecer um suporte valioso para a aquisição cognitiva necessária no processo de produção de inteligência de ameaça. Esses estágios representam os diferentes estados psicológicos envolvidos na progressão da incompetência para a competência em uma habilidade, permitindo uma abordagem de aprendizado contínuo e adaptativo.

Estudos indicam que compreender o nível de consciência e competência é fundamental para lidar com as mudanças inerentes aos ambientes cibernéticos complexos e dinâmicos [111]. Em tais ambientes, situações novas surgem com frequência, desafiando até mesmo os especialistas em determinadas disciplinas e expondo suas limitações. Nesse sentido, o ciclo de aprendizagem dos estágios de competência, inconsciente-incompetente, consciente-incompetente, consciente-competente e inconsciente-competente, representa um processo contínuo e crescente de aquisição de conhecimento e habilidades que se adapta às demandas em constante evolução [111].

O modelo de aprendizagem por competência consciente (*Conscious Competence Learning* - CCL), desenvolvido por Abraham Maslow e Noel Burch [112], é particularmente relevante para a produção de

inteligência de ameaça cibernética. Sua aplicação versátil encontra respaldo em diferentes áreas, incluindo educação, empresas e medicina. No contexto da segurança cibernética, esse modelo proporciona uma estrutura adequada para enfrentar a natureza dinâmica e complexa do ambiente cibernético, no qual novas ameaças, vetores de ataque e vulnerabilidades surgem com frequência.

A abordagem de aprendizado contínuo baseada nos estágios de competência incentiva a conscientização das limitações inerentes à evolução tecnológica e promove o desenvolvimento constante de conhecimentos e informações relevantes. Esse enfoque capacita os profissionais de segurança cibernética a adaptarem-se rapidamente às mudanças de cenário, atualizando suas competências e aprimorando suas habilidades para enfrentar as ameaças emergentes.

A aplicação dos estágios de competência como suporte para a produção de inteligência de ameaça cibernética pode ser uma abordagem eficaz para enfrentar os desafios inerentes a um ambiente cibernético em constante evolução. Através do reconhecimento dos diferentes estados de consciência e competência, os profissionais podem adquirir e aprimorar as habilidades necessárias para detectar, analisar e responder às ameaças digitais de maneira mais eficiente.

## 3.7 5W3H

A gestão eficiente dos processos de CTI são fundamentais para produção de inteligência acionável. O modelo 5W3H é uma ferramenta poderosa para fornecer direcionamento e orientação de forma clara, organizada e eficaz. Com suas oito perguntas-chave, oferece um guia prático, abrangente e versátil, sendo capaz de garantir uma abordagem abrangente e estruturada, além de abordar aspectos fundamentais, independente da área de aplicação.

Diversos são os exemplos da versatilidade do 5W3H, como em [137] onde o método foi aplicado na gestão do ciclo de vida de materiais, desde de o planejamento de aquisição, passando pelo acompanhamento do pedido, recepção, conferência, guarda e distribuição para o usuário final. Inicialmente todas as etapas foram avaliadas para identificação de problemas, usando ferramentas como o diagrama de causa e efeito ou diagrama de *Ishikawa* e o 5W3H. Na proposta de solução foi o empregado o 5W3H em todas as etapas.

O emprego do 5W3H na organização de ações em rotinas médicas, também em conjunto com o diagrama de *Ishikawa*, é outro exemplo de versatilidade [140]. Essa flexibilidade também pode ser observada pelo seu emprego no controle de qualidade, seja na indústria, no campo ou comércio, geralmente associada ao diagrama de *Ishikawa* [139] [141] [142].

No âmbito da CTI o método 5W3H foi eficaz para verificar a relevância, oportunidade e clareza da informação, de modo que, quanto mais respostas para os questionamentos do 5W3H maior a capacidade e a completude da inteligência produzida [59], [81].

Nesse sentido, modelo 5W3H se revela como uma opção para a produção de inteligência de ameaças, proporcionando direcionamento e estrutura para as atividades de direção e planejamento, coleta, processamento, análise e implantação e disseminação de informações. Ao responder as perguntas "o quê, por quê,

quem, quando, onde, como, quanto tempo e quanto", os profissionais de inteligência de ameaças podem definir o escopo, justificar a importância, identificar os atores, estabelecer períodos de monitoramento, selecionar áreas geográficas relevantes, adotar métodos e técnicas adequadas e alocar recursos necessários. A aplicação criteriosa do modelo 5W3H contribui para uma abordagem sistemática e eficiente na produção de inteligência de ameaças, contribuindo a identificação e mitigação proativa de riscos cibernéticos.

## 3.8 INTEGRAÇÃO DE MÉTODOS

A integração de características complementares dos métodos, como o ciclo de inteligência, a consciência situacional, a CCL e o modelo 5W3H, como representado na Figura 3.3, pode desempenhar um papel importante na produção de inteligência de ameaça cibernética. Essa integração estabelece diretrizes e padrões que unificam os estudos, atualmente fragmentados, proporcionando uma abordagem mais abrangente e estruturada.

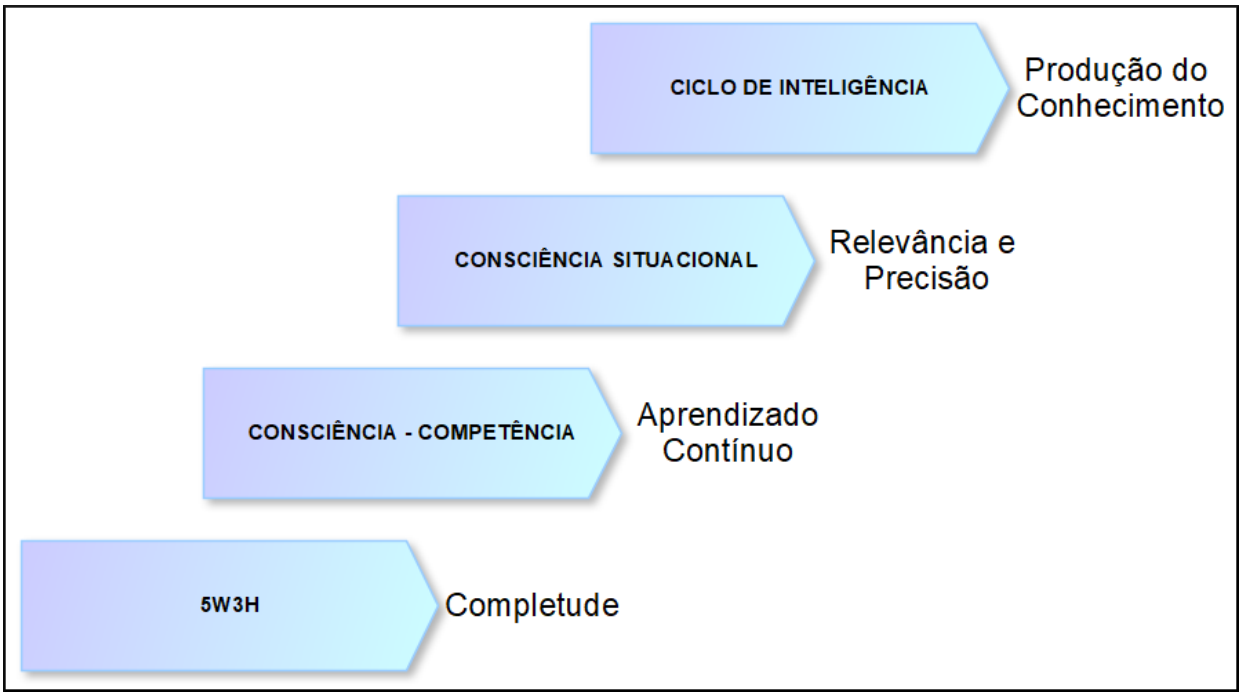


Figura 3.3: Métodos Complementares

A consciência situacional, ao fornecer uma compreensão atualizada do ambiente cibernético da organização, contribui na orientação correta das ações de segurança. Essa consciência permite uma avaliação precisa do estado atual do ambiente operacional, identificando vulnerabilidades, ameaças em potencial e possíveis impactos. Ao integrar a consciência situacional com o ciclo de inteligência, é possível obter uma visão mais ampla do cenário de ameaças, possibilitando uma resposta mais efetiva.

A aplicação da CCL, devido à natureza dinâmica e complexa do ambiente cibernético, é particularmente relevante. Esse modelo de aprendizado contínuo incentiva o desenvolvimento constante e a busca por novos conhecimentos e informações relevantes para uma adaptação rápida às mudanças de cenário. A

CCL permite a identificação de lacunas no conhecimento, a análise de tendências e a definição de diretrizes para aprimorar a produção de inteligência de ameaça cibernética.

O modelo 5W3H, por sua vez, se destaca por sua facilidade de uso e capacidade de fornecer uma visão completa do contexto da ameaça. Ao responder às perguntas "o quê, por quê, quem, quando, onde, como, quanto tempo e quanto", esse modelo ajuda a visualizar a completude das informações, garantindo uma abordagem abrangente na produção de inteligência de ameaça cibernética.

A integração desses métodos em um *framework* de produção de conhecimento tende a oferecer orientação e suporte ao analista ao longo de todo o processo. Ao unir características complementares, como a orientação estratégica do ciclo de inteligência, a compreensão do ambiente proporcionada pela consciência situacional, a adaptabilidade da CCL e a visão abrangente do contexto do modelo 5W3H, é possível obter uma abordagem mais consistente e eficiente na produção de inteligência de ameaça cibernética.

Em suma, a integração dessas características complementares dos métodos mencionados fortalece a produção de inteligência de ameaça cibernética, permitindo uma compreensão mais abrangente do ambiente operacional, uma avaliação mais precisa das ameaças e uma resposta mais efetiva aos desafios cibernéticos em constante evolução. Essa abordagem integrada contribui para a geração de conhecimentos mais sólidos e acionáveis, fornecendo às organizações as ferramentas necessárias para proteger seus ativos e enfrentar as ameaças cibernéticas com maior eficácia.

# 4 PROPOSTA DE SOLUÇÃO

Reconhecendo a importância de uma abordagem abrangente e estruturada fundamenta em processo científico e metodológico de produção do conhecimento de inteligência, nesse capítulo são apresentados aspectos que envolvem o desenvolvimento de um *framework* para emprego na produção de CTI, com a premissa de abranger os aspectos de relevância, precisão e completude.

Em [56], se explorou a lacuna existente referente à baixa qualidade na produção de inteligência de ameaças, decorrente, dentre outros fatores, da falta de metodologia de produção de conhecimento e inteligência no âmbito da CTI. Nesse estudo foi apresentado um caso de uso que teve maior foco na fase de análise, sem levar em conta o contexto da organização. Nesse sentido, apesar de demonstrar a relevância da metodologia proposta por meio da completude das informações produzidas, deixa um hiato no que se refere ao levantamento de requisitos da fase de direção e planejamento, uma vez que as questões de inteligência foram hipotéticas e não fruto aplicação do processo de levantamento de requisitos.

## 4.1 INTELIGÊNCIA DE AMEAÇA CIBERNÉTICA E O CICLO DE INTELIGÊNCIA

Nos trabalhos selecionados foram observadas diversas afirmações acerca do emprego do ciclo de inteligência. Alguns autores apontam a fase de coleta como a mais abordada, outros afirmam que a fase de direção e planejamento é a mais negligenciada. Entretanto observou-se apenas um artigo em que baseado num conjunto de 28 trabalhos, foi realizado mapeamento de cada um deles para as diferentes fases do ciclo de inteligência [17], cuja distribuição resultou em: Direção e Planejamento 0%, Coleta 39%, Processamento 25%, Análise 64,3% e Divulgação 46,4%.

A partir dessa perspectiva, para compreender a abrangência de pesquisas relacionadas à inteligência de ameaças cibernéticas que façam referência ao ciclo de inteligência, foram selecionadas a partir do referencial teórico todas as publicações científicas revisadas por pares que tem relação direta com o tema CTI, resultando num conjunto de 80 publicações, que foram criteriosamente analisadas quanto a abordagem de quaisquer das fases do ciclo de inteligência.

Para alcançar maior abrangência na análise das publicações, foi considerado como ciclo de inteligência qualquer divisão em fases ou etapas que tenham relação com o processo de construção do conhecimento, com quantidade de fases variando entre quatro e oito. Por exemplo, em [113] os autores usam a classificação “fases do CTI” sendo que as fases são as mesmas do ciclo de inteligência. Já em [69] o autor empregou a expressão “ciclo de vida da inteligência de ameaças”. Avaliamos que essa abordagem não é prejudicial, pois não altera o conceito do ciclo de inteligência, tendo em vista, que a variação na quantidade de fases corresponde ao agrupamento ou detalhamento maior das cinco fases que adotamos nessa pesquisa, à exceção da fase de *feedback*, que não adotamos e foi abordada em alguns trabalhos.

O resultado pode ser observado na Tabela 4.1, onde AG são publicações que abordam aspectos gerais da CTI, como definições, comparações, padrões, dentre outros, e NR são publicações que não mencionam

ao ciclo de inteligência.

Tabela 4.1: Publicações e as Fases do Ciclo de Inteligência

**DP: Direção e Planejamento**
**CO: Coleta**
**PR: Processamento**
**AN: Análise**
**DI: Disseminação e Implantação**
**NR: Não Menciona o Ciclo**
**AG: Aspectos Gerais de CTI**

| **Referências** | **DP** | **CO** | **PR** | **AN** | **DI** | **NR** | **AG** | **%** |
|---|---|---|---|---|---|---|---|---|
| [17] | x | x | x | x | x | | | **1,25%** |
| [69] | x | x | | | | | | **1,25%** |
| [87, 88, 35] | | x | x | x | x | x | | **3,75%** |
| [94, 34] | | x | x | x | x | | | **2,50%** |
| [20, 23, 114, 115, 116, 117, 118] | | x | x | x | | x | | **8,75%** |
| [119, 120, 12, 21, 59, 67, 25, 121, 122] | | x | x | x | | | | **11,25%** |
| [79, 16] | | x | | x | x | | | **2,50%** |
| [63, 123] | | x | | x | | x | | **2,50%** |
| [124] | | x | | x | | | | **1,25%** |
| [125, 18, 22] | | x | | | | x | | **3,75%** |
| [19, 89] | | x | | | | | | **2,50%** |
| [26] | | | x | x | x | x | | **1,25%** |
| [126, 127, 128] | | | x | x | | x | | **3,75%** |
| [129] | | | x | x | | | | **1,25%** |
| [130] | | | x | | | x | | **1,25%** |
| [85] | | | | x | x | x | | **1,25%** |
| [11, 91, 86, 93, 131, 132, 133, 134, 135, 136, 137, 138, 139] | | | | x | | x | | **16,25%** |
| [140, 113, 141, 90, 68] | | | | x | | | | **6,25%** |
| [70, 14, 84, 103, 97, 142] | | | | | x | x | | **7,5%** |
| [143, 72, 65] | | | | | x | | | **3,75%** |
| [15, 13, 24, 36, 38, 61, 62, 144, 101, 145] | | | | | | x | x | **12,50%** |
| [92, 6, 9] | | | | | | | x | **3,75%** |
| **Quantidade de Publicações:** | **2** | **33** | **28** | **51** | **19** | **50** | **13** | **80** |
| **Percentual** | **2,50%** | **41,25%** | **35%** | **63,75%** | **23,75%** | **62,50%** | **16,25%** | |
| | **DP** | **CO** | **PR** | **AN** | **DI** | **NR** | **AG** | |

16,25% das publicações selecionadas abordam questões gerais não relacionadas diretamente com a produção de inteligência, abordam questões como definições, comparações de plataformas e padrões empregados. Destas publicações apenas 23% mencionam o ciclo de inteligência.

62,50% das pesquisas abordam pelo uma das fases do ciclo de inteligência, porém, não se amparam em uma metodologia específica, dessa forma, as contribuições apresentadas carecem de estudos futuros para que sejam adequadas a um processo de produção de inteligência.

A fase de análise é a mais abordada e corresponde a 63,75% dos estudos selecionados, seguida da fase de coleta com 41,25%. A fase menos estudada é a de direção e planejamento, abordada em 2,5% das publicações.

A fase de direção e planejamento está associada à definição de objetivos, envolve a identificação das necessidades de inteligência, indicação de prazo, além da definição de estratégias para coleta e análise de informações. Embora essa fase não seja mencionada na maioria das publicações, ela deve ser incorporada nos processos de produção de inteligência, pois as metas e objetivos devem ser claramente definidos. Inteligência sem propósito não existe, tendo em vista que a razão de sua existência é apoiar a tomada de decisão.

## 4.2 CONSTRUÇÃO DO CONHECIMENTO

Alicerçado nos conceitos apresentados, foi estudada a melhor maneira de integrar os diversos conhecimentos, de modo a construir uma metodologia que sirva como base para implantação da Inteligência de Ameaça Cibernética em uma organização e, por conseguinte minimizar os desafios identificados ao longo dessa pesquisa.

Um dos pilares dessa proposta é o ciclo de inteligência, uma definição comumente empregada para o processo sistemático de obtenção do conhecimento, que é composto por fases que variam conforme a proposta do fluxo dos dados até o produto final. Nessa pesquisa foi adotado um ciclo de cinco fases: direção e planejamento; coleta; processamento; análise; e implantação e disseminação.

A adoção do modelo de cinco fases, tem base nas pesquisas realizadas no conjunto de publicações, incluindo *White papers* [146, 100], relacionadas tanto com a inteligência tradicional, quanto com inteligência cibernética. Em tese, a terminologia e a estrutura do ciclo de inteligência podem variar para atender às necessidades e contextos específicos.

Uma vez que foi verificado que a fase de planejamento tem sido fortemente negligenciada, e que grande parte dos pesquisadores almejam produzir inteligência sem objetivos claros, optou-se por uma fase de direção e planejamento para um detalhamento maior das atividades dessa fase.

A fase de direção e planejamento bem executada tem relação direta para que a inteligência produzida seja relevante, precisa e oportuna. Nessa fase ocorre a identificação de elemento importantes, como pontos fortes e fracos, eventos conhecidos e desconhecidos, além da formulação de objetivo e desenvolvimento de método para alcança-lo. Essa fase define o propósito e o escopo das etapas seguintes.

No que se refere a fase de processamento, em outros modelos ela é incorporada algumas vezes na coleta

e em outras na análise. Porém, pelo crescente volume da dados sobre ameaças cibernéticas, é essencial a adoção de processo adequado para avaliação, organização, enriquecimento e descoberta de correlações, dessa forma é adequado que o processamento seja uma fase isolada que funcione como filtro para garantir apenas informações relevantes e precisas para a consecução do objetivo. Ademais, como já foi visto, o excesso de informações pode travar o processo de análise.

No decorrer da pesquisa identificamos requisitos para produção de inteligência de ameaça cibernética de qualidade. Tais requisitos foram adotados, no âmbito desse trabalho, como pressupostos da CTI, quais sejam:

a. Os principais fatores que influenciam a qualidade da CTI são oportunidade, relevância, precisão e completude;

b. Quanto mais oportuna, relevante, precisa e completa for a informação, maior a probabilidade de termos inteligência acionável ao final do processo.

c. A coleta, enriquecimento e cruzamento de dados de diversas fontes somente serão válidos se tiverem correlação com o conjunto de dados coletados na própria organização. Maior número de correlações determina maior relevância.

d. Informação relevante, aliada à consciência situacional da ameaça, determinam a precisão.

A partir desses pressupostos, verifica-se que os requisitos relevância e precisão têm forte conexão com o contexto da organização, que por conseguinte, é obtido por meio da consciência situacional. Desse ponto de vista a consciência situacional é ponto de partida para elaboração dos requisitos de inteligência. Destacam-se duas observações sobre consciência situacional, a primeira indica a importância do seu emprego na metodologia proposta, a coleta de dados é premissa da consciência situacional, refere-se ao conjunto de elementos envolvidos em um determinado processo de percepção [77]. A segunda acende um alerta sobre a composição das equipes envolvidas nesse processo, muitas vezes a consciência situacional é baseada em analistas pouco conectados e não em uma equipe, isso decorre da barreira criada pela desigualdade de conhecimento entre os analistas, dessa forma a consciência de situação é frágil, confusa e pouco confiável [75]. Logo a experiência e conhecimento do analista de inteligência cibernética configuram-se pontos preponderantes para definição das equipes.

### 4.2.1 Considerações

#### 4.2.1.1 Direção e Planejamento

A fase de direção e de planejamento refere-se à definição de objetivos de informação, tópicos chave e questões de inteligência, também à identificação de segmentos, base de dados, tecnologias, sensores, fontes e ferramentas empregadas, também define a forma como o trabalho será conduzido. As questões de inteligência em alguns casos são denominadas requisitos de inteligência, ou seja, o que se pretende alcançar, são necessidades informacionais do tomador de decisão, podem ser formuladas demandas específicas, por suposições ou intuições originadas em assuntos de interesse ou fundamentada nos processos de negócio da organização, geralmente surge da falta de respostas para uma situação enfrentada.

Ao explorar a fase de direção e planejamento no nível das ações chega-se ao seguinte cenário:

a. **Direção:**

- Identificar necessidades de informação e perguntas chave
- Identificar base de dados, segmentos, tecnologias, sensores e fontes de informação

b. **Planejamento:**

- Elencar o que é conhecido e o que falta conhecer
- Definir requisitos de coleta para as fontes de informação
- Definir métodos analíticos
- Definir fontes de informação
- Definir recursos e prazos
- Prever atividades subsequentes

#### 4.2.1.2 Consciência Situacional

A análise da consciência situacional de um domínio, envolve listar dados e elementos através da identificação e coleta de informações essenciais, procurar respostas para "Quem?", "Onde?", "Quando?" e "Quantos?", baseado em dados oriundos do monitoramento do ambiente, entender a importância dos elementos, agregar significado às informações coletadas e verificar a relevância, permitindo entender a situação e sua criticidade, além de procurar respostas para "Porquê?", "Qual a capacidade?", "Qual a relevância?" e "Qual ação?", essa relação está representada na Figura 4.1. Essa descrição refere-se aos níveis de percepção e compreensão da consciência situacional, quando decomposta em ações, chegamos ao seguinte:

a. **Percepção:**

- Identificar entidades do domínio e suas propriedades
- Monitorar ativos
- Criar mecanismos de detecção

b. **Compreensão:**

- Detectar anomalias
- Minerar dados
- Reconhecer padrões
- Identificar correlações
- Interpretar informações

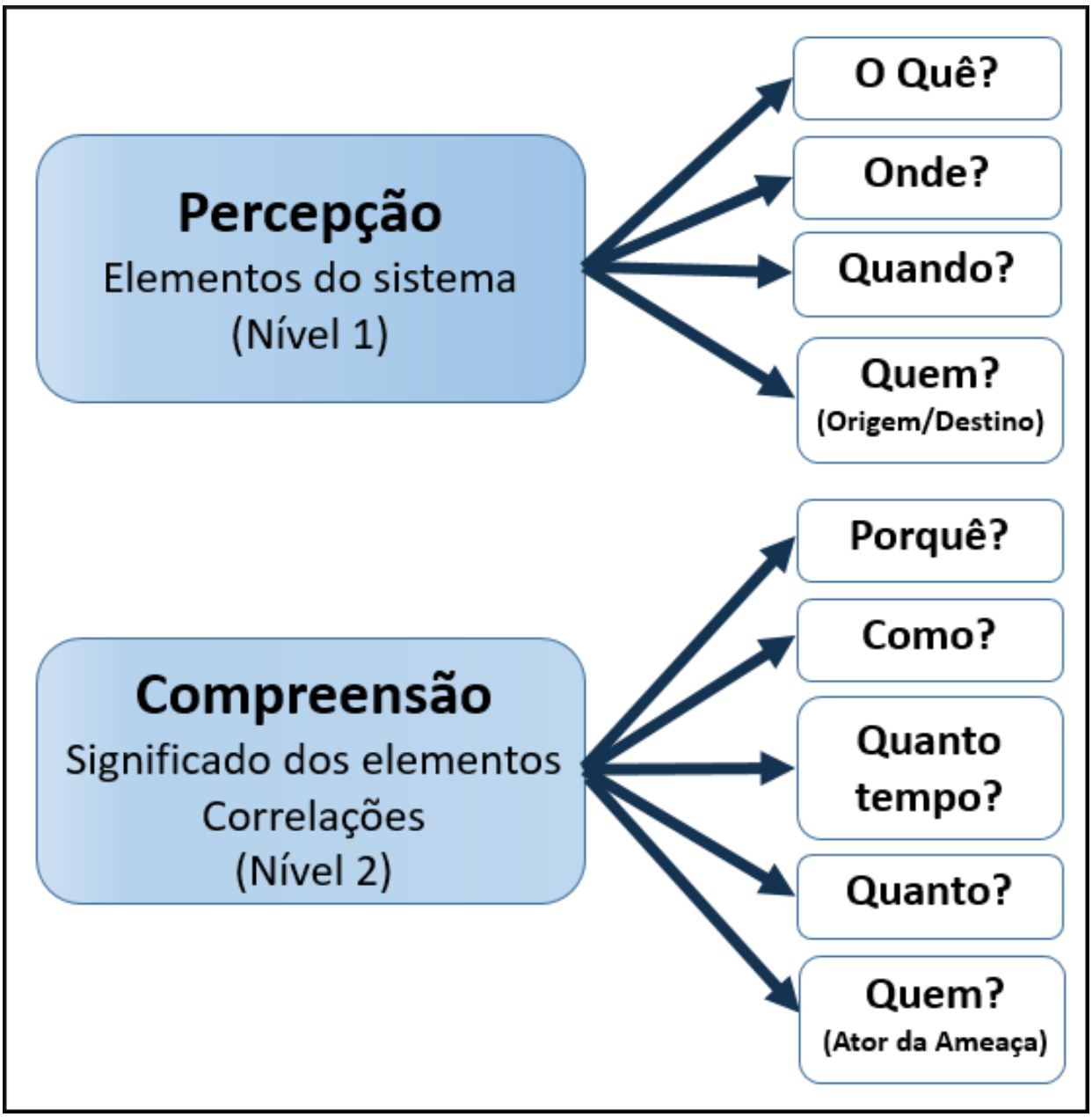


Figura 4.1: Níveis de Percepção e Compreensão

#### 4.2.1.3 Relação Entre Ciclo de Inteligência e Consciência Situacional

Enquanto a consciência situacional refere-se a um estado de conhecimento de um domínio através da identificação de seus elementos e suas relações com o meio, a inteligência é mais ampla, leva em conta a situação, capacidades, intenções, atores e ameaças conhecidas ou potenciais para produção de consciência de situação, avaliação de situação e avaliação de ameaça. Podemos correlacionar a consciência situacional com uma foto, enquanto a inteligência equivale a uma sequência de fotos. A "foto" atual da organização é o primeiro passo para a identificação dos requisitos e a formulação das questões de inteligência. Uma vez que tem relação tanto com o contexto predefinido, que é ponto de partida no ciclo de inteligência, quanto com a definição de consciência situacional. Logo, é imprescindível, antes de tudo, conhecer o contexto da

organização. Do mesmo modo, uma avaliação mais atenta permite concordar que os níveis de percepção e compreensão da consciência situacional englobam as quatro primeiras fases do ciclo de inteligência, uma vez que contempla ações de planejamento, coleta, processamento e análise. Tal observação pode ser melhor elucidada por meio da Figura 4.2, perceba que o ciclo de inteligência à direita é empregado para produção da consciência situacional da organização.

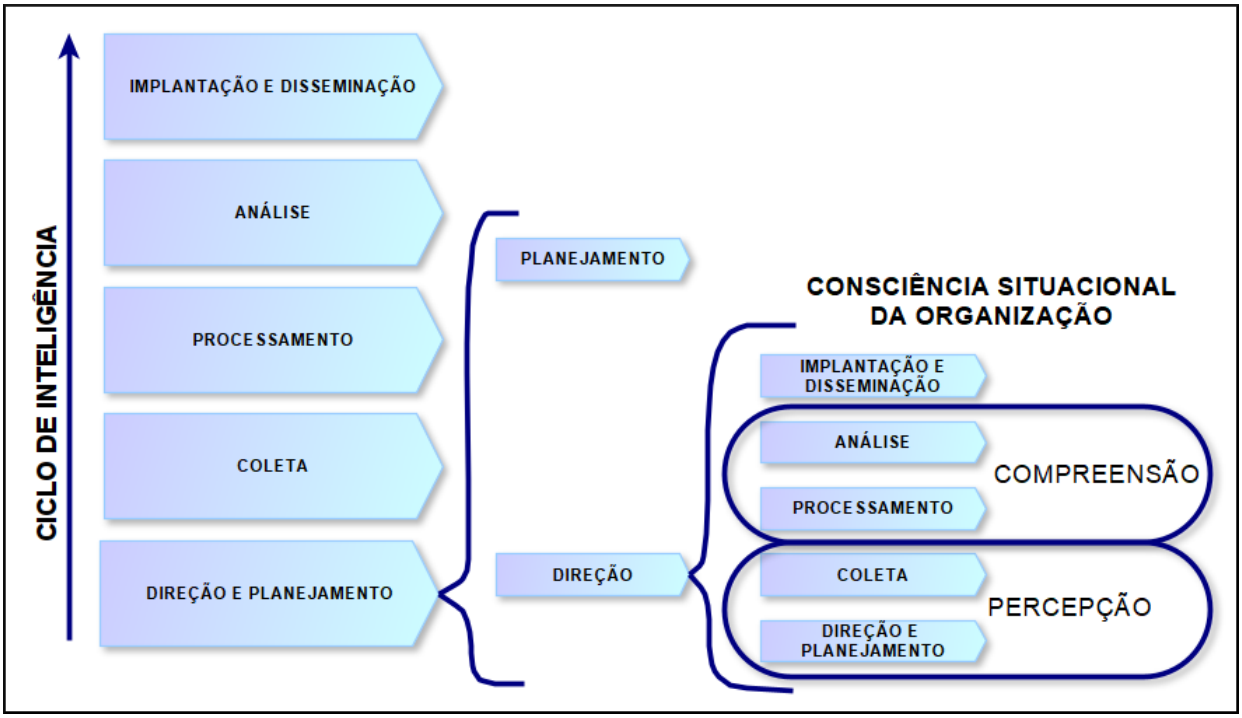


Figura 4.2: Correlação Entre Ciclo de Inteligência e Consciência Situacional

#### 4.2.1.4 Método 5W3H

O método 5W3H origina-se das sete circunstâncias de Aristóteles [147]. Esse método está relacionado a um conjunto de oito perguntas: o quê, quem, onde, por que, quando, como, quanto e por quanto tempo. É amplamente aplicado em diversas áreas a fim de se obter a contextualização de um tema em sua completude [6]. As questões 5W3h contribuem para a conscientização do nível de maturidade em relação ao conhecido e aos objetivos para geração de inteligência acionável.

Uma vez que a consciência situacional procura responder questões a fim de criar contexto e o método 5W3H foi empregado com essa mesma função nas primeiras etapas dessa pesquisa [56], logo o método 5W3H será mantido, sendo inicialmente empregado na fase de planejamento. A vantagem dessa abordagem é a facilidade de perceber quais perguntas necessitam de respostas.

Nas fases seguintes buscamos respostas para as questões que não foram respondidas na fase de planejamento, assim em cada ciclo de coleta, processamento e análise verificamos a completude do contexto, buscando respostas para todas as questões do método 5W3H. Quanto mais questões do 5W3H forem respondidas, maior será a completude do CTI e consequentemente maior a qualidade. Se ao final desse processo houver respostas para a maioria das perguntas, provavelmente teremos inteligência acionável [6].

O “o que” define o objeto a ser estudado, que no contexto da inteligência de ameaças, refere-se a ameaças ou incidentes. O “onde” refere-se à localização geográfica de origem do evento, podendo também ser o caminho percorrido até o destino. O “Quando” determina a data e a hora em que o evento ocorreu.

O “Como” define as táticas, técnicas e procedimentos empregados. O “Quanto” refere-se à capacidade de causar danos, podendo também estar relacionado ao financiamento. "Quanto tempo"indica a duração do evento, incidente ou ameaça. “Quem” associa a ameaça ou incidente organização ou indivíduo responsável. O “porquê” explica as motivações do responsável pelo evento. A Figura 4.3. apresenta a relação dos elementos do método 5W3H com as entidades envolvidas em um incidente ou ameaça.

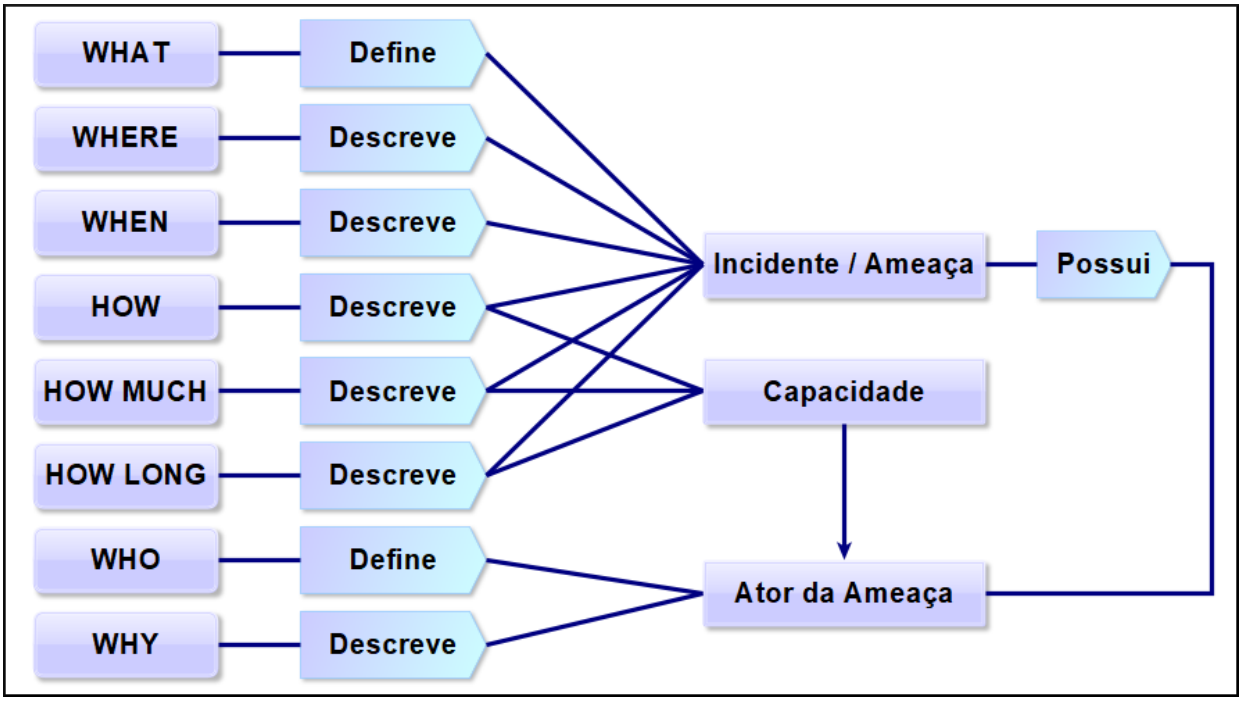


Figura 4.3: Relação Entre o Método 5W3H e as Entidades Envolvidas - Adaptado de [6]

#### 4.2.1.5 Estágios de Competência

A construção do conhecimento passa por quatro estágios [148] que levam da ignorância à inteligência acionável conforme representado na Figura 4.4 , em algumas pesquisas é representado por uma matriz de consciência x competência. O conhecimento desses estágios contribui para que analistas façam uma reflexão crítica sobre o nível de conhecimento em que encontram, pois com o aumento das ameaças avançadas, inevitavelmente, em algum momento estaremos no estágio de ignorância perante vulnerabilidades, ameaças e riscos existentes.

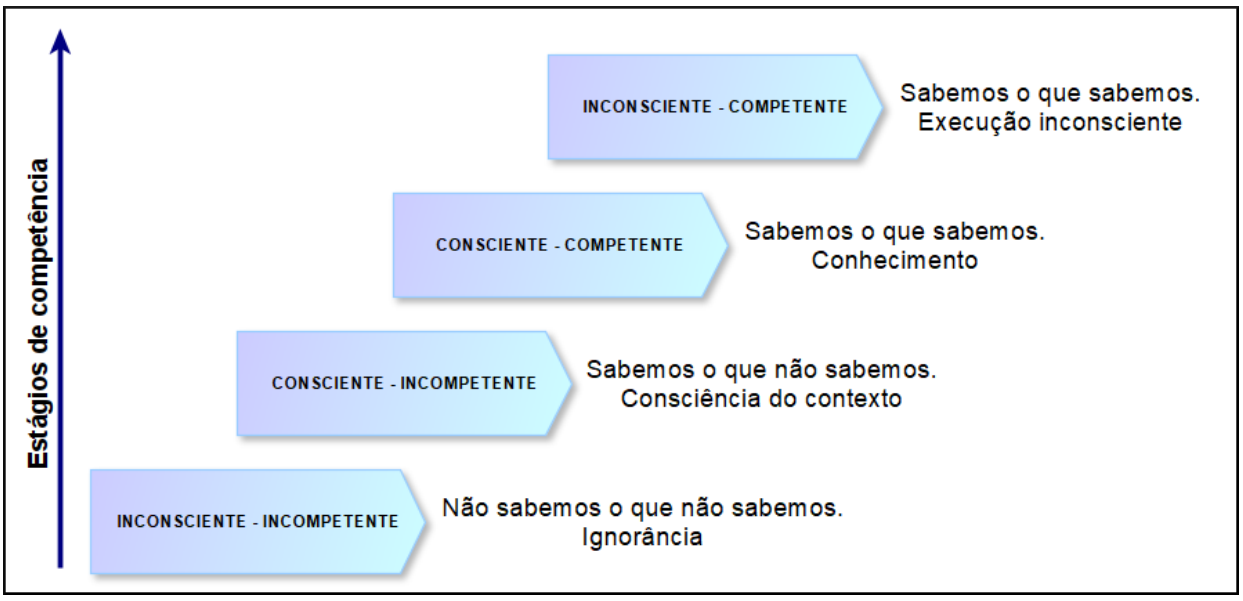


Figura 4.4: Estágios de Competência

"O que não sabemos que não sabemos" representa o estado de ignorância, a total ausência de conhecimento sobre determinado objeto. Nesta fase não conhecemos nossas vulnerabilidades, capacidades, nem as ameaças evidentes. Podemos correlacioná-lo com a Etapa de Direção da primeira Fase do ciclo de inteligência.

"O que sabemos que não sabemos" refere-se à consciência de que há algo a ser descoberto, porém, não temos esse conhecimento. É o conhecimento de uma certa vulnerabilidade, mas sem saber quem, o quê ou como ela pode ser explorada.

Expressa o estado de consciência sobre a meta a ser alcançada, seguindo a premissa de que essa meta deve ser útil, ou seja, precisa ser traduzida em ação. É a etapa mais trabalhosa do processo CTI devido à grande quantidade de dados. Pode ser correlacionada com o resultado do processamento dos dados coletados. Envolve a Etapa de Planejamento e as Fases de Coleta e de Processamento.

"O que sabemos que sabemos" corresponde à consciência e ao domínio sobre determinado assunto, é o primeiro passo para a padronização e ampliação do conhecimento.

Nesta etapa o objetivo é massificar o conhecimento. Associa-se com o resultado da Fase de Análise do ciclo de inteligência, bem como ao planejamento de ações futuras.

"O que não sabemos que sabemos" é o ápice do conhecimento, neste ponto o conhecimento está fortemente enraizado, de modo que certos processos são automatizados a ponto de passarem despercebidos. Desta forma, ao perceber uma determinada ameaça ou incidente, aciona-se automaticamente mecanismos de defesa sem a necessidade de esforço ou busca de novos conhecimentos para mitigar os efeitos da ameaça. Trata-se de proatividade, portanto, medidas para eliminar vulnerabilidades são tomadas antes que possam ser exploradas por uma ameaça. Está associada ao resultado da fase de implantação e disseminação do ciclo de inteligência. Aqui também estão as consequências, inferências e deduções do que se sabe que ainda não foram explicitadas.

## 4.3 FRAMEWORK PROPOSTO

Uma metodologia estruturada é essencial para garantir a qualidade do conhecimento. Sem uma abordagem sistemática, os analistas não seguem um processo consistente, resultando em lacuna, viés ou falta de rigor nas análises, além de gerar informações imprecisas, incompletas ou desatualizadas. Portanto, o ciclo de inteligência será o pilar fundamental do *framework* proposto. A Figura 4.5 contempla as fazes, principais ações e produto de cada fase do ciclo.

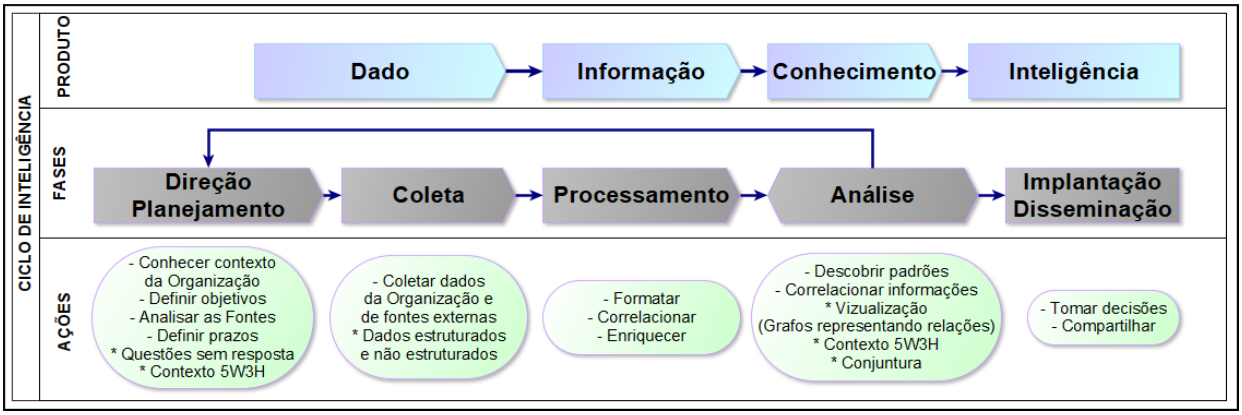


Figura 4.5: Ações, Fases e Produtos do Ciclo de Inteligência

No decorrer do processo de produção de inteligência foi empregado os estágio de competência, aliado à consciência situacional e ao método 5W3H para criar consciência situacional e esclarecer os objetivos em cada etapa do processo. O método 5W3H serve como diretriz (questões norteadoras) para identificar requisitos de inteligência e também para mensurar o resultado do processo. A medida que mais questões são respondidas melhor é a qualidade do produto gerado.

Durante a construção da consciência situacional busca-se evidências de atividades maliciosas em andamento na infraestrutura da organização. Nesse momento é essencial o domínio das táticas, técnicas e procedimentos (TTPs) empregados por atores adversários. A consciência situacional da organização serve de insumo para etapa de planejamento. A importância dessa etapa está na transição do nível inconsciente/incompetente para consciente/incompetente, também constrói uma base sólida para definição de fontes de dados externas e definição das atividades subsequentes. A metodologia proposta pode ser observada na Figura 4.6 e na descrição logo abaixo.

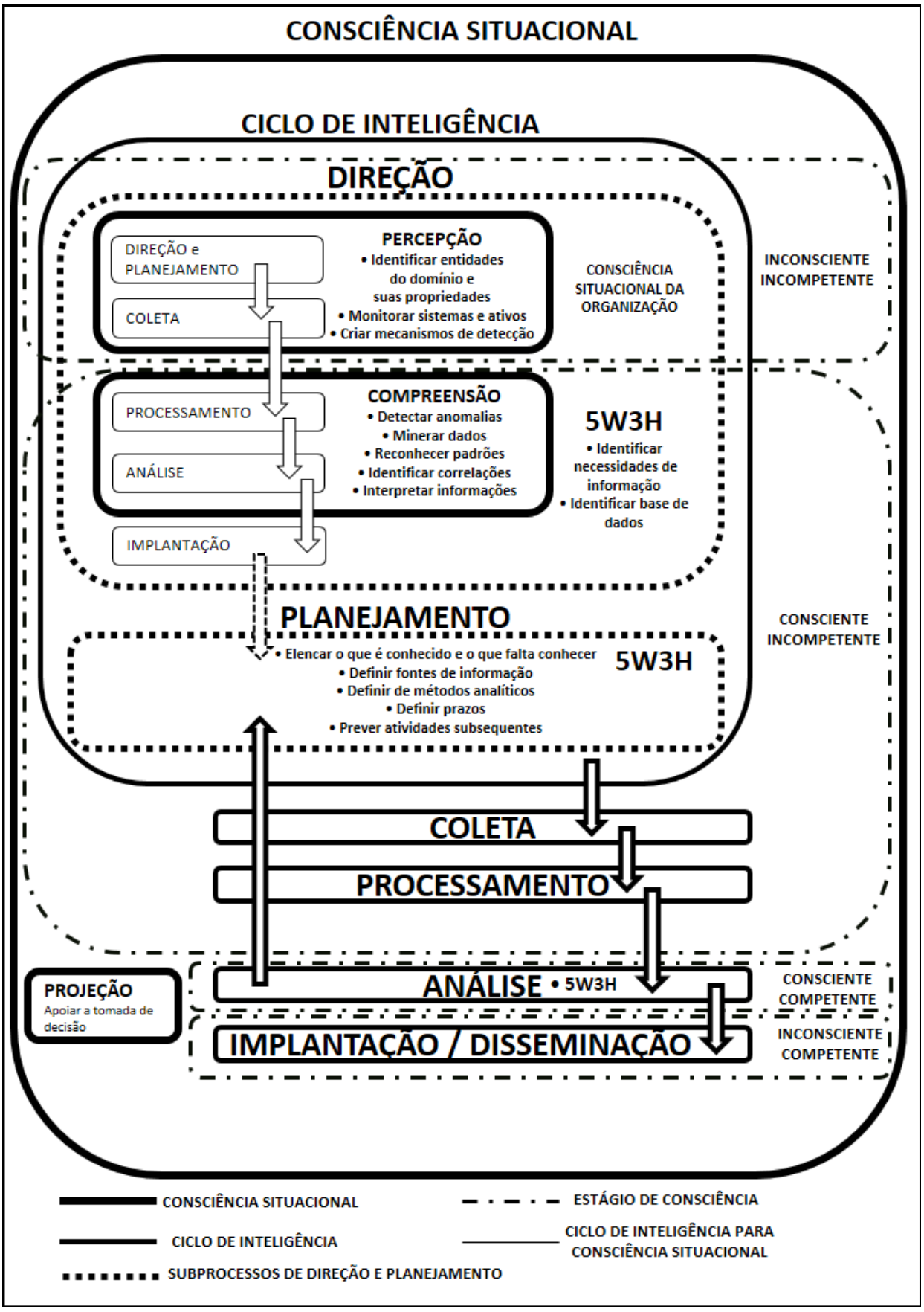


Figura 4.6: Framework para Produção de Inteligência de Ameaça Cibernética

Na fase de direção e planejamento, o primeiro passo é tomar conhecimento do cenário atual da organização, essa fase reflete em todos os processos subsequentes e pode ser retomada quando necessário. Envolve o levantamento das tecnologias utilizadas, da topologia, da análise de riscos, dos requisitos e das prioridades da organização. Nesta fase saímos do nível da ignorância, "não sabemos o que não sabemos", para a fase da consciência parcial, "sabemos que não sabemos".

Neste ponto já é possível entender o cenário interno e a partir da definição de prioridades, avaliar as vulnerabilidades existentes para cada ativo, seja software ou hardware. É crucial entender quais fatores externos influenciam a organização e os elementos que podem interessar aos agentes de ameaças. Também é fundamental coletar dados internos para comparação com dados de fontes externas, para comprovar a existência ou não de ações adversas e, dessa forma, garantir que as informações serão relevantes e precisas.

Em suma na fase de planejamento e direção é necessário estabelecer objetivos e metas, identificar as necessidades e definir as fontes de dados por meio da identificação de áreas de interesse estratégico, e das fontes de informação relevantes. Em seguida ocorre a determinação do que deve ser monitorado e analisado, assim como a lista de requisitos e preparação do plano de coleta para percepção básica de dados importantes. Então, encerra-se o nível de percepção dos elementos relacionados no contexto da ameaça que interferem nos processos de negócio da organização. No nível de compreensão ocorre a interpretação e combinação de dados para gerar conhecimento e entender a organização através da avaliação das ameaças, riscos, oportunidades, operações e aspectos tecnológicos (dispositivos de rede e aplicações), dentre outros dados coletados. Envolve a seleção de dados necessários para criar inteligência cibernética, através das informações oriundas do cruzamento de dados dos ativos da organização. Implica em desafios técnicos e cognitivos dos analistas.

Conforme o status da consciência situacional, ou seja, a primeira "foto", o analista de inteligência de ameaças já é capaz de gerar relatório, ou automatizar a disseminação de IoCs que indicam fortemente uma ameaça iminente ou um incidente, essa ação reflete o resultado da análise inicial e na sequência a disseminação, em virtude da capacidade de prever eventos futuros e suas implicações. Decorrente do impacto dessa ação o analista deve decidir por uma nova "foto" ou pela continuidade do processo. Ao decidir pela continuidade, o emprego do método 5W3H ajuda a delinear os aspectos relevantes que precisam ser conhecidos para a construção do contexto. Isso nos leva ao estágio em que estamos cientes das perguntas sem resposta. Então ocorre a definição das fontes de dados relevantes para complementar o contexto por meio das perguntas não respondidas.

Na fase de Coleta, logo após a definição das fontes e estratégia de exploração, ocorre a coleta dos dados, passando à fase de Processamento, é necessário verificar a credibilidade e validade dos dados, bem como avaliar a possibilidade de enriquecimento de acordo com o tipo de conteúdo e *plug-ins* disponíveis. Essa fase também necessita de planejamento prévio, a fim de definir que tipo de enriquecimento pode contribuir para a integralidade do contexto.

Na fase de Análise, as informações geradas pelo enriquecimento são analisadas à luz da expertise do analista de inteligência de ameaças e das correlações das informações vindas da fase de processamento. Tais informações foram originadas das correlações e padrões avistados do cruzamento de dados de fontes externas, cuja relevância foi verificada pela presença ou ausência de relacionamentos com os dados da própria organização, além de assuntos de interesse que podem afetar positiva ou negativamente os processos

de negócio.

Neste ponto, o método 5W3H é empregado novamente, a fim de verificar a completude o conhecimento, caso seja necessário, um novo planejamento é estabelecido com o objetivo de propor ações pertinentes, para nova coleta ou revisão dos *plug-ins* de enriquecimento empregados. Se a completude for satisfatória procede-se a implantação, que inclui dentro outros a proposta de diretrizes de salvaguarda, por exemplo, envio automatizado de IoCs para os sistemas de segurança cibernética, mitigação de vulnerabilidades e incidentes, confecção de relatórios para tomadores de decisão entre outras. O analista ainda pode optar por disseminar a inteligência produzida, lembrando de adicionar atributos que elevem a credibilidade, por exemplo informar a validade da inteligência e a metodologia empregada para chegar ao resultado.

Aplicação dos métodos selecionados por meio das características complementares, e principalmente o emprego do ciclo de inteligência como base, garantem a relevância, precisão e completude ao longo de todo o processo. Outras propostas de solução enfrentam pontos intermediários, como por exemplo a coleta, e não adotam medidas de verificação quanto a aplicação dos resultados. Dado o alto volume de dados disponíveis, na maioria das vezes o resultado será irrelevante, pois não tem um propósito definido.

Outros autores que desenvolvem trabalhos que propõem metodologias ou *frameworks*, enfrentam desafios para alcançar um nível adequado de qualidade da CTI gerada, que atenda aos requisitos de relevância, e precisão. A principal causa está no ponto de partida do processo, que em todos os casos é a coleta, passando pelas demais fases até a disseminação. Poucos autores conseguiram contornar esse desafio confrontando os dados coletados de fontes externas com os dados da própria organização, contudo os processos empregados, normalmente automatizados, não contemplam a verificação no nível de completude, nesse caso, embora contribuam para a relevância e precisão, não há como verificar a completude a informação produzida, logo tendo impacto na qualidade da CTI gerada.

Dada essas considerações, o *framework* proposto tende a ser uma solução de referência, visto que atende pelo menos três dos quatro fatores que exercem influência na qualidade de inteligência de ameaça cibernética

Resumidamente, a base do *framework* proposto foi o ciclo de inteligência, que na fase de direção e planejamento esteve apoiado pela consciência situacional, a fim de entender o contexto da organização, uma vez que o produto da CTI só faz sentido se apoiar a tomada de decisão, ou seja, deve ser relevante e preciso. Paralelamente, manteve-se a orientação em relação ao estágio de competência, no qual presumidamente o analista de inteligência de ameaças parte de um estágio mental de ignorância, isto significa desconhecer o desconhecido.

Nesse ponto há um detalhe interessante, assim como a consciência situacional apoia o ciclo de inteligência, o contrário também é verdadeiro. A principal motivação do emprego da consciência situacional deve-se a busca de contexto da organização. Dada as características das ações demandas, que envolvem planejamento, coleta, processamento e análise, verificamos que a aplicação do ciclo de inteligência contribui positivamente para esse processo.

Seguindo linha de complementaridade, o método 5W3H é uma ferramenta simples que permite verificar a completude do contexto a partir de perguntas norteadoras que buscam descrever a ameaça ou incidente, assim como as capacidades, seja do autor ou vetor da ameaça e também procura identificar os atores

envolvidos. Esse método já foi objeto de estudo em outras pesquisas relacionadas a inteligência de ameaça cibernética, por exemplo, [7] apresenta um modelo de avaliação de qualidade baseado na quantidade de perguntas respondidas conforme representado na Tabela 4.2.

Tabela 4.2: Níveis de Avaliação - Adaptado de [7]

| **Quantidade de Questões Respondidas** | **Percentual** | **Classificação** |
|---|---|---|
| 0-1 | 0% - 25% | Insatisfatória |
| 2-4 | 25% - 50% | Pouco Satisfatória |
| 5-6 | 50% - 75% | Satisfatória |
| 7-8 | 75% - 100% | Muito Satisfatória |

A consciência situacional realizada na etapa de direção deve ser uma ação continuada, dessa forma o analista de inteligência de ameaças cibernética mantém-se atualizado sobre o cenário atual e também é capaz de identificar questões de inteligência baseado nos processos de negócio da organização, assim iniciando um novo ciclo sem a necessidade de demandas específicas. O nível de projeção da consciência situacional não foi empregado devido a sobreposição com a fase de análise, além de que por definição prevê estados de elementos para um futuro próximo, em outras palavras, projeções de curto prazo, enquanto a análise é capaz de fornecer tendências de mais longo prazo.

A falta de planejamento para a fase de processamento pode impactar a qualidade das informações produzidas, uma vez que o volume de dados pode crescer exponencialmente sem que sejam acrescidos de relevância e dessa forma dificultando ou até inviabilizando a fase de análise. Isso decorre da característica do dado, que pode ser explorado de diversas maneiras. O processo de enriquecimento deve ser transparente de modo que as contribuições após cada rodada de enriquecimento possam ser identificadas de forma clara, essa prática aumenta o nível de confiança.

Com relação a avaliação de publicações científicas quanto a adesão ao ciclo de inteligência, a primeira abordagem para classificação foi por meio da criação de um conjunto das publicações de interesse, que tiveram seu conteúdo indexado. Baseado nesse índice foram aplicados filtros avançados com critérios de consulta condicionais com emprego dos operadores lógicos “E” e “OU”, ocorre que, durante a validação foram encontrados vários falso positivo, devido à mera menção no texto de palavras chaves sem que o assunto fosse abordado de forma consistente. A solução adotada foi realizar a leitura de todas as publicações.

Por fim, o *framework* proposto está fundamento em processo científico e metodológico de produção do conhecimento de inteligência, baseado na complementaridade de métodos. Possui facilidade de emprego, pois é independente de ferramentas, uma vez que é baseado em métodos, técnicas e sistemas de informação necessários.

# 5 CONCLUSÃO

A inteligência de ameaças sozinha não é capaz de proteger uma organização, mas complementa componentes de segurança relacionados à detecção, resposta e prevenção, com a finalidade de reduzir os possíveis danos causados por determinada ameaça por meio do aumento da eficácia dos componentes de segurança, diminuição do tempo de resposta, redução do tempo de recuperação do dano e redução do tempo de permanência do adversário no ambiente da organização.

O *framework* proposto aborda todas as fases do ciclo de inteligência, contudo, o foco principal foi sobre a fase de direção e planejamento, haja vista que é a mais negligenciada dentre as demais do ciclo de inteligência. No entanto, contribui significativamente para o desafio de melhorar a qualidade da CTI. Porém o emprego desse *framework* não deve ser entendido como condição suficiente para o êxito de um trabalho de Inteligência, mas, como condição necessária. Seu emprego contribui para garantir que todos os aspectos do problema sejam considerados, produzindo conhecimento com base científica, uniformizando procedimentos e assegurando credibilidade ao conhecimento produzido.

À medida que os componentes de segurança se tornam mais robustos por meio de informações provenientes do CTI, a previsão de ameaças se torna mais próxima da realidade, pois a mitigação de ameaças é mais inerente ao estado de segurança da organização do que ao estudo dos dados que trafegam na rede.

Embora o *framework* proposto seja capaz de produzir inteligência de ameaças cibernéticas de qualidade, prever o futuro com precisão é desafiador, a CTI pode ajudar a identificar tendências, cenários e possíveis desdobramentos com base nas informações e conhecimentos atuais. Essas projeções fornecem uma base para a tomada de decisões, mas devem ser consideradas como probabilidades e sujeitas a revisões contínuas à medida que novas informações se tornam disponíveis. Daí a necessidade do processo de consciência situacional ser continuo, a fim de detectar rapidamente qualquer alteração no cenário atual.

O *framework* proposto contribui na solução da falta de contexto e eleva o nível de consciência situacional. Graças a adoção da fase de direção e planejamento, normalmente negligenciada, uma vez que, a consciência de situação adquirida nessa fase é um dos pontos chave para a precisão das informações. Outro ponto de contribuição é a relevância, gerada a partir do cruzamento de dados de fontes externas com os dados da organização. E por fim, a adoção do método 5W3H, que, além de fácil emprego, serve de diretriz e facilita a visualização da completude da inteligência produzida. Deste modo, são abordados diretamente três dos quatro atributos que definem a qualidade da inteligência de ameaça cibernética.

Sobre a verificação de publicações científicas que abordam o ciclo de inteligência, dois pontos tem destaque. O primeiro é que apenas 2,5% abordam a fase de direção e planejamento, mesmo com a flexibilização para aumentar a abrangência da pesquisa, onde para essa fase seriam consideras nomenclaturas equivalentes, por exemplo, direção, planejamento ou definição. Isso é preocupante a medida que pesquisas aponta que a fase de direção e planejamento é determinante para a qualidade de CTI. O segundo é que 62,5% das publicações não fazem qualquer menção ao ciclo de inteligência, tampouco, a qualquer metodologia ou processo de produção de conhecimento. Essa informação precisa servir de alerta, pois esse pode ser um dos motivos para a produção de CTI de baixa qualidade.

À medida que os componentes de segurança se tornam mais robustos por meio de informações provenientes da inteligência de ameaça cibernética, a previsão de ameaças se torna mais próxima da realidade, pois a mitigação de ameaças é mais inerente ao estado de segurança da organização do que ao estudo dos elementos no seu entorno. Mas como ter certeza de que o estado de segurança é adequado, senão analisando o ambiente ao redor.

## 5.1 TRABALHOS FUTUROS

O emprego do framework proposto se traduz numa iniciativa para enfrentar o problema da falta de adoção de metodologia para produção de inteligência de ameaça, que é apontada em diversas pesquisas, mas ainda restam outros desafios que impactam na qualidade da CTI, tal como a avaliação da credibilidade das fontes, ou a transparência sobre a origem da informação.

Assim como o primeiro passo da CTI é a consciência situacional da organização, da mesma forma é imprescindível esclarecer o cenário de pesquisas sobre a inteligência de ameaça cibernética. Uma análise superficial da Tabela 4.1 "Publicações e as Fases do Ciclo de Inteligência" é o bastante para elevar o nível de atenção, a ponto de elaborar a seguinte pergunta: "É razoável que se aborde qualquer questão relacionada à disciplina de inteligência, sem que se esteja balizado por um método orientador que defina como escolher o melhor caminho e quais as melhores práticas?".

A análise mais aprofundada do cenário das pesquisas relacionadas à CTI, pode contribuir para orientar a comunidade acadêmica quanto a adoção e adequação dos conceitos da atividade de Inteligência clássica no contexto da inteligência de ameaça cibernética. Esse estudo pode analisar além de periódicos científicos revisados por pares, incluir artigos de empresas que atuam nesse setor, os chamados *"Whitepapers"*, tendo em vista que, alguns dos *"Whitepapers"* analisados no decorrer dessa pesquisa relatam o emprego do ciclo de inteligência.

O estudo do cenário atual da CTI, confrontado com uma metodologia clara e robusta para adoção de processos e procedimentos sistemáticos e consistentes, pode orientar a escolha de temas de pesquisa que proponham soluções mais unificadas, integradas e abrangentes, pois muitas das abordagens atuais parecem superficiais e fragmentadas.

Da mesma forma, estudos acerca dessa pesquisa devem ser aprofundados a fim de detalhar os processos e técnicas envolvidos em cada fase, aumentando a transparência para que possa ser facilmente compreendido, contribuindo para consistência na execução das atividades, e também para que se torne confiável e adaptável para organizações de diferentes contextos.

Nesse sentido as TIP podem ser aprimoradas para incorporar mecanismos que permitam uma melhor integração entre as fases de direção e planejamento e coleta. Atualmente não há plataformas de código aberto que incorporem de maneira simples a possibilidade de selecionar fontes de coleta baseadas no contexto da organização e em requisitos de inteligência previamente definidos.

Outra melhoria relacionada à fase de coleta, diz respeito a capacidade de decisão sobre os dados que deve permanecer armazenado, pois no decorrer do processo de produção de inteligência, muitos dados

coletados são insignificantes. A falta dessa facilidade contribui para que as TIP se tornem grandes repositórios de dados irrelevantes. Os processos dessa fase podem ser melhor detalhados seja para adotar mecanismos de avaliação da fonte e dos dados, seja para selecionar *plugins* de enriquecimento adequados para cada tipo de dado. Com base nesses avanços, será possível fortalecer a eficácia e confiabilidade da produção de inteligência de ameaça cibernética, proporcionando uma defesa mais sólida contra as ameaças digitais em constante evolução.

# REFERÊNCIAS BIBLIOGRÁFICAS


1 ABNT. *NBR ISO/IEC 27032 - Tecnologia da informação - Técnicas de segurança - Diretrizes para segurança cibernética*. Primeira. [S.l.]: Associação Brasileira de Normas Técnicas, 2015. 62 p. ISBN 978-85-07-05629-4.

2 ENDSLEY, M. Endsley, m.r.: Toward a theory of situation awareness in dynamic systems. human factors journal 37(1), 32-64. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, v. 37, p. 32–64, 03 1995.

3 CORPORATION, T. M. *MITRE ATT&CK Matrix for Enterprise*. 2023. Disponível em: <https://attack.mitre.org/matrices/enterprise/>.

4 David J. Bianco. *The Pyramid of Pain*. 2013. Disponível em: <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>.

5 SANS Internet Storm Center. *DShield API - SANS Internet Storm Center*. Disponível em: <https://www.dshield.org/api/>.

6 de Melo e Silva, A.; GONDIM, J. J. C.; de Oliveira Albuquerque, R.; VILLALBA, L. J. G. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet*, v. 12, n. 6, 2020. ISSN 19995903.

7 de Melo e Silva, A.; GONDIM, J. J. C.; de Oliveira Albuquerque, R. *Metodologia integrativa para produção de inteligência de ameaças cibernéticas utilizando plataformas de código aberto*. 72 p. Tese (Dissertação) — Universidade de Brasília, 2020. Disponível em: <https://repositorio.unb.br/handle/10482/40541>.

8 SECURITY, A. *Cyber Threatscape Report*. [S.l.], 2020. Disponível em: <https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf>.

9 ABU, M. S.; SELAMAT, S. R.; ARIFFIN, A.; YUSOF, R. Cyber threat intelligence – Issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, v. 10, n. 1, p. 371–379, 2018. ISSN 25024760.

10 CHECK, P. *Cyber securit y report 2021*. San Carlos, CA, 2021. 77 p. Disponível em: <https://pages.checkpoint.com/cyber-security-report-2021.html?utm_source=cp-home{&}utm_medium=cp-website{&}utm_campaign=pm_wr_21q1_ww_security_>.

11 HUSARI, G.; AL-SHAER, E.; AHMED, M.; CHU, B.; NIU, X. TTPDrill: Automatic and accurate extraction of threat actions from unstructured text of CTI Sources. *ACM International Conference Proceeding Series*, Association for Computing MachineryNew YorkNYUnited States, Orlando FL USA, Part F1325, p. 103–115, 2017. Disponível em: <https://dl.acm.org/doi/abs/10.1145/3134600.3134646https://doi.org/10.1145/3134600.3134646>.

12 KORTE, K. *Measuring the quality of Open Source Cyber Threat Intelligence Feeds*. 62 p. Tese (Master's thesis) — JAMK University of Applied Sciences - Finland, 2021. Disponível em: <https://www.theseus.fi/handle/10024/500534http://urn.fi/URN:NBN:fi:amk-202105178967>.

13 NIKOLAIENKO, B.; VASYLENKO, S. Application of the Threat Intelligence Platform To Increase the Security of Government Information Resources. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, v. 11, n. 4, p. 9–13, 2021. ISSN 2083-0157.

14 PREUVENEERS, D.; JOOSEN, W. Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. *Journal of Cybersecurity and Privacy*, v. 1, n. 1, p. 140–163, 2021. Disponível em: <https://doi.org/10.3390/jcp1010008https://www.mdpi.com/2624-800X/1/1/8/htm>.

15 TOUNSI, W.; RAIS, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, Elsevier Ltd, v. 72, p. 212–233, jan 2018. ISSN 01674048. Disponível em: <https://doi.org/10.1016/j.cose.2017.09.001https://linkinghub.elsevier.com/retrieve/pii/S0167404817301839>.

16 KOLOVEAS, P.; CHANTZIOS, T.; ALEVIZOPOULOU, S.; SKIADOPOULOS, S.; TRYFONOPOULOS, C. InTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics (Switzerland)*, v. 10, n. 7, 2021. ISSN 20799292.

17 SAUERWEIN, C.; FISCHER, D.; RUBSAMEN, M.; ROSENBERGER, G.; STELZER, D.; BREU, R. From Threat Data to Actionable Intelligence: An Exploratory Analysis of the Intelligence Cycle Implementation in Cyber Threat Intelligence Sharing Platforms. *ACM International Conference Proceeding Series*, 2021.

18 TEKIN, U.; YILMAZ, E. N. Obtaining Cyber Threat Intelligence Data from Twitter with Deep Learning Methods. *ISMSIT 2021 - 5th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings*, p. 82–86, 2021.

19 SCHABERREITER, T.; KUPFERSBERGER, V.; RANTOS, K.; SPYROS, A.; PAPANIKOLAOU, A.; ILIOUDIS, C.; QUIRCHMAYR, G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources. *ACM International Conference Proceeding Series*, 2019.

20 AZEVEDO, R.; MEDEIROS, I.; BESSANI, A. Automated Solution for Enrichment and Quality IoC Creation from OSINT. *Simpósio de Informática (INForum 2018)*, p. 12, 2018. Disponível em: <http://disiem-project.eu/wp-content/uploads/2018/11/INForum2018_enr-IoC.pdfhttps://www.researchgate.net/publication/327835294_Automated_Solution_for_Enrichment_and_Quality_IoC_Creation_from_OSINT>.

21 SAMTANI, S. *Developing proactive cyber threat intelligence from the online hacker community: a computational design science approach*. 206 p. Tese (Dissertação) — THE UNIVERSITY OF ARIZONA, 2018. Disponível em: <http://hdl.handle.net/10150/628454>.

22 RAHMAN, M. R.; MAHDAVI-HEZAVEH, R.; WILLIAMS, L. A Literature Review on Mining Cyberthreat Intelligence from Unstructured Texts. *IEEE International Conference on Data Mining Workshops, ICDMW*, IEEE, v. 2020-Novem, p. 516–525, nov 2020. ISSN 23759259.

23 ZHAO, J.; YAN, Q.; LIU, X.; LI, B.; ZUO, G. Cyber threat intelligence modeling based on heterogeneous graph convolutional network. In: *RAID 2020 Proceedings - 23rd International Symposium on Research in Attacks, Intrusions and Defenses*. 23rd International Symposium on Research in Attacks, Intrusions and Defenses, 2020. p. 241–256. ISBN 9781939133182. Disponível em: <https://www.usenix.org/conference/raid2020/presentation/zhao>.

24 OOSTHOEK, K.; DOERR, C. Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence*, v. 34, n. 2, p. 1–16, 2020. ISSN 15210561.

25 ZHAO, J.; YAN, Q.; LI, J.; SHAO, M.; HE, Z.; LI, B. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Computers and Security*, v. 95, 2020. ISSN 01674048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404820301395>.

26 MAVROEIDIS, V.; BROMANDER, S. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In: *2017 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 2017. v. 2017-Janua, n. March, p. 91–98. ISBN 978-1-5386-2385-5. Disponível em: <http://ieeexplore.ieee.org/document/8240774/>.

27 GANDOTRA, E.; BANSAL, D.; SOFAT, S. A framework for generating malware threat intelligence. *Scalable Computing*, v. 18, n. 3, p. 195–205, 2017. ISSN 18951767.

28 ABNT. *NBR ISO/IEC 27002 - Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação*. Terceira. [S.l.]: Associação Brasileira de Normas Técnicas, 2022. 191 p. ISBN 978-85-07-09276-6.

29 ABNT. *NBR ISO/IEC 27005 - Segurança da informação, segurança cibernética e proteção à privacidade - Orientações para gestão de riscos de segurança da informação*. Quarta. [S.l.]: Associação Brasileira de Normas Técnicas, 2023. 75 p. ISBN 978-85-07-09650-4.

30 ABNT. *NBR ISO/IEC 27701 - Técnicas de segurança - Extensão da ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e diretrizes*. Primeira. [S.l.]: Associação Brasileira de Normas Técnicas, 2019. 82 p. ISBN 978-85-07-08355-9.

31 WADLOW, T. A. *The Process of Network Security: Designing and Managing a Safe Network*. USA: Addison-Wesley Longman Publishing Co., Inc., 2000. ISBN 0201433176.

32 LI, Y.; HUANG, G.-q.; WANG, C.-z.; LI, Y.-c. Analysis framework of network security situational awareness and comparison of implementation methods. *EURASIP Journal on Wireless Communications and Networking*, EURASIP Journal on Wireless Communications and Networking, v. 2019, n. 1, p. 205, dec 2019. ISSN 1687-1499. Disponível em: <https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1506-1>.

33 BOEHM, J.; DIAS, D.; LEWIS, C.; LI, K.; WALLACE, D. *Cybersecurity trends: Looking over the horizon*. 2022. Disponível em: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon/>.

34 AMARO, L. J. B.; AZEVEDO, B. W. P.; MENDONCA, F. L. L. de; GIOZZA, W. F.; ALBUQUERQUE, R. d. O.; VILLALBA, L. J. G. Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data. *Applied Sciences (Switzerland)*, v. 12, n. 3, 2022. ISSN 20763417.

35 TOUNSI, W. *What is cyber threat intelligence and how is it evolving?* [S.l.: s.n.], 2019. 1–49 p. ISBN 9781119618393.

36 ZHANG, Q.; LI, H.; HU, J. A study on security framework against advanced persistent threat. In: *2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*. IEEE, 2017. v. 2, p. 128–131. ISBN 978-1-5090-3025-5. Disponível em: <http://ieeexplore.ieee.org/document/8076527/>.

37 CENTER, N. C. S. R. *NIST - Advanced Persistent Threat*. Disponível em: <https://csrc.nist.gov/glossary/term/advanced_persistent_threat>.

38 AHMED, Y.; ASYHARI, A.; Arafatur Rahman, M. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. *Computers, Materials & Continua*, v. 67, n. 2, p. 2497–2513, 2021. ISSN 1546-2226. Disponível em: <https://csrc.nist.gov/glossary/term/advanced_persistent_threat/https://www.techscience.com/cmc/v67n2/41316>.

39 ALSHAMRANI, A.; MYNENI, S.; CHOWDHARY, A.; HUANG, D. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys and Tutorials*, IEEE, v. 21, n. 2, p. 1851–1877, 2019. ISSN 1553877X.

40 LAB, K. *What Is an Advanced Persistent Threat (APT)?* 2022. Disponível em: <https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats>.

41 Sarah Maloney. *WHAT IS AN ADVANCED PERSISTENT THREAT (APT)?* 2018. Disponível em: <https://www.cybereason.com/blog/advanced-persistent-threat-apt>.

42 ZOU, Q.; SUN, X.; LIU, P.; SINGHAL, A. An Approach for Detection of Advanced Persistent Threat Attacks. *Computer*, v. 53, n. 12, p. 92–96, dec 2020. ISSN 0018-9162. Disponível em: <https://ieeexplore.ieee.org/document/9269909/>.

43 CHEN, P.; DESMET, L.; HUYGENS, C. A Study on Advanced Persistent Threats. In: De Decker, B.; ZÚQUETE, A. (Ed.). *Communications and Multimedia Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. p. 63–72. ISBN 978-3-662-44885-4. Disponível em: <http://link.springer.com/10.1007/978-3-662-44885-4_5>.

44 KHALID, A.; ZAINAL, A.; MAAROF, M. A.; GHALEB, F. A. Advanced Persistent Threat Detection: A Survey. *2021 3rd International Cyber Resilience Conference, CRC 2021*, n. i, 2021.

45 MELHORAMENTOS, E. *MICHAELIS*. Disponível em: <https://michaelis.uol.com.br/busca?id=PqO2A>.

46 PRESS, O. U. *Oxford Learner's Dictionaries*. Disponível em: <https://www.oxfordlearnersdictionaries.com/us/definition/english/intelligence?q=intelligence>.

47 United States, D. o. D. *US JP-2.0, Joint Intelligence*. 2013. Disponível em: <https://irp.fas.org/doddir/dod/jp2_0.pdf>.

48 VARDANGALOS, G.; BANOUTSOS, A.; PROEDROU, F.; KIOUSIS, D.; PROTOPAPAS, G. Cyber-intelligence and Cyber Counterintelligence (CCI): General definitions and principles Board of Directors. *Center For international Strategic Analyses*, 2016. Disponível em: <https://kedisa.gr/wp-content/uploads/2016/07/Cyber-intelligence-and-Cyber-Counterintelligence-CCI-General-definitions-and-principles-2.pdf>.

49 BUBACH, R.; HERKENHOFF, H. G.; HERKENOFF, L. S. B. *O cilclo da inteligência e os requisitos para a produção do conhecimento*. 125 p. Tese (Masther Thesis) — Universidade Vila Velha, 2019. Disponível em: <https://repositorio.uvv.br//handle/123456789/570>.

50 TROPOTEI, T. O. CRITICISM AGAINST THE INTELLIGENCE CYCLE. *SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE*, v. 20, p. 77–88, jun 2018. ISSN 22473173. Disponível em: <http://www.afahc.ro/ro/afases/2018/9-TeodorOctavianTROPOTEI.pdf>.

51 DUVENAGE, M. A. Intelligence Analysis in the Knowledge Age. n. March, p. 1–142, 2010.

52 Nicolae Sfetcu. *Epistemologia serviciilor de informaţii*. MultiMedia Publishing, 2020. v. 5. 248–253 p. ISBN 978-606-033-160-5. Disponível em: <https://www.telework.ro/ro/e-books/epistemologia-serviciilor-de-informatii/>.

53 ROBERTSON, K. G. Intelligence, Terrorism and Civil Liberties. *Journal of Conflict Studies*, v. 7, n. 2, p. 43–62, 1987. ISSN 1715-5673. Disponível em: <https://journals.lib.unb.ca/index.php/JCS/article/view/14756>.

54 UK, M. o. D. *JP-2-00, Understanding and Intelligence Support to Joint Operations*. 2011. 155 p. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf>.

55 RESENDEZ, C. F. L. The Intelligence Cycle as a Tool for Effective Information Security Infrastructure Design. In: *2013 European Intelligence and Security Informatics Conference*. IEEE, 2013. p. 194–197. ISBN 978-0-7695-5062-6. Disponível em: <http://ieeexplore.ieee.org/document/6657153/>.

56 Machado da Silva, R.; Costa Gondim, J. J.; de Oliveira Albuquerque, R. Methodology to Improve the Quality of Cyber Threat Intelligence Production Through Open Source Platforms. In: GARCIA, M. V.; GORDÓN-GALLEGOS, C. (Ed.). *CSEI: International Conference on Computer Science, Electronics and Industrial Engineering (CSEI)*. Cham: Springer Nature Switzerland, 2023. p. 86–98. ISBN 978-3-031-30592-4. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-031-30592-4_7https://link.springer.com/10.1007/978-3-031-30592-4_7>.

57 AYDIN, B.; OZLEBLEBICI, Z. Should We Rely on Intelligence Cycle? *Journal of Military and Information Science*, v. 3, n. 3, p. 93, may 2015. ISSN 2148-3124. Disponível em: <http://dergipark.gov.tr/doi/10.17858/jmisci.78166>.

58 LUZ, A. R. *O EMPREGO DA TÉCNICA DE AVALIAÇÃO DE DADOS (TAD) NA PRODUÇÃO DO CONHECIMENTO DE INTELIGÊNCIA*. 55 p. Tese (Pós-Graduação Lato Sensu) — Universidade do Sul de Santa Catarina - UNISUL, 2019.

59 GIOE, D. V.; GOODMAN, M. S.; STEVENS, T. Intelligence in the Cyber Era: Evolution or Revolution? *Political Science Quarterly*, v. 135, n. 2, p. 191–224, 2020. ISSN 1538165X.

60 MEDEIROS, F. de. A atividade de inteligência no mundo atual. p. 14, 2009.

61 ROSA, I.; BATISTA, R.; GONÇALVES, R.; MARTINS, J.; BRANCO, F. Cyber Threat Intelligence Architecture for Applied Cybersecurity Scenarios PhD Thesis Proposal in Web Science and Technology. In: *Iberian Conference on Information Systems and Technologies, CISTI*. IEEE, 2022. v. 2022-June, n. June 2022, p. 1–6. ISBN 9789893334362. ISSN 21660735. Disponível em: <https://ieeexplore.ieee.org/document/9820152/>.

62 NIEKERK, B. van; RAMLUCKAN, T.; DUVENAGE, P. An analysis of selected cyber intelligence texts. *European Conference on Information Warfare and Security, ECCWS*, v. 2019-July, n. Cci, p. 551–559, 2019. ISSN 20488610. Disponível em: <https://www.academia.edu/43667559/An_Analysis_of_Selected_Cyber_Intelligence_Texts>.

63 IRFAN, A. N.; CHUPRAT, S.; MAHRIN, M. N.; ARIFFIN, A. Taxonomy of Cyber Threat Intelligence Framework. In: *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2022. p. 1295–1300. ISBN 978-1-6654-9939-2. Disponível em: <https://ieeexplore.ieee.org/document/9952616/>.

64 Rob McMillan. *Definition: Threat Intelligence*. 2013. Disponível em: <https://www.gartner.com/en/documents/2487216>.

65 ZIBAK, A.; SAUERWEIN, C.; SIMPSON, A. C. Threat Intelligence Quality Dimensions for Research and Practice. *Digital Threats: Research and Practice*, p. 1–22, sep 2021. ISSN 2692-1626. Disponível em: <https://dl.acm.org/doi/10.1145/3484202>.

66 RIESCO, R.; LARRIVA-NOVO, X.; VILLAGRA, V. A. Cybersecurity threat intelligence knowledge exchange based on blockchain. *Telecommunication Systems*, v. 73, n. 2, p. 259–288, 2020. ISSN 1572-9451. Disponível em: <https://doi.org/10.1007/s11235-019-00613-4>.

67 MARTINS, C.; MEDEIROS, I. Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy. *ACM Transactions on Privacy and Security*, v. 25, n. 3, p. 1–39, aug 2022. ISSN 2471-2566. Disponível em: <https://dl.acm.org/doi/10.1145/3530977>.

68 ARIKAN, S. M.; ACAR, S. A Data Mining Based System for Automating Creation of Cyber Threat Intelligence. *9th International Symposium on Digital Forensics and Security, ISDFS 2021*, IEEE, 2021.

69 Miranda Lopez, E. *A Framework to Establish aThreat Intelligence Program*. 73 p. Dissertação (Mestrado) — Luleå University of Technology, 2021. Disponível em: <https://www.diva-portal.org/smash/record.jsf?pid=diva2{\%}3A1629834{&}dswi>.

70 ZIBAK, A.; SIMPSON, A. Cyber Threat Information Sharing: Perceived Benefits and Barriers. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, 2019. p. 1–9. ISBN 9781450371643. Disponível em: <https://dl.acm.org/doi/10.1145/3339252.3340528>.

71 STOJKOVSKI, B.; LENZINI, G.; KOENIG, V.; RIVAS, S. What s in a Cyber Threat Intelligence sharing platform? *ACM International Conference Proceeding Series*, p. 385–398, 2021.

72 SAUERWEIN, C.; SILLABER, C.; MUSSMANN, A.; BREU, R. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. *The 13th International Conference on Wirtschaftsinformatik*, p. 837–851, 2017. Disponível em: <https://wi2017.ch/images/wi2017-0188.pdfhttp://aisel.aisnet.org/wi2017/track08/paper/3>.

73 BERTI, C. B. *Modelo preditivo de situações como apoio à consciência situacional e ao processo decisório em sistemas de resposta à emergência*. 153 p. Tese (Doctorate Degree) — Universidade Federal de São Carlos, 2017. Disponível em: <https://repositorio.ufscar.br/bitstream/handle/ufscar/10119/BERT_Claudia_2018.pdf?isAllowed=y{&}sequenc>.

74 STEINBERG, A. Foundations of Situation and Threat Assessment. In: . [s.n.], 2008. p. 437–501. ISBN 9781420053098. Disponível em: <http://www.crcnetbase.com/doi/abs/10.1201/9781420053098.ch18>.

75 AHMAD, A.; MAYNARD, S. B.; DESOUZA, K. C.; KOTSIAS, J.; WHITTY, M. T.; BASKERVILLE, R. L. How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, Elsevier Ltd, v. 101, p. 102122, feb 2021. ISSN 01674048. Disponível em: <https://doi.org/10.1016/j.cose.2020.102122https://linkinghub.elsevier.com/retrieve/pii/S0167404820303953>.

76 RAZZAQ, A.; HUR, A.; AHMAD, H. F.; MASOOD, M. Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. *Proceedings - 2013 11th International Symposium on Autonomous Decentralized Systems, ISADS 2013*, IEEE, 2013.

77 LI, Y.; WANG, C. Z.; HUANG, G. Q.; ZHAO, X.; ZHANG, B.; LI, Y. C. *A Survey of Architecture and Implementation Method on Cyber Security Situation Awareness Analysis*. 2019. 927–945 p. Disponível em: <https://www.ejournal.org.cn/CN/10.3969/j.issn.0372-2112.2019.04.021>.

78 FRANKE, U.; BRYNIELSSON, J. Cyber situational awareness – A systematic review of the literature. *Computers & Security*, v. 46, p. 18–31, oct 2014. ISSN 01674048. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0167404814001011>.

79 PERC, B. W. *Modelo de referência para o desenvolvimento de aplicações de inteligência de ameaças cibernéticas e sua aplicabilidade para o compartilhamento de dados*. Tese (Dissertação de Mestrado) — Universidade de Brasília, 2020. Disponível em: <https://repositorio.unb.br/handle/10482/39792>.

80 BERADY, A.; Viet Triem Tong, V.; GUETTE, G.; BIDAN, C.; CARAT, G. Modeling the Operational Phases of APT Campaigns. In: *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2019. p. 96–101. ISBN 978-1-7281-5584-5. Disponível em: <https://ieeexplore.ieee.org/document/9071286/>.

81 BLAKE, S.; ANDY, A.; DOUG, M.; KATHRYN, N.; ADAM, P.; CODY, T. MITRE ATT&CK: Design and Philosophy - whitepaper. n. July 2018, 2020. Disponível em: <https://attack.mitre.org/resources/>.

82 YUCEL, C.; CHALKIAS, I.; MALLIS, D.; KARAGIANNIS, E.; CETINKAYA, D.; KATOS, V. On the assessment of completeness and timeliness of actionable cyber threat intelligence artefacts. *Communications in Computer and Information Science*, v. 1284 CCIS, n. January 2021, p. 51–66, 2020. ISSN 18650937.

83 BROMANDER, S. *Understanding Cyber Threat Intelligence - Towards Automation*. Tese (Doctor Thesis) — University of Oslo, 2021. Disponível em: <http://urn.nb.no/URN:NBN:no-87408https://www.duo.uio.no/handle/10852/84713>.

84 CHANTZIOS, T.; KOLOVEAS, P.; SKIADOPOULOS, S.; KOLOKOTRONIS, N.; TRYFONOPOULOS, C.; BILALI, V.-G.; KAVALLIEROS, D. The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform. In: *Proceedings of the 8th International Conference on Data Science, Technology and Applications*. SCITEPRESS - Science and Technology Publications, 2019. p. 369–376. ISBN 978-989-758-377-3. Disponível em: <http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0007978103690376>.

85 BROMANDER, S.; SWIMMER, M.; MULLER, L. P.; JØSANG, A.; EIAN, M.; SKJØTSKIFT, G.; BORG, F. Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange. *Digital Threats: Research and Practice*, v. 3, n. 1, p. 1–22, mar 2022. ISSN 2692-1626. Disponível em: <https://dl.acm.org/doi/10.1145/3458027>.

86 GAO, Y.; LI, X.; PENG, H.; FANG, B.; YU, P. S. HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. *IEEE Transactions on Knowledge and Data Engineering*, IEEE, v. 34, n. 2, p. 708–722, feb 2022. ISSN 1041-4347. Disponível em: <https://ieeexplore.ieee.org/document/9072563/>.

87 FAIELLA, M.; GONZALEZ-GRANADILLO, G.; MEDEIROS, I.; AZEVEDO, R.; GONZALEZ-ZARZOSA, S. Enriching threat intelligence platforms capabilities. *ICETE 2019 - Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*, v. 2, n. Icete, p. 37–48, 2019.

88 GONZÁLEZ-GRANADILLO, G.; FAIELLA, M.; MEDEIROS, I.; AZEVEDO, R.; GONZÁLEZ-ZARZOSA, S. ETIP: An Enriched Threat Intelligence Platform for improving OSINT correlation, analysis, visualization and sharing capabilities. *Journal of Information Security and Applications*, Elsevier Ltd, v. 58, n. February, p. 102715, may 2021. ISSN 22142126. Disponível em: <https://doi.org/10.1016/j.jisa.2020.102715https://linkinghub.elsevier.com/retrieve/pii/S2214212620308589>.

89 VIELBERTH, M.; MENGES, F.; PERNUL, G. Human-as-a-security-sensor for harvesting threat intelligence. *Cybersecurity*, Cybersecurity, v. 2, n. 1, p. 23, dec 2019. ISSN 2523-3246. Disponível em: <https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0040-0>.

90 BASHEER, R.; ALKHATIB, B. Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. *Journal of Computer Networks and Communications*, v. 2021, p. 1–21, dec 2021. ISSN 2090-715X. Disponível em: <https://www.hindawi.com/journals/jcnc/2021/1302999/>.

91 SCHLETTE, D.; BÖHM, F.; CASELLI, M.; PERNUL, G. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, Springer Berlin Heidelberg, v. 20, n. 1, p. 21–38, 2021. ISSN 16155270. Disponível em: <https://doi.org/10.1007/s10207-020-00490-y>.

92 PAPAIOANNOU, F. *Threat Intelligence Platforms evaluation*. Tese (Master's Thesis) — University of Piraeus, 2021. Disponível em: <https://dione.lib.unipi.gr/xmlui/handle/unipi/13346http://dx.doi.org/10.26267/unipi_dione/769>.

93 HETTEMA, H. Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence. *Computers and Security*, Elsevier Ltd, v. 109, p. 102396, 2021. ISSN 01674048. Disponível em: <https://doi.org/10.1016/j.cose.2021.102396>.

94 SAKELLARIOU, G.; FOULIRAS, P.; MAVRIDIS, I.; SARIGIANNIDIS, P. A Reference Model for Cyber Threat Intelligence (CTI) Systems. *Electronics*, v. 11, n. 9, p. 1401, apr 2022. ISSN 2079-9292. Disponível em: <https://www.mdpi.com/2079-9292/11/9/1401>.

95 WANG, J.; LIU, Y.; LI, P.; LIN, Z.; SINDAKIS, S.; AGGARWAL, S. Overview of Data Quality: Examining the Dimensions, Antecedents, and Impacts of Data Quality. *Journal of the Knowledge Economy*, n. 0123456789, 2023. ISSN 1868-7865.

96 QIANG, L.; ZHENGWEI, J.; ZEMING, Y.; BAOXU, L.; XIN, W.; YUNAN, Z. A Quality Evaluation Method of Cyber Threat Intelligence in User Perspective. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, IEEE, p. 269–276, 2018.

97 SILLABER, C.; SAUERWEIN, C.; MUSSMANN, A.; BREU, R. Data quality challenges and future research directions in threat intelligence sharing practice. *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, p. 65–70, 2016.

98 PAWLIŃSKI, P.; JAROSZEWSKI, P.; KIJEWSKI, P.; SIEWIERSKI, L.; JACEWICZ, P.; ZIELONY, P.; ŻUBER, R. *Actionable Information for Security Incident Response*. [s.n.], 2014. 1–79 p. ISBN 9789292041076. Disponível em: <https://www.enisa.europa.eu/publications/actionable-information-for-security>.

99 JOHNSON, C. S.; BADGER, M. L.; WALTERMIRE, D. A.; SNYDER, J.; SKORUPKA, C. *Guide to Cyber Threat Information Sharing*. Gaithersburg, MD, 2016. v. 150, 35 p. Disponível em: <http://csrc.nist.gov/publications/PubsSPs.htmlhttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.

100 European Union Agency for Network and Information Security (ENISA). Exploring the opportunities and limitations of current Threat Intelligence Platforms. n. December, p. 42, 2017. Disponível em: <https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019>.

101 ZIBAK, A.; SAUERWEIN, C.; SIMPSON, A. A success model for cyber threat intelligence management platforms. *Computers and Security*, Elsevier Ltd, v. 111, p. 102466, 2021. ISSN 01674048. Disponível em: <https://doi.org/10.1016/j.cose.2021.102466>.

102 VERIZON. *Data, 2016 Breach Investigations Report*. [S.l.], 2016. 85 p. Disponível em: <https://cdn2.hubspot.net/hubfs/340834/Documents_-_Contact_Attachments_for_CRM_records_in_HS/rp_DBIR_2016_Report_en_xg.pdfhttps://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2b_Verizon_Data-Breach-Investigations-Report_2016_R>.

103 WAGNER, T. D.; MAHBUB, K.; PALOMAR, E.; ABDALLAH, A. E. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, Elsevier Ltd, v. 87, p. 101589, nov 2019. ISSN 01674048. Disponível em: <https://doi.org/10.1016/j.cose.2019.101589https://linkinghub.elsevier.com/retrieve/pii/S016740481830467X>.

104 MAYMI, F.; BIXLER, R.; JONES, R.; LATHROP, S. Towards a definition of cyberspace tactics, techniques and procedures. In: *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017. p. 4674–4679. ISBN 978-1-5386-2715-0. Disponível em: <http://ieeexplore.ieee.org/document/8258514/>.

105 KHAROUNI, L.; HACQUEBORD, F.; HUQ, N.; GOGOLINSKI, J.; MERCÊS, F.; REMORIN, A.; OTIS, D. *Operation Pawn Storm: Using Decoys to Evade Detection [white paper]*. 2014. 1–21 p. Disponível em: <https://documents.trendmicro.com/assets/wp/wp-operation-pawn-storm.pdf>.

106 CHAWLA, A. Pegasus Spyware – 'A Privacy Killer'. *SSRN Electronic Journal*, 2021. ISSN 1556-5068. Disponível em: <https://www.ssrn.com/abstract=3890657>.

107 ZHANG, H.; YI, Y.; WANG, J.; CAO, N.; DUAN, Q. Network security situation awareness framework based on threat intelligence. *Computers, Materials and Continua*, v. 56, n. 3, p. 381–399, 2018. ISSN 15462226.

108 JIRSIK, T.; CELEDA, P. *Cyber Situation Awareness via IP Flow Monitoring*. 181 p. Tese (Doctoral Thesis) — Masaryk University, 2018.

109 ÜNAL, U.; KAHYA, C. N.; KURTLUTEPE, Y.; DAğ, H. Investigation of Cyber Situation Awareness via SIEM tools: a constructive review. *Proceedings - 6th International Conference on Computer Science and Engineering, UBMK 2021*, IEEE, p. 676–681, 2021.

110 WEBB, J.; AHMAD, A.; MAYNARD, S. B.; SHANKS, G. A situation awareness model for information security risk management. *Computers & Security*, v. 44, p. 1–15, 2014. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404814000571>.

111 GATEWAY, B.; HAGUE, T. Consciousness , Competence , and Organizational Change. v. 47, n. 4, p. 32–38, 2019.

112 HARIANTO, G. Model by Abraham Maslow as Four Stage of Learning. *Inculco Journal of Christian Education*, v. 1, n. 1, p. 45–52, 2021.

113 YEBOAH-OFORI, A.; ISLAM, S.; LEE, S. W.; SHAMSZAMAN, Z. U.; MUHAMMAD, K.; ALTAF, M.; AL-RAKHAMI, M. S. Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. *IEEE Access*, v. 9, p. 94318–94337, 2021. ISSN 2169-3536. Disponível em: <https://ieeexplore.ieee.org/document/9448097/>.

114 ZHU, Z.; DUMITRAS, T. ChainSmith: Automatically Learning the Semantics of Malicious Campaigns by Mining Threat Intelligence Reports. In: *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018. p. 458–472. ISBN 978-1-5386-4228-3. Disponível em: <https://ieeexplore.ieee.org/document/8406617/>.

115 SÜLÜ, M.; DAŞ, R. Graph Visualization of Cyber Threat Intelligence Data for Analysis of Cyber Attacks. *Balkan Journal of Electrical and Computer Engineering*, n. August, jul 2022. ISSN 2147-284X. Disponível em: <https://dergipark.org.tr/en/doi/10.17694/bajece.1090145>.

116 SOLANGE, V.; LEGOY, M.; THESIS, M. S.; CASELLI, M. *Retrieving ATT&CK tactics and techniques in cyber threat reports*. Tese (M.Sc. Thesis) — University of Twente, 2019. Disponível em: <http://purl.utwente.nl/essays/80012>.

117 SARHAN, I.; SPRUIT, M. Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph. *Knowledge-Based Systems*, Elsevier B.V., v. 233, p. 107524, 2021. ISSN 09507051. Disponível em: <https://doi.org/10.1016/j.knosys.2021.107524>.

118 RAHMAN, M. R.; MAHDAVI-HEZAVEH, R.; WILLIAMS, L. What are the attackers doing now? Automating cyber threat intelligence extraction from text on pace with the changing threat landscape: A survey. *CSUR '21: ACM Computing Survey*, Association for Computing Machinery, v. 1, n. 1, p. 1–35, 2021. Disponível em: <http://arxiv.org/abs/2109.06808>.

119 SAMTANI, S.; ABATE, M.; BENJAMIN, V.; LI, W. Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, n. September, 2020. Disponível em: <https://link.springer.com/referenceworkentry/10.1007/978-3-319-90307-1_8-1>.

120 PINCOVSCY, J. A.; GONDIM, J. J. C. *Metodologia Para Inteligência De Ameaças Cibernéticas Com Integração De Sensores*. Tese (Doutorado) — Universidade de Brasília - UNB, 2022. Disponível em: <https://ppee.unb.br/wp-content/uploads/2023/01/METODOLOGIA-PARA-INTELIGENCIA.pdf>.

121 BAUER, S.; FISCHER, D.; SAUERWEIN, C.; LATZEL, S.; STELZER, D.; BREU, R. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In: . [s.n.], 2020. p. 10. Disponível em: <https://hdl.handle.net/10125/63978>.

122 SUN, T.; YANG, P.; LI, M.; LIAO, S. An automatic generation approach of the cyber threat intelligence records based on multi-source information fusion. *Future Internet*, v. 13, n. 2, p. 1–19, 2021. ISSN 19995903. Disponível em: <https://doi.org/10.3390/fi13020040https://www.mdpi.com/1999-5903/13/2/40/htm>.

123 ALMOHANNADI, H.; AWAN, I.; Al Hamar, J.; CULLEN, A.; DISSO, J. P.; ARMITAGE, L. Cyber Threat Intelligence from Honeypot Data Using Elasticsearch. In: *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2018. v. 2018-May, p. 900–906. ISBN 978-1-5386-2195-0. ISSN 1550445X. Disponível em: <https://ieeexplore.ieee.org/document/8432334/>.

124 KIM, B. I.; KIM, N.; LEE, S.; CHO, H.; PARK, J. A Study on a Cyber Threat Intelligence Analysis (CTI) Platform for the Proactive Detection of Cyber Attacks Based on Automated Analysis. *2018 International Conference on Platform Technology and Service, PlatCon 2018*, IEEE, p. 1–4, 2018.

125 BAYER, M.; FREY, T.; REUTER, C. Multi-Level Fine-Tuning, Data Augmentation, and Few-Shot Learning for Specialized Cyber Threat Intelligence. jul 2022. Disponível em: <http://arxiv.org/abs/2207.11076>.

126 RAHMAN, M. R.; WILLIAMS, L. From Threat Reports to Continuous Threat Intelligence: A Comparison of Attack Technique Extraction Methods from Textual Artifacts. 2022. Disponível em: <http://arxiv.org/abs/2210.02601https://doi.org/10.48550/arXiv.2210.02601>.

127 AFZALISERESHT, N.; MIAO, Y.; MICHALSKA, S.; LIU, Q.; WANG, H. From logs to Stories: Human-centred data mining for cyber threat intelligence. *IEEE Access*, v. 8, p. 19089–19099, 2020. ISSN 21693536.

128 ZHOU, Y.; TANG, Y.; YI, M.; XI, C.; LU, H. CTI View: APT Threat Intelligence Analysis System. *Security and Communication Networks*, v. 2022, n. December 2015, p. 1–15, jan 2022. ISSN 1939-0122. Disponível em: <https://www.hindawi.com/journals/scn/2022/9875199/>.

129 ABU, M. S.; ARIFFIN, A.; SELAMAT, S. R.; YUSOF, R. An attribution of cyberattack using association rule mining (ARM). *International Journal of Advanced Computer Science and Applications*, v. 11, n. 2, p. 352–358, 2020. ISSN 21565570. Disponível em: <https://pdfs.semanticscholar.org/bffe/538023f3dbd7bf4db437f233e60552df40e8.pdfhttps://thesai.org/Publications/ViewPaper?Volume=11{&}Issue=2{&}Code=IJACSA{&}Se>.

130 WANG, M.; YANG, L.; LOU, W. A Comprehensive Dynamic Quality Assessment Method for Cyber Threat Intelligence. In: *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2022. p. 178–181. ISBN 978-1-6654-0262-0. Disponível em: <https://ieeexplore.ieee.org/document/9833837/>.

131 NGUYEN, C.; MORGAN, C.; MITTAL, S. *Poster CTI4AI: Threat Intelligence Generation and Sharing after Red Teaming AI Models*. [S.l.]: Association for Computing Machinery, 2022. v. 1. 3431–3433 p. ISSN 15437221. ISBN 9781450394505.

132 ANGELELLI, M.; ARIMA, S.; CATALANO, C.; CIAVOLINO, E. Cyber-risk Perception and Prioritization for Decision-Making and Threat Intelligence. 2023. Disponível em: <http://arxiv.org/abs/2302.08348>.

133 ZENEBE, A.; SHUMBA, M.; CARILLO, A.; CUENCA, S. Cyber threat discovery from dark web. *EPiC Series in Computing*, v. 64, p. 174–183, 2019. ISSN 23987340.

134 GAO, Y.; LI, X.; LI, J.; GAO, Y.; GUO, N. Graph Mining-based Trust Evaluation Mechanism with Multidimensional Features for Large-scale Heterogeneous Threat Intelligence. In: *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018. p. 1272–1277. ISBN 978-1-5386-5035-6. Disponível em: <https://ieeexplore.ieee.org/document/8622111/>.

135 PIPLAI, A.; MITTAL, S.; ABDELSALAM, M.; GUPTA, M.; JOSHI, A.; FININ, T. Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior. In: *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 2020. p. 1–6. ISBN 978-1-7281-8800-3. Disponível em: <https://ieeexplore.ieee.org/document/9280512/>.

136 MERAH, Y.; KENAZA, T. Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence. In: *The 16th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, 2021. p. 1–8. ISBN 9781450390514. Disponível em: <https://dl.acm.org/doi/10.1145/3465481.3470024>.

137 BURGER, E. W.; GOODMAN, M. D.; KAMPANAKIS, P.; ZHU, K. A. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. In: *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security - WISCS '14*. New York, New York, USA: ACM Press, 2014. v. 2014-Novem, n. November, p. 51–60. ISBN 9781450331517. ISSN 15437221. Disponível em: <http://dl.acm.org/citation.cfm?doid=2663876.2663883>.

138 MAVROEIDIS, V.; HOHIMER, R.; CASEY, T.; JESANG, A. Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. In: *2021 13th International Conference on Cyber Conflict (CyCon)*. IEEE, 2021. v. 2021-May, n. 303585, p. 327–352. ISBN 978-9916-9565-5-7. ISSN 23255374. Disponível em: <https://ieeexplore.ieee.org/document/9468305/>.

139 ALMASHOR, M.; AHMED, E.; PICK, B.; ABUADBBA, S.; XUE, J.; GAIRE, R.; WANG, S.; CAMTEPE, S.; NEPAL, S. Unraveling Threat Intelligence Through the Lens of Malicious URL Campaigns. *INFORMS journal on computing*, aug 2022. Disponível em: <http://arxiv.org/abs/2208.12449>.

140 BERNDT, A.; OPHOFF, J. Exploring the Value of a Cyber Threat Intelligence Function in an Organization. In: *IFIP Advances in Information and Communication Technology*. Springer International

Publishing, 2020. v. 579 IFIP, p. 96–109. ISBN 9783030592905. ISSN 1868422X. Disponível em: <https://link.springer.com/10.1007/978-3-030-59291-2_7>.

141 ORBINATO, V.; BARBARACI, M.; NATELLA, R.; COTRONEO, D. Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study: (Practical Experience Report). *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*, v. 2022-Octob, p. 181–192, 2022. ISSN 10719458.

142 WAGNER, C.; DULAUNOY, A.; WAGENER, G.; IKLODY, A. MISP - The design and implementation of a collaborative threat intelligence sharing platform. *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, p. 49–56, 2016.

143 DUNNETT, K.; PAL, S.; PUTRA, G. D.; JADIDI, Z.; JURDAK, R. A Trusted, Verifiable and Differential Cyber Threat Intelligence Sharing Framework using Blockchain. In: *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2022. p. 1107–1114. ISBN 978-1-6654-9425-0. Disponível em: <https://ieeexplore.ieee.org/document/10063731/>.

144 SCHLETTE, D.; CASELLI, M.; PERNUL, G. A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, v. 23, n. 4, p. 2525–2556, 2021. ISSN 1553-877X. Disponível em: <https://ieeexplore.ieee.org/document/9557787/>.

145 CONTI, M.; DARGAHI, T.; DEHGHANTANHA, A. Cyber Threat Intelligence: Challenges and Opportunities. In: *Advances in Information Security*. [s.n.], 2018. v. 70, p. 1–6. Disponível em: <http://link.springer.com/10.1007/978-3-319-73951-9_1>.

146 BROWN, R.; LEE, R. M. *2021 SANS Cyber Threat Intelligence ( CTI ) Survey Written by Rebekah Brown*. [S.l.], 2021.

147 SLOAN, M. Aristotle's as the Original Locus for the Septem Circumstantiae. *Classical Philology*, v. 105, p. 236–251, 2010.

148 BUSINESSBALLS. *Conscious Competence Learning Model*. Disponível em: <https://www.businessballs.com/self-awareness/conscious-competence-learning-model/{\#}theories_models_change_learn>.