risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 23/09/2023
Aceitação/Acceptance: 29/11/2023

Análise de Feeds de Inteligência de Ataques DDoS sob a Ótica da Qualidade da Informação

Edvan Gomes da Silva[1], Alexander Andre de Souza Vieira[1],
Luiz Augusto dos Santos Pires[1], Robson de Oliveira Albuquerque[1],
Rafael Rabelo Nunes[1,2]

edvan402@gmail.com; aaalexander95@gmail.com; luiz.pires11@gmail.com; robson@redes.unb.br; rafaelrabelo@unb.br

[1] Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - Zipcode 70910-900.

[2] Centro Universitário UniAtenas, Paracatu-MG, Brasil – Zipcode 38602-108.

Pages: 622-635

Resumo: A segurança de servidores web é uma preocupação crítica para organizações diante de ameaças cibernéticas, entre elas os ataques de negação de serviço distribuídos (DDoS). Em um ambiente onde a disponibilidade online é vital, informações confiáveis desempenham um papel crucial na proteção contra ataques cibernéticos. Nesse sentido, o uso de feeds de inteligência desempenha um papel preventivo crucial no reforço da segurança cibernética. Este estudo elaborou métricas para avaliar a qualidade de feeds de inteligência e utilizou essas métricas para analisar relatórios de empresas de segurança cibernética, focando em ataques DDoS recentes, buscando aprimorar critérios de avaliação da qualidade desses relatórios com o objetivo de auxiliar equipes de TI na tomada de decisão sobre sua utilidade na modelagem de ameaças e estratégia de defesa contra ataques DDoS. A análise revelou deficiências em completude, oportunidade e capacidade de ação, variando entre as fontes de informação. Essas descobertas têm implicações significativas para equipes de TI ao considerar a utilidade desses relatórios na modelagem de ameaças e estratégias de defesa contra DDoS.

Palavras-chave: Inteligência de Ameaça Cibernética; AlienVault; DDoS; Relatórios.

Analysis of DDoS Attack Intelligence Feeds from the Perspective of Information Quality

Abstract: Web server security is a critical concern for organizations facing cyber threats and among them there are Distributed Denial of Service (DDoS) attacks. Considering systems where online availability is crucial, reliable information plays an important role in protecting against cyberattacks. In this sense, the use of intelligence feeds helps strengthening cybersecurity. This work assessed cybersecurity reports, focusing on recent DDoS attacks, aiming to enhance metrics for evaluating the quality of such reports. To achieve this, metrics were developed

to evaluate the quality of the reports considered in this study. The main objective is to assist IT teams in decision-making regarding their utility in threat modeling and DDoS defense strategy. The analysis revealed deficiencies in completeness, timeliness, and actionable information, varying among different information sources. These findings have significant implications for IT teams when considering the utility of these reports in threat modeling and DDoS defense strategies.

Keywords: Cyber Threat Intelligence; AlienVault; DDoS; Reports.

1. Introdução

O avanço tecnológico e a digitalização das atividades impuseram desafios substanciais em relação à segurança da informação. Um dos desafios preeminentes enfrentados por organizações e indivíduos é o aumento dos ataques Distributed Denial of Service (DDoS), que buscam sobrecarregar sistemas ou redes, tornando-os indisponíveis para usuários legítimos (Akamai, 2023). No setor público, que é um alvo frequente de ataques cibernéticos, a segurança é de extrema importância (Georg et al., 2023). Portanto, é fundamental realizar planejamento de segurança e investimentos para se adaptar às novas realidades (Trinks et al., 2022).

Nesse contexto, os relatórios de Cyber Threat Intelligence (CTI) fornecem informações sobre as ameaças cibernéticas mais recentes, incluindo seus métodos, objetivos e vetores de ataque. Com essas informações, as organizações podem identificar possíveis pontos fracos em sua infraestrutura de segurança e tomar medidas para corrigi-los antes que sejam explorados por atacantes (Cisco, 2023).

Esses relatórios são elaborados por equipes especializadas em segurança. Normalmente fazem uso de um ciclo que envolve a coleta, análise e interpretação das informações sobre ameaças, vulnerabilidades e tendências no cenário de segurança cibernética. Por meio dos dados incluídos em relatórios de CTI é possível saber quem são os possíveis atacantes, como eles operam e quais são seus objetivos, além de obter insights valiosos para a prevenção, detecção e resposta a incidentes de segurança (TIVIT, 2023).

Em paralelo, a qualidade da informação tornou-se um aspecto crítico na era digital. Devido à ubiqüidade dos dados eletrônicos, a qualidade dos dados desempenha um papel crucial em todas as aplicações comerciais e governamentais. A qualidade dos dados é amplamente reconhecida como um fator crítico que impacta o desempenho dos processos operacionais (Eckerson, W. W., 2006).

Considerando tais aspectos, o objetivo deste trabalho é realizar uma análise dos atributos de qualidade da informação presentes em relatórios selecionados sobre ataques DDoS, em particular, os disponíveis na plataforma Alien Vault. Para uma compreensão completa deste estudo, será apresentado os conceitos relacionados aos ataques DDoS, aos repositórios de CTI e à qualidade da informação. Os resultados mostram que algumas características de qualidade da informação evidenciam deficiências, mesmo diante da relevância e confiabilidade das fontes.

A pesquisa em questão segue uma estrutura que se desdobra em várias seções distintas. Além desta introdução, a seção 2 é dedicada à construção do arcabouço teórico, incluindo aspectos sobre DDoS e realizando uma revisão concisa dos conceitos relacionados

aos repositórios de CTI, além de abordar a conceituação da qualidade da informação, incluindo suas múltiplas dimensões. A seção 3 procede com uma revisão da literatura que engloba trabalhos previamente desenvolvidos sobre o tema abordado. A seção 4 descreve a metodologia empregada na condução deste estudo. A seção 5 apresenta de maneira sistemática os resultados obtidos e consequente análise. Por fim, a seção 6 consolida as descobertas obtidas ao longo da pesquisa e faz o fechamento do trabalho.

2. Referencial Teórico

2.1. Ataques Distributed Denial of Service (DDoS)

Os ataques DDoS têm suscitado crescente apreensão devido ao incremento em sua escala, como documentado por fontes como Cloudflare (2023), que relata a coordenação de um conjunto de dispositivos comprometidos capazes de gerar tráfego na ordem de terabits por segundo (Tbps). Adicionalmente, sua frequência tem demonstrado um aumento significativo, como evidenciado no relatório da (Radware, 2023), que apontam ocorrências de ataques dirigidos tanto a usuários domésticos quanto a entidades governamentais e empresariais

A finalidade desse tipo de ataque é sobrecarregar de maneira deliberada as capacidades de processamento e a largura de banda de alvos específicos. Isso é alcançado através do aumento significativo do tráfego de rede, utilizando malware que se propaga automaticamente, como os botnets (Gondim et al., 2020). Este fenômeno se caracteriza por uma configuração em três fases discretas, nomeadamente, recrutamento de dispositivos, disseminação de informações e execução do ataque, além da presença de quatro elementos distintos, conforme elucidado na investigação realizada por Mahjabin et al. (2017). Estes quatro elementos consistem no atacante, múltiplos controladores, múltiplos dispositivos zumbis e a vítima (máquina alvo do ataque).

Além disso, é importante ressaltar que os ataques podem ser categorizados em três principais grupos (Mahjabin et al., 2017). O primeiro deles busca esgotar os recursos de largura de banda dos canais de comunicação com a vítima (James, Kevin, 2023). O segundo grupo visa esgotar os recursos do sistema da vítima, incluindo memória, sockets e CPU (Liu et al., 2009). Por fim, temos os ataques zero day, que são aqueles que não possuem defesa prévia estabelecida (SentinelOne, 2021).

Existem diversas estratégias mitigatórias para prevenir ataques DDoS. Entre essas abordagens, destacam-se métodos de filtragem que são eficazes na abordagem de falsificação de endereço IP, como documentado em pesquisas anteriores, como os estudos de Ferguson e Senie (2000) e Jin et al. (2003). Outra tática relevante envolve a implementação de *honeypots*, concebidos para ludibriar os atacantes e colher informações destinadas a combater os ataques DDoS, conforme ilustrado no trabalho de Weiler (2002). Além disso, a distribuição equilibrada de carga entre os servidores, uma proposição apresentada por McMullin (2016), é uma estratégia adotada para mitigar esses ataques. Por fim, a conscientização dos usuários, especialmente em ambientes de segurança frágil, como ambientes de Internet das Coisas (IoT), desempenha um papel fundamental na prevenção de ataques DDoS.

A prevenção dos ataques é fundamental para defender grande parte dos ataques DDoS, porém ainda existirão atualizações e ataques com novas assinaturas. Para garantir a defesa nestes casos é necessário implementar mecanismos de mitigação como a detecção e resposta aos ataques (Mahjabin et al, 2017). Sobre a detecção pode-se usar mecanimos de detecção por assinatura, detecção por anomalia ou ambas em conjunto (Zekri, 2017). Já em relação a resposta aos ataques normalmente usa-se técnicas de filtragem ou limita-se a taxa de envio de pacotes por origem a depender da precisão dos mecanismos de detecção dos ataques (Kaspersky, 2022).

2.2. Qualidade da informação

A qualidade dos dados desempenha uma função de primordial relevância em todas as aplicações de caráter comercial e governamental, dado o amplo alcance da disseminação de dados eletrônicos, conforme (Batini et al., 2009). No cenário em constante evolução, marcado pela crescente complexidade das estruturas organizacionais, a importância da qualidade dos dados e da informação assume um caráter ainda mais preponderante para todas as instituições, influenciando de modo significativo as tomadas de decisão em todas as instâncias (O'Brien, 2015).

A classificação das dimensões relacionadas à qualidade dos dados tem sido amplamente explorada na literatura. No entanto, divergências significativas permeiam as definições da maioria dessas dimensões, resultantes da natureza intrinsecamente contextual da qualidade dos dados (Batini et al., 2009). O conceito de "adequação ao uso" emerge como um pilar fundamental na literatura sobre qualidade de dados, destacando a importância de adotar uma perspectiva centrada no consumidor dos dados em relação à qualidade, uma vez que é o próprio usuário final quem, em última análise, avaliará se a informação é ou não adequada para sua finalidade específica (Wang & Strong, 1996).

(Caltagirone, 2022) destaca que atualmente não existe uma ciência estabelecida para avaliar a qualidade dos relatórios de inteligência de ameaças. Entretanto, isso não significa que não seja possível criar uma forma de avaliação. Na verdade, as organizações precisam se esforçar um pouco mais para buscar características qualitativas que permitam avaliar periodicamente seus fornecedores de informações de inteligência de ameaças.

No estudo de Griffioen, Booij e Doerr (2020), é mencionado que Pawlinski e Kompanek propuseram uma taxonomia para avaliar a inteligência de ameaças através das dimensões de *Relevance*, *Accuracy*, *Completeness*, *Timeliness* e *Ingestibility*. Em sua publicação, (Caltagirone, 2022) propõe um acrônimo denominado CART - *Completeness, Accuracy, Relevance & Timeliness* e destaca a importância dessas dimensões para avaliar a qualidade dos provedores de informações de tecnologia da informação.

Roberts e Brown (2017) enfatizam duas dimensões essenciais: *Actionability e Credibility*. Na dimensão *Actionability*, os autores sustentam que os produtos de inteligência devem demonstrar utilidade prática, ou seja, fornecer informações precisas no formato apropriado, permitindo que o consumidor tome ações ou decisões mais informadas do que seria possível sem o auxílio do produto.

A dimensão *Credibility* realça a importância de possuir profundo conhecimento sobre o tema tratado, a fim de escrever com autoridade e de estar familiarizado com o público-

alvo. Isso é crucial para transmitir as informações de forma a atender às necessidades específicas da audiência. Os autores alertam que a ausência desses requisitos pode resultar em produtos de inteligência defeituosos e com baixa credibilidade, levando ao desperdício de informações valiosas que não são compreendidas devidamente (Roberts & Brown, 2017).

2.3. Repositórios de CTI

De acordo com Barnum (2012), o conceito de Inteligência de Ameaça Cibernética (CTI) surgiu como uma resposta preventiva a uma variedade de ameaças cibernéticas e vulnerabilidades de segurança. A CTI é um modelo de conhecimento baseado em evidências que engloba informações relacionadas a ataques cibernéticos, seus mecanismos, indicadores, danos previstos, contramedidas, ameaças futuras, riscos e ativos expostos a esses riscos.

Amoroso (2012) complementa a definição de CTI, afirmando que ela consiste em elementos como IPs, domínios, *hashes* de arquivos, bem como outros dados seguros, incluindo Inteligência de Fontes Abertas (OSINT), inteligência de mídias sociais e inteligência humana, entre outros. Quando combinados, esses elementos de CTI podem dar suporte a um mecanismo eficaz de prevenção de invasões para infraestruturas de Tecnologia da Informação (TI) e Tecnologia Operacional (OT).

O compartilhamento eficiente de CTI é de extrema importância para a detecção e prevenção de ameaças cibernéticas, uma vez que possibilita a criação de ferramentas automatizadas com recursos defensivos sofisticados e eficazes. Essas ferramentas analisam continuamente grandes volumes de CTI heterogêneas relacionadas às Táticas, Técnicas e Procedimentos (TTPs) dos invasores, bem como Indicadores de Comprometimento (IoC) (Appala et al., 2015).

Segundo Ramsdale et al. (2020), as fontes de CTI podem ser categorizadas como “fontes internas”, “observáveis de origem externa” e “inteligência de código aberto externa”. A CTI de fontes internas compreende eventos observáveis ocorridos na rede interna e nos hosts de uma organização, fornecendo indicadores de ameaças que ultrapassaram o perímetro de segurança, violaram as regras internas de controle de acesso, infectaram sistemas ou tentaram obter acesso a sistemas restritos.

Os observáveis de origem externa referem-se às CTIs obtidas de fontes abertas e gratuitas, com formatos e linguagens voltados para interpretação por máquina. Por fim, a inteligência de código aberto externa é obtida a partir de fontes publicamente disponíveis, contribuindo para a compreensão do cenário de ameaças, mas frequentemente apresenta desestruturação e uma abordagem mais voltada para o entendimento humano do que para máquinas.

Em um estudo conduzido por Ooshthoek et al. (2021), verifica-se que atualmente, a CTI ainda está em seus estágios iniciais e carece de processos bem definidos, o que resulta em consequências para sua utilização adequada. O estudo conclui que a análise na área da CTI muitas vezes é inadequada devido a falhas em sua metodologia, resultando em um produto de CTI falho devido a um processo também defeituoso.

Por outro lado, Gong et al. (2018) propõem um novo modelo para analisar a confiabilidade e validade dos dados de CTI, empregando uma análise comparativa entre os dados de CTI e apresentando critérios para avaliar a confiabilidade das fontes que fornecem dados de CTI. De acordo com esta abordagem, o uso do modelo proposto pode resultar em níveis razoáveis de segurança ao utilizar a CTI.

3. Trabalhos Relacionados

Existem diversas abordagens para avaliar fontes de CTI, e alguns trabalhos relacionados já abordaram esse tópico. A seguir, apresenta-se uma breve visão geral desses trabalhos.

No artigo de Schlette et al. (2020), é proposto um método para avaliar a qualidade dos artefatos de CTI, o que desempenha um papel crucial na eficácia da detecção e defesa contra ataques cibernéticos. Nesse trabalho, foram identificadas dimensões e métricas relevantes de qualidade, e uma ferramenta de análise de CTI existente foi aprimorada para tornar a avaliação de qualidade mais transparente para os analistas de segurança. O método introduziu um conjunto básico de dimensões, derivadas de dimensões de qualidade de dados amplamente aceitas, destacando a falta de controle de qualidade em plataformas de compartilhamento de CTI como um desafio significativo a ser enfrentado. Em resumo, essa abordagem representa um primeiro passo essencial em direção a uma metodologia abrangente de gerenciamento de qualidade para CTI.

O artigo intitulado "A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources" (Schaberreiter et al., 2019) propõe uma metodologia baseada em parâmetros quantitativos para avaliar a qualidade das fontes de CTI. A abordagem busca facilitar o estabelecimento de confiança nas fontes de CTI por meio de uma avaliação ponderada que pode ser adaptada às necessidades e prioridades individuais de cada entidade. Embora a análise seja quantitativa, é importante observar que os parâmetros utilizados são uma adaptação das variáveis de qualidade dos dados, o que significa que, embora a abordagem seja quantitativa, ainda leva em consideração aspectos qualitativos importantes na avaliação da qualidade das fontes de CTI.

Em um estudo conduzido por Griffioen et al. (2020) para avaliar a qualidade dos *feeds* de Inteligência de Ameaças, são propostas quatro métricas (pontualidade, sensibilidade, originalidade e impacto) para avaliar a qualidade desses feeds ao longo de vários meses. Os resultados revelaram uma variação significativa no tempo de inserção de relatórios de atividades indesejadas nos feeds, variando de dias a meses após o início, o que surpreendeu os autores, dada a semelhança na sensibilidade na identificação de atividades. Além disso, o estudo destacou a falta de sobreposição de atividades nos *feeds*, levantando questões sobre se os feeds de CTI fornecem informações suficientes para combater atividades anômalas quando identificadas.

Outro fator importante que afeta a qualidade da CTI é o *feed* que a compartilha. Weissenfelt (2022) conduziu um estudo para determinar qual *feed* de CTI seria mais adequado para fins de ensino relacionados à cibersegurança. O estudo comparou a acurácia e o escopo dos eventos, bem como a facilidade de uso e implementação de diversos feeds, incluindo PhishTank, Dshield, Emerging Threats C&C, Emerging Threats - Compromised e AlienVault. Após análises detalhadas, todos os feeds mostraram-se

equilibrados quanto à qualidade da CTI gerada e à sua usabilidade. No entanto, optou-se por usar a ferramenta AlienVault devido à maior familiaridade com ela.

Em resumo, esses estudos oferecem abordagens variadas para avaliar a qualidade das fontes de CTI, considerando diferentes dimensões e métricas. Eles contribuem para o desenvolvimento de métodos mais eficazes de avaliação de CTI, essenciais para a segurança cibernética eficaz.

4. Metodologia

Trata-se de uma pesquisa aplicada, com objetivos exploratórios e descritivos. O trabalho possui características exploratórias, já que seu principal objetivo é aprimorar ideias ou descobrir intuições, o que requer um planejamento flexível capaz de considerar vários aspectos relacionados ao fato estudado (Gil, 2009, p. 41). Ele é descritivo pois "consiste em investigações de pesquisa empírica cuja principal finalidade é o delineamento ou análise das características de fatos ou fenômenos, a avaliação de programas, ou o isolamento de variáveis principais ou chave" (Marconi e Lakatos, 2003, p. 187).

O estudo adotou uma abordagem predominantemente qualitativa, já que buscou compreender e explorar "universos de significados, motivos, aspirações, crenças, valores e atitudes", ou seja, um espaço mais profundo de relações e fenômenos que não podem ser mensurados apenas pela operacionalização de variáveis (Minayo, 2002, p. 21).

Um total de 21 feeds relacionados a ataques DDoS no AlienVault foram analisados entre 6 e 12 de junho de 2023. Todos os feeds foram avaliados de acordo com seis dimensões de qualidade da informação, conforme a tabela 1.

Item	Descrição
Completude (Co)	Requer informações detalhadas sobre o ataque, como o tipo de ataque, origem, alvos, duração e outras informações relevantes
Oportunidade (Op)	Exige que o relatório seja emitido o mais rápido possível após o ataque, para que a equipe de segurança possa tomar medidas efetivas.
Credibilidade (Cr)	Pressupõe o uso de fontes confiáveis, como relatórios de organizações governamentais, grupos de pesquisa em segurança cibernética ou outras fontes reconhecidas.
Precisão (Pr)	Implica na disponibilização de informações precisas sobre o ataque, incluindo sua origem e técnicas utilizadas.
Relevância (Re)	Requer que o relatório forneça informações úteis para a organização, ajudando-a a identificar e mitigar ameaças específicas.
Capacidade de ação (Ac)	Exige que o relatório forneça orientações claras sobre as medidas de segurança a serem tomadas para mitigar o ataque.

Tabela 1 – Dimensões de qualidade da informação utilizadas

A análise dos feeds foi conduzida utilizando estatística descritiva, visando classificar a ordem dos feeds com base em um *rating* de até 6 pontos. A pontuação máxima é alcançada quando todas as 6 dimensões avaliadas na análise qualitativa estão presentes, adicionando um ponto ao *rating* para cada dimensão. Além disso, a estatística descritiva

será aplicada para explorar as relações entre o *rating* obtido e outras informações dos feeds, a fim de obter uma compreensão mais aprofundada do cenário analisado.

5. Resultados e Discussões

Os resultados da análise dos atributos de qualidade da informação, dos relatórios selecionados sobre ataques DDoS, na plataforma Alien Vault, estão apresentados na Tabela 2. A média das notas finais obtidas foi de 4,09 pontos. Verifica-se que apenas 10 relatórios obtiveram notas acima da média, e apenas 3 deles alcançaram a pontuação máxima de 6 pontos, indicando que eles possuem todos os atributos de qualidade da informação avaliados.

A nota final mais comum foi de 3 pontos, com 8 relatórios, seguida pela nota 5, com 7 relatórios. As pontuações menos frequentes foram 4 e 2 pontos, com 2 e 1 relatórios, respectivamente. Outro ponto relevante é que todos os relatórios receberam pelo menos um ponto, com nenhum deles recebendo a nota 0.

Relatório	Co	Op	Cr	Pr	Re	Ac	NF
Uncovering HinataBot: A Deep Dive into a Go-Based Threat	1	1	1	1	1	1	**6**
New Medusa Botnet Emerging Via Mirai Botnet Targeting Linux Users	1	1	1	1	1	1	**6**
Mirai Variant MooBot Targeting D-Link Devices	1	1	1	1	1	1	**6**
Prometei botnet improves modules and exhibits new capabilities in recent updates	0	1	1	1	1	1	**5**
KmsdBot: The Attack and Mine Malware	1	1	1	0	1	1	**5**
So RapperBot, What Ya Bruting For?	1	1	1	0	1	1	**5**
PYbot DDoS Malware Being Distributed Disguised as a Discord Nitro Code Generator	1	0	1	0	1	1	**4**
Typosquatting Campaign Targeting Python's Top Packages, Dropping GitHub Hosted Malware with DGA Capabilities	1	1	1	1	1	0	5
Rise in XorDdos: A deeper look at the stealthy DDoS malware targeting Linux devices	1	0	1	1	1	1	**5**
Moobot Strikes Again - Targeting Cacti And RealTek Vulnerabilities	1	1	1	1	1	0	5
Mirai Variant V3G4 Targets IoT Devices	0	0	1	1	1	1	**4**
NoName057(16) - The Pro-Russian Hacktivist Group Targeting NATO	0	1	1	1	1	0	4
ChinaZ DDoS Bot Malware Distributed to Linux SSH Servers	0	0	1	1	1	0	3
Kaiji Botnet Resurfaces, Unmasking Ares Hacking Group?	0	1	1	0	1	0	3
BB17 distribution Qakbot (Qbot) activity	1	0	1	0	1	0	3
Vulnerability Attack Threats on the Cloud	0	0	1	0	1	1	**3**
Who Broke NPM? Malicious Packages Flood Leading to Denial of Service	0	1	1	0	1	0	3

Relatório	Co	Op	Cr	Pr	Re	Ac	NF
Mirai Botnet and Gafgyt DDoS Team Up Against SOHO Routers.	1	0	1	0	1	0	3
MANGA aka Dark Mirai-based Campaign Targets New TP-Link Router RCE Vulnerability	0	1	1	0	1	0	3
Andoryu Botnet. A New Botnet Based on Socks Protocol	0	1	1	0	1	0	3
ShellBot Malware Being Distributed to Linux SSH Servers - ASEC BLOG	0	0	1	0	1	0	2

Tabela 2 – Análise dos atributos dos relatórios selecionados
Rótulos: Co – Completude; Op – Oportunidade; Cr – Credibilidade; Pr – Precisão; Re – Relevância; Ac – Capacidade de Ação; NF – Nota Final;

Na Figura 1, a distribuição dos 21 relatórios analisados mostra uma predominância notável nos atributos de credibilidade e relevância, presentes em todos os relatórios. A oportunidade é evidente em 13 relatórios, enquanto completude e precisão ocupam a terceira posição, com 11 relatórios cada. A capacidade de ação está presente em 10 relatórios.

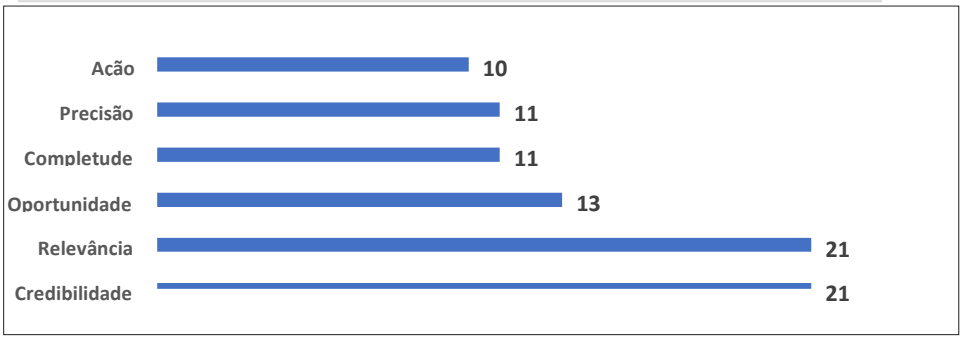

Figura 1 – Relatórios por atributo da qualidade da informação

Apesar da robusta presença em credibilidade e relevância, indicando fontes confiáveis e informações úteis, há lacunas de qualidade devido à ausência dos atributos de oportunidade, completude, precisão e capacidade de ação. O atributo de oportunidade revela a demora na disponibilidade das informações, a completude demanda mais detalhes sobre os ataques, incluindo origem e alvo, a precisão questiona a acurácia das informações sobre técnicas de ataque, e a capacidade de ação ressalta a necessidade de orientações mais claras sobre medidas de segurança para conter os ataques.

A distribuição dos relatórios coletados e analisados de acordo com as fontes digitais encontradas na plataforma Alien Vault é ilustrada na Figura 2. É possível observar que as fontes digitais que mais contribuíram com relatórios sobre ataques DDoS foram a Fortinet e a Asec, com 3 publicações cada. Em seguida, temos a Akamai, Sans e QiAnXin,

todas com 2 publicações. Essas cinco fontes digitais combinadas representam mais da metade dos relatórios selecionados. As demais bibliotecas digitais agrupadas na categoria “Outros”, apresentaram apenas 1 publicação, totalizando 9 relatórios.

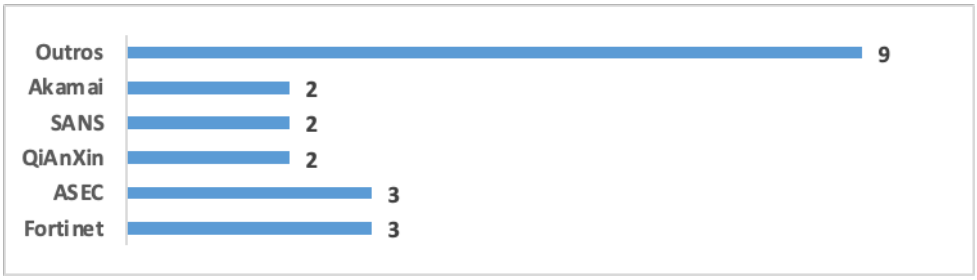

Figura 2 – Relatórios por fontes de informação

Esses resultados ressaltam a importância das fontes digitais como a Fortinet, Asec, Akamai, Sans e QiAnXin, na disseminação de conhecimento e pesquisa sobre o tema dos ataques DDoS. Essas fontes têm contribuído para a compreensão e o avanço nessa área, fornecendo informações para a comunidade de segurança cibernética.

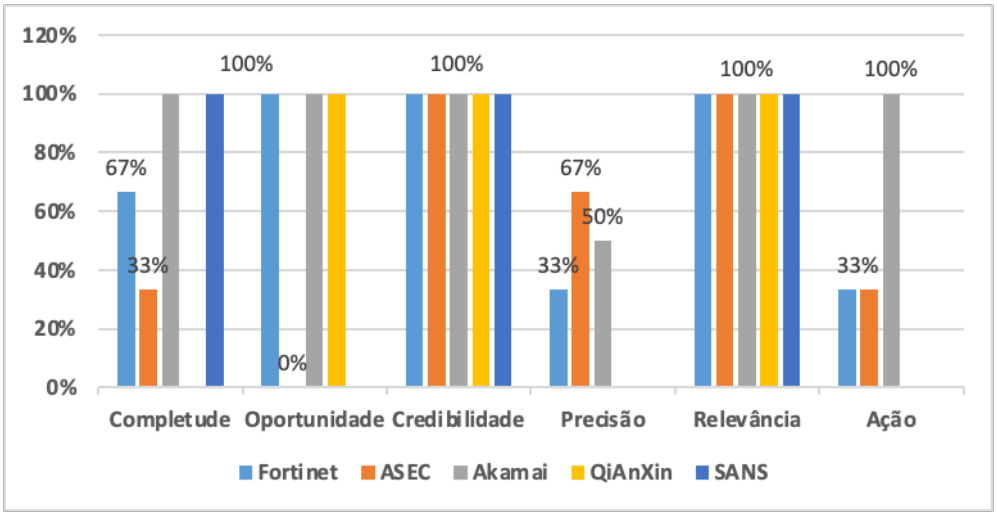

Figura 3 – Percentual dos atributos por fonte de informação

Na Figura 3, a análise cruzada das principais fontes de informação com os relatórios analisados revela a percentagem de publicações que possuem o atributo de completude. A SANS e a Akamai se destacam, tendo todos os seus relatórios com informações detalhadas sobre os ataques. A Fortinet e a ASEC possuem, respectivamente, 67% e 33%

de completude em suas publicações, enquanto a QiAnXin não alcançou a completude em nenhum de seus relatórios. Quanto ao atributo de oportunidade, que indica a rapidez na emissão dos relatórios após os ataques, a maioria das fontes atingiu 100%, com exceção da SANS, que não alcançou essa qualidade em nenhuma de suas publicações.

O atributo de credibilidade foi satisfatoriamente atendido por todos os relatórios analisados, baseando-se em fontes confiáveis. No entanto, em relação ao atributo de precisão, que aborda informações detalhadas sobre táticas e procedimentos utilizados nos ataques, apenas a Fortinet, ASEC e Akamai apresentaram relatórios com esse atributo, com taxas de 33%, 67% e 50%, respectivamente. As outras fontes não incluíram essas informações. Quanto à relevância, todos os relatórios de todas as fontes alcançaram 100%, indicando informações de alta importância para a identificação e mitigação de ameaças de DDoS. Finalmente, o atributo de capacidade de ação, que fornece orientações claras sobre a mitigação de ataques e medidas de segurança, foi melhor atendido pela fonte Akamai, com 100%, enquanto Fortinet e ASEC atingiram 33%. As demais fontes não incluíram informações sobre esse atributo, destacando a importância de relatórios abrangentes para orientações eficazes na proteção contra ataques e na implementação de medidas de segurança adequadas.

6. Conclusão

Este estudo teve como objetivo a análise dos atributos de qualidade da informação nos relatórios relacionados a ataques DDoS na plataforma Alien Vault. Foram avaliados 21 feeds específicos sobre ataques DDoS no AlienVault. A análise abordou seis dimensões de qualidade da informação, a saber: completude, oportunidade, credibilidade, precisão, relevância e capacidade de ação. Utilizou-se estatística descritiva para classificar os feeds com base em um *rating* de até 6 pontos, atribuindo um ponto para cada dimensão considerada na avaliação qualitativa. Adicionalmente, a estatística descritiva foi aplicada para investigar as relações entre o *rating* obtido e outras informações dos feeds, contribuindo para uma compreensão mais profunda do cenário analisado.

Os resultados da análise dos atributos de qualidade da informação revelam lacunas significativas, apesar da relevância e confiabilidade das fontes. Há deficiências em completude, precisão, oportunidade e capacidade de ação, variando consideravelmente entre as fontes de informação. É importante notar que nenhuma das fontes analisadas alcançou total precisão, conforme evidenciado ao avaliar separadamente a presença do atributo em questão.

No entanto, é necessário reconhecer as limitações deste estudo, uma vez que todos os atributos de qualidade foram tratados com igual ponderação na computação da nota. Para superar essa limitação, sugere-se em estudos futuros, adotar um método multicritério que permita a avaliação ponderada dos atributos. A atribuição de pesos apropriados a cada atributo de qualidade será baseada em entrevistas com profissionais especializados em Threat Intelligence, visando uma análise mais precisa e equilibrada da qualidade da informação.

Referências

Akamai (2023). “DDoS Attacks: Evolution.” https://l1nq.com/V64hT.

Amoroso, E., G. (2012). Cyber Attacks: Protecting National Infrastructure. Amsterdam, The Netherlands: Elsevier.

Appala, S.; Cam–Winget, N.; McGrew, D.A.; Verma, J.(2015). An actionable threat intelligence system using a publish–subscribe communications model. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, Denver, CO, USA, 12–16 October 2015; pp. 61–70.

Barnum, S. (2012). “Standardizing cyber threat intelligence information with the structured threat information expression (stix),” MITRE Corp., vol. 11, pp. 1– 22.

Batini, C., Cappiello, C., Francalanci, C., & Maurino, A. (2009). Methodologies for data quality assessment and improvement. ACM Computing Surveys, 41(3), 1– 52.

Brown, R., & Lee, R. M. (2019). The evolution of cyber threat intelligence (cti): 2019 sans cti survey. SANS Institute. Available online: https://www. sans. org/white-papers/38790/.

Caltagirone, S. (2019). How to Evaluate Your ICS/OT Threat Intelligence Providers: Four Key Traits to Assess Intel Quality: Completeness, Accuracy, Relevance & Timeliness. Whitepaper. Dragos, Inc.

Cisco (2022). “Colaboração e Compartilhamento de Inteligência de Ameaças.” Distrito, Mar. 2022, https://l1nq.com/UHiig.

CloudFlare, Inc. (2023). Ataques DDoS famosos | Os maiores ataques DDoS de todos os tempos. CloudFlare. https://urx1.com/2WZFq.

Eckerson, W., W (2006). Data quality and the bottom line: Achieving business success through a commitment to high quality data. https://urx1.com/tV4Yy.

Ferguson, P., & Senie, D. (2000). RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC Editor, USA.

Georg, M.A.C., Rodrigues, W.M.S., Alves, C.A.M., Junior, A.S., & Nunes, R.R. (2023). Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. https://ury1.com/6W12Z.

Gil, A. C. (2009). Como elaborar projetos de pesquisa (4a ed.). São Paulo, Atlas.

Gong, S.; Cho, J.; Lee, C. (2018). “A Reliability Comparison Method for OSINT.

Gondim, J.J.C., Albuquerque, R.O., & Orozco, A.L.S. (2020). Mirror saturation in amplified reflection Distributed Denial of Service: A case study using SNMP, SSDP, NTP, and DNS protocols. https://doi.org/10.1016/j.future.2020.01.024.

Griffioen, H., Booij, T., & Doerr, C. (2020). Quality Evaluation of Cyber Threat Intelligence Feeds. International Conference on Applied Cryptography and Network Security (ACNS).

Intelligence with Cyber Kill Chain for Adversarial Aware Security" Mathematics 10, no. 12: 2054. https://doi.org/10.3390/math10122054.

James, Kevin. (2023). What Is A Botnet?: Types Of Botnets Attacks, Examples & Prevention Measures. https://urx1.com/K6Udu.

Jin, C., et al.., (2003). Hop-count filtering: an effective defense against spoofed DDoS traffic. In Proceedings of the 10th ACM conference on Computer and communications security, 30-41.

Kaspersky. (2022). Spoofing de IP: como ele funciona e como evitá-lo. https://www.kaspersky.com.br/resource-center/threats/ip-spoofing.

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., & Zhang, J. (2009). Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. In EURASIP Journal on Wireless Communications and Networking (Vol. 2009, No. 1, p. 692654). doi:10.1155/2009/692654.

Mahjabin, T., et.al. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1550147717741463

Marconi, M. A., & Lakatos, E. M. (2003). Fundamentos de metodologia científica (5ª ed.). Atlas.

McMullin M. (2016). DNS, load balancing and DDoS attacks. https://kemptechnologies.com/blog/load-balancingand-ddos-attacks/

Minayo, M. C. D. S. (2002). Pesquisa Social: Teoria, Método e Criatividade. 21ª Edição. Petrópolis: Editora Vozes.

O'Brien, T. (2015). "Accounting" for Data Quality in Enterprise Systems. Procedia Computer Science, 64, 442-449.

Oosthoek, K.; Doerr, C. (2021). Cyber Threat Intelligence: A Product Without a Process?, International Journal of Intelligence and CounterIntelligence, 34:2, 300-315, DOI: 10.1080/08850607.2020.1780062

Radware. (2023). Radware Full Year 2022 Report: Malicious DDoS Attacks Rise 150%. Radware. https://urx1.com/n31ea.

Ramsdale, A.; Shiaeles, S.; Kolokotronis, N. 2020. "A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages" Electronics 9, no. 5: 824. https://doi.org/10.3390/electronics9050824.

Roberts, S. J., & Brown, R. (2017). Intelligence-Driven Incident Response.

Schaberreiter, T., Kupfersberger, V., Rantos, K., Spyros, A., Papanikolaou, A., Ilioudis, C., & Quirchmayr, G. (2019). A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources. Proceedings of the 14th International Conference on Availability, Reliability and Security.

Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2020). Measuring and visualizing cyber threat intelligence quality. International Journal of Information Security.

Sentinelone. (2021). Botnets: What They Are & How To Stop Them. https://www.sentinelone.com/cybersecurity-101/botnets/.

Trinks, V.d.M.D.; Albuquerque, R.d.O.; Nunes, R.R.; Mota, G.A. Strategic Assessment of Cyber Security Contenders to the Brazilian Agribusiness in the Beef Sector. https://doi.org/10.3390/info13090431.

Tivit (2023). "Cyber Threat Intelligence: o que é e como pode proteger grandes empresas?" Blog TIVIT, https://blog.tivit.com/cyber-threat-intelligence.

Validity Analysis," in IEEETransactions on Industrial Informatics, vol. 14, no. 12, pp. 5428-5435, Dec. 2018, doi: 10.1109/TII.2018.2857213.

Wang, R. Y., & Strong, D. M. (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. Journal of Management Information Systems, 12(4), 5-33.

Weiler, N. (2002). Honeypots for distributed denial-of-service attacks. In Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 109-114.

Weissenfelt, Kati (2022). Open Cyber Threat Information Feeds for Cyber Security Education. Master's Degree Programme in Information Technology. Jamk – University of Applied Sciences.

Yamin, Muhammad Mudassar, Mohib Ullah, Habib Ullah, Basel Katt, Mohammad Hijji, and Khan Muhammad. 2022. "Mapping Tools for Open Source.

Zekri, M., et al. (2017). DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd international conference of cloud computing technologies and applications (CloudTech), 1-7.