DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Metodologia para Inteligência de Ameaças Cibernéticas com Integração de Sensores

João Alberto Pincovscy

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

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Metodologia para Inteligência de Ameaças Cibernéticas com Integração de Sensores

João Alberto Pincovscy

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,
Doutor, FT/UnB
Orientador

Prof. André Ricardo Abed Grégio,
Doutor, DInf/UFPR
Examinador Externo

Prof. Fábio Lúcio Lopes de Mendonça,
Doutor, FT/UnB
Examinador interno

FICHA CATALOGRÁFICA

PINCOVSCY, JOÃO ALBERTO
Metodologia para Inteligência de Ameaças Cibernéticas com Integração de Sensores [Distrito Federal] 2022.
xvi, 50 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Inteligência de Ameaças	2. Detecção de Intrusão
3. Análise de Anomalias	4. Indicadores de Ameaças
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

PINCOVSCY, J. A. (2022). *Metodologia para Inteligência de Ameaças Cibernéticas com Integração de Sensores*. Dissertação de Mestrado Profissional, Publicação PPEE.MP.029, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 50 p.

CESSÃO DE DIREITOS

AUTOR: João Alberto Pincovscy
TÍTULO: Metodologia para Inteligência de Ameaças Cibernéticas com Integração de Sensores.
GRAU: Mestre em Engenharia Elétrica ANO: 2022

João Alberto Pincovscy
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Este trabalho é especialmente dedicado à minha esposa e aos meus filhos.

E aos meus pais *in memoriam*.

AGRADECIMENTOS

Agradeço a ABIN pela oportunidade.

Aos meus professores pelos ensinamentos, especialmente aos meus orientadores formais e informais.

Aos meus colegas de trabalho que me ajudaram ativamente na montagem e automação da prova de conceito.

Especialmente, à minha família pelo apoio e incentivo sempre presente.

E a Deus, sempre.

RESUMO

Identificar ataques em redes de computadores é uma tarefa complexa, dada a enorme quantidade de máquinas, diversidade dos dados e grande volume de dados. A Inteligência de Ameaças Cibernéticas consiste na coleta, classificação, enriquecimento, classificação dos dados e produção de conhecimento sobre ameaças nos sistemas de defesa das redes. Neste cenário encontramos os Sistemas de Detecção de Intrusão de rede que especificamente analisam o tráfego de rede e através de assinaturas detectam anomalias, gerando registros para os operadores do sistema. A proposta deste trabalho é apresentar uma metodologia para gerar conhecimento sobre Inteligência de Ameaças, a partir dos registros de sensores de rede, coletando Indicadores de Ameaças ou Comprometimento e enriquecendo-os para alimentar Plataformas de Compartilhamento de Inteligência de Ameaças. Nossa metodologia acelera o processo de tomada de decisão, pois incorpora um repositório público e atualizado de assinaturas já no coletor, eliminando a fase de identificação de ameaças em uma etapa adicional. Para a demonstração e avaliação da metodologia foi realizada uma prova de conceito que contemplou todo o ciclo da identificação de ameaças.

ABSTRACT

Identifying attacks on computer networks is a complex task, given the huge number of machines, data diversity, and a large volume of data. Cyber Threat Intelligence consists of collecting, classifying, enriching, classifying data, and producing knowledge about threats in network defense systems. In this scenario, we find network Intrusion Detection Systems that specifically analyze network traffic and detect anomalies through signatures, generating records for system operators. The purpose of this work is to present a methodology to generate knowledge about Threat Intelligence, from the records of network sensors, collecting Threat or Compromise Indicators and enriching them to feed Threat Intelligence Sharing Platforms. Our methodology accelerates the decision-making process, as it incorporates an up-to-date, public repository of signatures already in the collector, eliminating the threat identification phase in an additional step. For the demonstration and evaluation of the methodology, a proof of concept was carried out that covered the entire threat identification cycle.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

A maioria dos relatos divulgados de intrusões conhecidas envolvem aqueles que ocorrem através de redes, então se um computador está conectado a uma rede ele está mais suscetível a ser invadido (1). Principalmente nos últimos anos com o desenvolvimento da tecnologia de comunicação digital e o aumento do teletrabalho em todo o planeta (2).

A Internet se popularizou e verificamos um crescimento em larga escala da Internet das Coisas (IoT – *Internet of Things*), que nos últimos anos contribuiu a um aumento significativo da computação em nuvem, cidades inteligentes e Indústria 4.0, aumentando também a superfície de ataque e a diversidade dos mesmos (3). A IoT oferece aos atacantes sistemas inteligentes que pouco se preocupam com a segurança do dispositivo, com várias vulnerabilidades a ataques cibernéticos, forçando os pesquisadores a desenvolverem mecanismos sofisticados para proteção dos dispositivos, por exemplo, como em (4), onde é desenvolvida uma pesquisa para proteção dos sistemas domésticos inteligentes. Estes são projetados como plataformas para conectar sensores, eletrodomésticos e dispositivos para trocar dados e, em última análise, fornecer serviços úteis aos residentes domésticos, mas possuem limitações de processamento e em seus protocolos de comunicação, objeto da pesquisa. Na esfera da Inteligência de Estado Digital, a evolução tecnológica das redes possibilitou a criação das Ameaças Persistentes Avançadas (APT - *Advanced Persistent Threat*), proposta pela primeira vez pelo Departamento de Defesa dos EUA e pela Força Aérea dos EUA, com ataques avançados, furtivos, contínuos e de longo prazo em redes de alvos específicos (5).

Diante deste cenário, qualquer dispositivo que se conecte na Internet, potencialmente, pode ser vetor de invasão ou alvo, com milhares de dispositivos gerando um volume enorme de informações sobre as conectividades dos mesmos, podendo necessitar dos serviços de Inteligência de Ameaças Cibernéticas (CTI - *Cyber Threat Intelligence*) para analisar e filtrar os dados identificando possíveis ataques (6).

O principal objetivo da CTI é apoiar as organizações no entendimento dos riscos e ameaças conhecidas, APT e ameaças desconhecidas chamadas de dia zero ou *zero-day* (5) (6) (7) (8).

Cabe aqui ressaltar que a terminologia Inteligência foi cunhada muito antes da criação dos computadores e sempre coletou informações. No que lhe concerne, contém lacunas que devem ser preenchidas, pois nem sempre estas informações possuem a qualidade necessária para a produção de Inteligência (9). Com a CTI algo similar ocorre, pois as informações são também incompletas, imprecisas ou desatualizadas, sendo um desafio para os especialistas das organizações identificar com rapidez a exatidão dos ataques mais sofisticados (8). Metodologias e sistemas estão sendo continuamente aprimorados e desenvolvidos para minimizar esta aparente fragilidade da CTI, construindo redes de compartilhamento de informações, Indicador de Comprometimento (IoC - *Indicator of Compromise*) utilizando protocolos específicos como o *Structured Threat Information Expression* (STIX), desenvolvido pelo MITRE (6)(10). A adoção do STIX por organizações de serviços financeiros e vários Centros de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT´s) (11), por todo o mundo, resultou em uma complementação ao protocolo chamado *Trusted Automated Exchange of Indicator Information* (TAXII) (12), que melhor correlaciona Técnicas, Táticas e Procedimentos (TTP) em sistemas especializados para CTI (13). Atualmente

o STIX/TAXII estão na versão 2.1 (14) (15) (16).

As ferramentas de Informações de Segurança e Gerenciamento de Eventos (SIEM - *Security Information and Event Management*) são usadas dentro das empresas para realizar a correlação de eventos cibernéticos na tentativa de produzir CTI, mas são comumente produtos comerciais com custos elevados e de difícil adoção por várias organizações, impactando na disseminação das informações(13). A solução é adoção de Plataformas de Compartilhamento de Inteligência de Ameaças (TISP - *Threat Intelligence Sharing Platforms*) (17) de código aberto, adotadas pelas CERTS e agora disseminada pelas organizações para uma CTI mais eficiente, sendo a *Malware Information Sharing Platform* (MISP) a mais conhecida e utilizada (18) (19) (20) (21) (22) (23). Outra plataforma que está se destacando pela sua versatilidade é a *Open Cyber Threat Intelligence* (OpenCTI) (24) (25) (26) (27) (28) que oferece inclusive interoperabilidade com a plataforma MISP (29).

Os sistemas de Inteligência carecem de mecanismos para coleta e classificação preliminar da informação (9), em CTI são utilizados sensores que comumente fazem parte dos sistemas de *firewall* das redes (30). Estes sistemas de *firewall* podem ser compostos por roteadores de borda com Listas de Controle de Acesso (ACL - *access-control list*), por computadores que processam pacotes e os reencaminham conforme as políticas de segurança da organização, por computadores que coletam pacotes para análises de intrusão, dentre outros vários dispositivos que podem ser combinados em várias arquiteturas (31). A questão mais importante sobre as arquiteturas de *firewall* é que são locais nas redes que propiciam a instalação de sensores para coleta por serem naturalmente pontos obrigatórios de concentração e passagem de tráfego (32).

Como veremos a seguir, apesar dos avanços recentes na coleta, análise e armazenamento de indicadores de incidentes empregados em CTI (3) (33) (34), as soluções adotadas como suporte para coleta não são otimizadas para identificação e correlação com Indicadores de Ameaças. Os Indicadores de Ameaças podem ser Indicadores de Comprometimento (IoC - *Indicator of Compromise*) ou Indicadores de Ataque (IoA - *Indicator of Attack*), ou ambos (35). Além disso, os IoCs necessitam de informações adicionais para serem mais facilmente avaliados em TISP.

Esta monografia propõe a integração de Sistemas de Detecção de Intrusão (IDS - *Intrusion Detection System*) ou Sistemas de Prevenção de Intrusão (IPS - *Intrusion Prevention System*) (36) para coleta de registros utilizando assinaturas e *Honeypots* (37) para geração de evidências através do acompanhamento das ameaças, diante do comportamento de aplicações. Assim, produzindo registros de possíveis ataques e comprometimentos, para em seguida proceder com o enriquecimento dos dados dos registros através da coleta de informações complementares relevantes. E finalmente carregá-los em Plataformas de Compartilhamento de Inteligência de Ameaça (TISP). A principal contribuição é propor uma Metodologia para gerar conhecimento sobre Inteligência de Ameaças, a partir dos registros de sensores de rede, com a demostração de sua viabilidade, com a execução de uma prova de conceito. Após a execução da prova de conceito constatamos a aplicabilidade imediata dos conhecimentos aqui descritos em quaisquer infraestruturas de rede TCP/IP que se conecte à Internet.

Desta contribuição foram gerados dois artigos científicos aceitos, que estão em fase de apresentação e publicação, no *IV Congress Of Computer Science, Electronics, and Industrial (CSEI 2022)* e na *9ª Conferência Ibero-Americana Computação Aplicada (CIACA 2022)*. Este último ganhou o prêmio de melhor

artigo da Conferência.

Esta dissertação está organizada em Capítulos. No Capítulo 2 são apresentadas definições e trabalhos correlatos, seguida do Capítulo 3 que apresenta a metodologia proposta. No Capítulo 4 é apresentada a prova de conceito com os resultados e sua discussão. As conclusões fecham o Capítulo 5.

2 DEFINIÇÕES E TRABALHOS CORRELATOS

Desde a antiguidade o ser humano constrói cientificamente os experimentos considerando a coleta de dados, seu processamento, análise e armazenamento. Em termos científicos, o nível de abstração apresentado é a Leitura produzindo a Mensuração, a Conversão produz Dados, a Análise produz Informação, a Experiência produz Conhecimento e o Julgamento produz Sabedoria (38). Então, detalhando os níveis de abstração temos:

- "Mensuração"é definida como a Leitura de fenômenos coletada por instrumentos ou observações;
- “Dado” são os símbolos, números, cláusulas textuais e outras descrições, obtidas após a Conversão da Mensuração;
- “Informação” é construída a partir da organização dos dados e por meio de Análises dos Dados, resultando em equações matemáticas, textos, gráficos e/ou imagens;
- “Conhecimento” é gerado pela execução da Experiência aplicada à Mensuração, Dados e Informações; e
- “Sabedoria” é o resultado da aplicação do Julgamento sobre as demais abstrações.

Assim é montada a pirâmide Sabedoria, Conhecimento, Informação, Dado e Mensuração (WKIDM), Figura 2.1:

Figura 2.1: Pirâmide WKIDM discreta (38).

No escopo deste trabalho estaremos trabalhando com dados estruturados e informações quantitativas (38). Todas as fontes de dados já oferecem a Mensuração, os Dados e algumas Informações. É objetivo da

Metodologia Proposta a geração de Conhecimento através da Inteligência de Ameaças, conforme veremos a seguir.

2.1 PROCESSO DE GERAÇÃO DE INTELIGÊNCIA DE AMEAÇAS

Em se tratando de Inteligência, o modelo militar apresenta um sistema de alerta antecipado de inteligência complexo e composto por vários módulos. O módulo de coleta, módulo de processamento, módulo de análise e módulo de desenvolvimento de ações preventivas (39), conforme Figura 2.2.

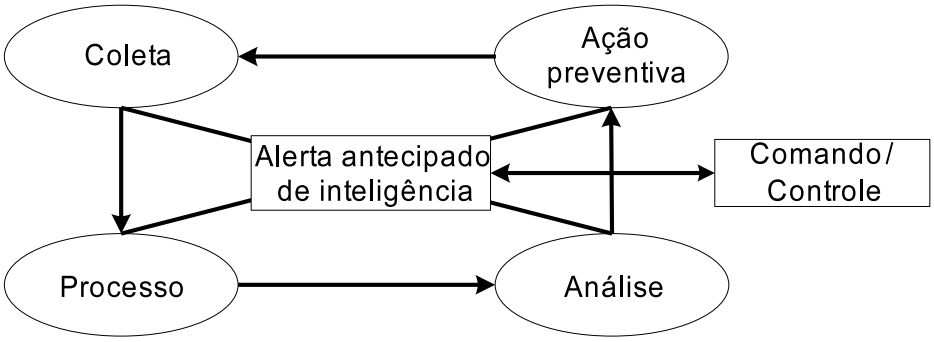


Figura 2.2: Estrutura de alerta antecipado de inteligência militar (39).

Detalhando a Figura 2.2, temos:

- A "**Coleta**"sendo realizada no meio militar através da vigilância e monitoração de indicadores específicos de inteligência determinados pelos comandantes;
- O "**Processamento**" é importante, pois ocorrem conflitos entre as informações obtidas por vários canais, necessária a sua organização, classificação e armazenamento;
- A "**Análise**"é responsável por modificar as informações rastreadas e armazenadas, por métodos como análises Bayesianas, regressão, correlação, análise de séries, análise de cenários, dentre outros métodos;
- As "**Ações Preventivas**" são resultantes do monitoramento e da inteligência preditiva situacional, com atitudes tomadas para minimizar as crises, tais como planos de contingência e recuperação de desastres;
- Os "**Alertas antecipados de inteligência**"podem ser produzidos em qualquer etapa do fluxo, sob ação do "Comando e Controle", no caso militar, do Comandante.

Esta abordagem também pode ser adaptada ao contexto de Inteligência de Ameaças Cibernéticas (CTI), descrita como a coleta, agregação, transformação, análise, interpretação, enriquecimento de informações e implantação sobre ameaças para fornecer o contexto necessário que pode auxiliar na tomada de decisões (40), conforme mostrado na Figura 2.3. Sendo que enriquecimento é o processo de agregação de informações ou dados adicionais externos (41) à rede da organização. Assim, o enriquecimento tem a finalidade de trazer maior qualidade ao módulo de análise. Assim teríamos o seguinte fluxo adaptado:

- **Agregação** - sendo realizada uma coleta de dados de vários sensores de segurança da rede determinados pela política de segurança da organização e pela característica dos sistemas e serviços presentes na rede;
- **Enriquecimento de Informação** - feita para a agregação organizada dos registros recebidos das diversas fontes evitando repetição de informações, com a devida classificação e armazenamento;
- **Análise** - é responsável por agregar dados adicionais modificando as informações originais, por buscas de bases de informações complementares fora da organização;
- **Transformação** - são as regras resultantes da análise, mitigando as ameaças identificadas;
- **Interpretação** - realizada pelos analistas de segurança que a qualquer ponto do fluxo podem antecipar ações e realizar a "Implantação"como controle da rede, baseados nas Políticas e características da organização.

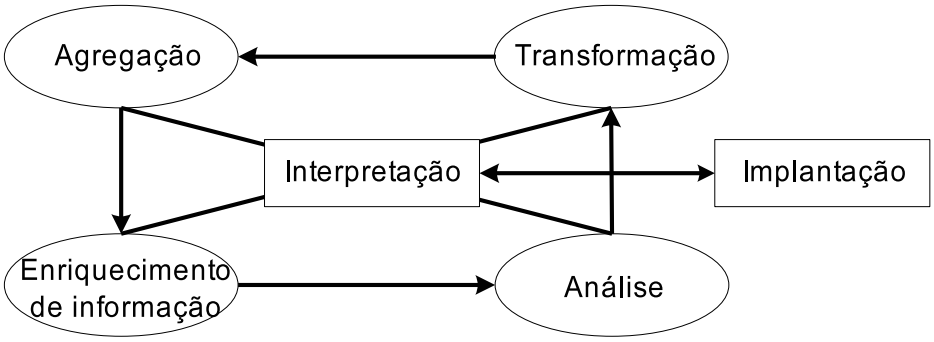


Figura 2.3: Estrutura de alerta antecipado de inteligência militar, adaptada ao contexto de CTI pelo autor desta monografia.

Cabe ressaltar que Uma Ameaça Cibernética é “qualquer circunstância ou evento com potencial para impactar adversamente as operações organizacionais” (42), caracterizando nas bases de registro como Informações sobre estas ameaças.

Informação de ameaça é qualquer informação que ajude a organização a se proteger de uma ameaça ou detectar as atividades de um atacante. Times de segurança necessitam de um alto grau de maturidade para conseguirem interpretar dados técnicos de coletas, organizá-los em informações e correlacionar estas informações produzindo CTI (43). As Informações produzidas de Dados coletados podem ser classificadas conforme os seguintes tipos (40):

- **Indicadores** - são registros que sugerem que um ataque em andamento ou indícios de um comprometimento já ocorrido.
- **Táticas, técnicas e procedimentos (TTPs)** - descrevem o comportamento de um atacante. As técnicas são descrições deste comportamento no contexto de uma tática e os procedimentos são descrições detalhadas de uma técnica.
- **Alertas de segurança** - são notificações técnicas curtas sobre vulnerabilidades, explorações e outros problemas de segurança.

- **Relatórios de inteligência de ameaças** - são documentos que descrevem TTPs, tipos de sistemas e outras informações relacionadas a ameaças que fornecem maior consciência situacional a uma organização. Tudo produzido através do processamento, enriquecimento e análise, a partir dos dados e informações coletados.

Diante destas definições, outra interpretação muito interessante foi abordada no trabalho (29), onde o processo de geração de inteligência foi descrito como mostrado na Figura 2.3:

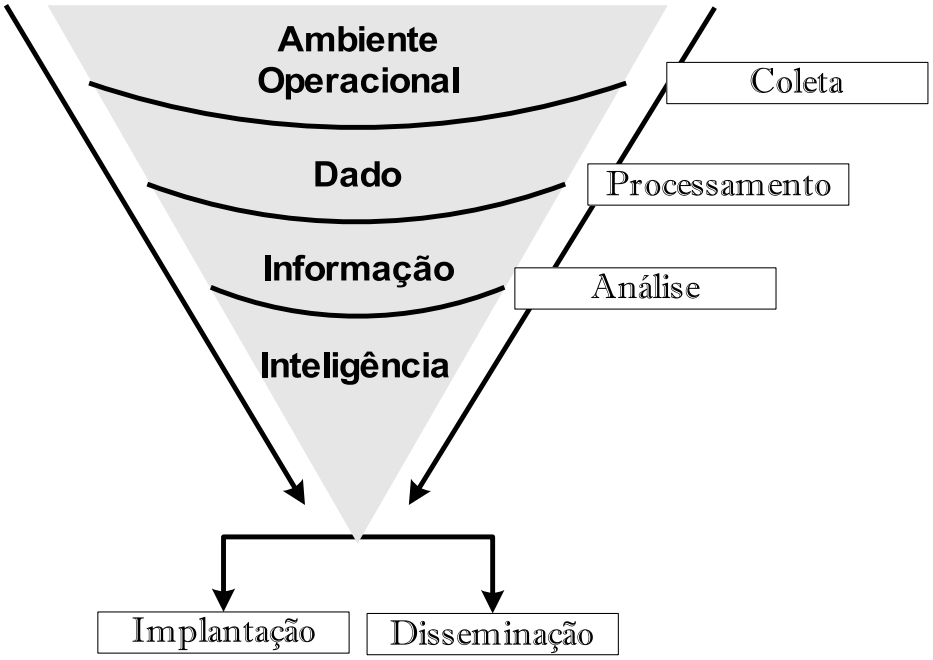


Figura 2.4: Fluxo do Processo de Produção de Inteligência de Ameaças, adaptado de (29).

Esta interpretação leva à junção dos conceitos já descritos nas Figuras 2.1, 2.2 e 2.3. Nesta interpretação, o processo de geração de inteligência de ameaças pode ser assim detalhado:

- **Coleta**: essa etapa se refere a extração, junto ao Ambiente Operacional, de dados em formatos padronizados.
- **Processamento**: trabalha na filtragem, aglutinação e formatação única dos dados, para melhor visualização das evidências com a finalidade de para gerar informações.
- **Análise**: avalia todos os dados e informações, para propiciar a descoberta de padrões em cenários específicos e na produção de inteligência.
- **Implantação**: após a produção da inteligência, ou a descoberta de padrões, é possível implantar a contramedida para garantir a mitigação de ameaças de forma proativa. Esta implantação deve ser conduzida por tomada de decisão sob controle e comando de analistas, pois é necessária a avaliação da nova regra aplicada.
- **Disseminação**: compartilhamento do conhecimento com partes interessadas.

2.2 MODELO DE DADOS

Na pesquisa em busca do modelo de dados mais adequado, encontramos um importante estudo que se encaixa perfeitamente em nossa metodologia, chamado de método 5W3H (*What, Who, Why, When, Where, How, How much* e *How long*) (29). Este método subsidia a tomada de decisão em relação à escolha dos dados a serem enriquecidos. Ele responde às questões apresentadas da Tabela 2.1.

Tabela 2.1: Descrição do método 5W3H (29).

Pergunta	**Descrição**
What	Descreve diretamente o tópico que está sendo abordado
Where	Especifica referências geográficas sobre o tópico
When	Especifica prazos relevantes para o tópico, como data e hora
Who	Associa o tópico a uma entidade capaz de executá-lo
Why	Descreve as possíveis motivações para a ocorrência do tópico
How	Descreve as principais características e mecanismos do tópico
How much	Refere-se aos custos e impactos gerados pelo tema
How long	Descrição da eficácia do tópico no que se refere ao tempo

O método é originalmente conhecido como 5W2H (*what, who, why, When, where, how, how much*). Ele é aplicado em diferentes áreas com o objetivo avaliar um determinado elemento (44). O método 5W3H é uma extensão do 5W2H e se mostrou interessante porque além de tratar do registro em todas as suas dimensões também trata da persistência, *How long*. Assim, este método possibilita a caracterização completa de uma ameaça.

Na adequação a este trabalho, "*What*" é usado para definir elemento em análise. Em CTI pode ser traduzido como a classificação da ameaça. Pode-se criar diversos parâmetros de classificação, desde tipos de ameaças até grupos de assinaturas utilizadas na coleta. Em seguida temos o "*Where*" que pode caracterizar a origem. O "*When*" fornece o momento do registro caracterizado pela data e hora do evento. "*How*" fornece o método ou as TTPs utilizadas pela ameaça. Em toda evidência de ameaça ou incidente é essencial a atribuição da ação a um autor, caracterizado pelo "*Who*". Para uma atribuição mais assertiva é importante buscar definir o "*Why*", contextualizado o cenário através das motivações do evento. Outra questão a ser respondida é a intensidade do evento respondida pelo "*How much*". E por fim a durabilidade do evento respondida pelo "*How long*". Este questionamento do método é especialmente importante para CTI quando se trata busca identificar de ameaças do tipo APT.

2.2.1 Qualificação dos dados e tipos de registros

Para produção da inteligência com qualidade necessitamos buscar os dados conforme o cenário apresentado (8) (9). Diante deste desafio buscamos no processo de produção de CTI a coleta de dados relevantes. Assim, necessitamos qualificar e identificar adequadamente os dados coletados, pois estes revelam informações diferentes quando confrontados com cenários diferentes (45). Estes cenários são determinados pelo Modelo 5W3H (29). Primeiramente temos que diferenciar registro e dado. Um registro é composto por vários dados como podemos observar na Tabela 2.2, construída pelo autor desta monografia com base no método 5W3H.

Tabela 2.2: Tipos de registro.

Registros	What	Who	Why	When	Where	How	How much	How long	Tipo
{"timestamp":"2022-04-01T14:49:36.000929-0300", "flow_id":977849080155645, "event_type":"flow", "src_ip":"168.197.141.175", "src_port":61342, "dest_ip":"164.163.0.226", "dest_port":53, "proto":"UDP", "app_proto":"dns", "flow":{"pkts_toserver":1, "pkts_toclient":0, "bytes_toserver":69, "bytes_toclient":0, "start":"2022-04-01T14:49:05.921085-0300", "end":"2022-04-01T14:49:05.921085-0300", "age":0, "state":"new", "reason":"timeout", "alerted":false}}	"proto":"UDP", "flow":{"pkts_toserver":1, "bytes_toserver":69, "state":"new",	"src_ip":"168.197.141.175",	"app_proto":"dns", "dest_port":53, "proto":"UDP", "state":"new",	{"timestamp":"2022-04-01T14:49:36.000929-0300",	"dest_ip":"164.163.0.226",	"state":"new", "reason":"timeout",	"age":0,	"start":"2022-04-01T14:49:05.921085-0300", "end":"2022-04-01T14:49:05.921085-0300",	Formato JavaScript Object Notation (JSON)
04/01/2022-14:55:03.032688 [Drop] [**] [1:2024792:4] ET POLICY Cryptocurrency Miner Checkin [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 51.81.195.38:40226 -> 164.163.0.226:80	[Classification: Potential Corporate Privacy Violation]	51.81.195.38	ET POLICY Cryptocurrency Miner Checkin	04/01/2022-14:55:03.032688	164.163.0.226	----	----	----	Formato específico de uma aplicação

Na Tabela 2.2 apresentamos o registro no formato JSON (46), este formato é padronizado para troca de dados. Observamos que nos dois tipos de registros existem uma coleção de dados e cada tipo de registro tem uma formatação própria. Um ponto em comum entre estes dois registros é a informação de data e hora do evento. Este dado é importante para determinar a dimensão "*When*" no modelo 5W3H. Outros dados importante é o endereço de Internet Protocol (IP) de origem e destino do evento, bem como a porta associada a estes endereços, respondendo às dimensões "*What*", "*Who*", "*Why*" e "*Where*". Neste ponto cabe ressaltar ser comum o mapeamento e análise das táticas, técnicas e procedimentos (TTP) utilizados pelos atores de ameaças (40) (47). Assim, após a análise de um conjunto de registros, temos a percepção se o evento ainda está ocorrendo ou já cessou e equacionando a dimensão "*How long*". Os eventos são comumente chamados de indicadores, quando contextualizados, qualificados e classificados (48).

2.3 DIFERENÇA ENTRE ATAQUES E AMEAÇAS EM INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS

Esta análise é extremamente importante para moldarmos o conceito de ataque, pois no momento que os eventos estão ocorrendo temos a configuração de um possível ataque. Caso os eventos tenham sido cessados, podemos ter um possível comprometimento. É importante ressaltar que a única diferença entre

ataque e comprometimento é se os indicadores já foram coletados no passado ou estão sendo coletados no presente, em tempo real (34). Então definimos Indicador de Comprometimento (IoC) (13) (49) e Indicador de Ataque (IoA), conforme ilustrado na Figura 2.5.

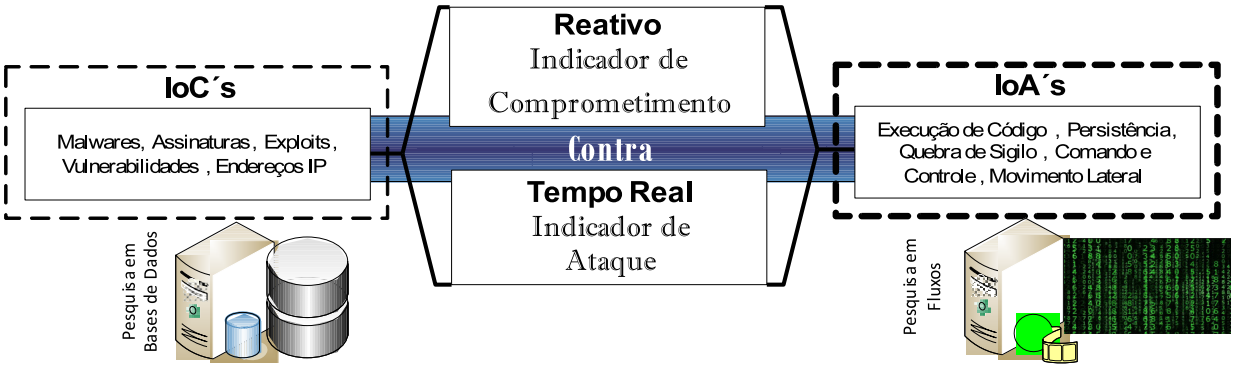


Figura 2.5: Elementos para diferenciação entre IoC em comparação a IoA, adaptado de (35).

Vale ressaltar que no processo de geração de CTI, não interessa saber se estamos tratando de IoC ou IoA. Essa diferenciação apenas se torna importante no momento da tomada de decisão da ação que será tomada ao final da geração de Inteligência. Se a decisão for intervir no sistema de defesa imediatamente ou é indicado o armazenamento da informação.

Neste artigo tratamos de uma metodologia para geração de CTI, portanto utilizaremos os dois indicadores indistintamente. Assim chegamos ao conceito de Indicadores de Ameaça, sendo a interseção entre IoC e IoA, como mostrado na Figura 2.6 construída pelo autor desta monografia.

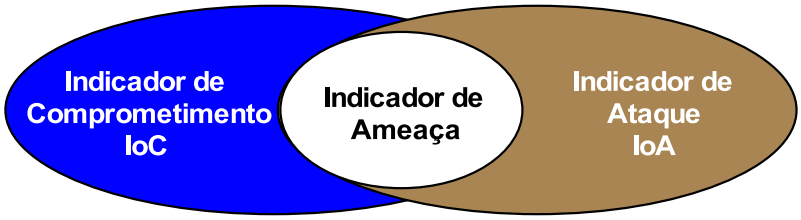


Figura 2.6: Indicador de Ameaça.

2.4 FERRAMENTAS DE GERENCIAMENTO E DISSEMINAÇÃO DE CTI

A *Malware Information Sharing Platform* (MISP) (18) é desenvolvida pela comunidade e mantida pela União Europeia (através do *Connecting Europe Facility*) (50) e pelo *Computer Incident Response Centre Luxembourg* (51), fornecendo um banco de dados central de IoC onde informações técnicas, TTP, códigos fonte, *hashs*, dentre outras informações sobre *malwares* (52) e ataques são armazenadas em formato estruturado (13). Além disso, permite a integração com outros sistemas, como sensores de coletas de dados, entrada de textos simples e saídas no formato *Extensible Markup Language* (XML) (53). A MISP também oferece a facilidade de compartilhamento seletivo e automático de informações a grupos de confiança interconectados diretamente via Internet (18).

A *Open Cyber Threat Intelligence* (OpenCTI) é uma plataforma de código aberto que busca agregar, informações gerais e técnicas do ligadas a CTI. Esta plataforma auxilia no gerenciamento de registros sobre ameaças, possibilitando a indexação, o armazenamento, a organização e a apresentação gráfica destes registros. O modelo utilizado pela plataforma é o STIX2 (54). O OpenCTI foi desenvolvido pela Luatix (55), uma organização sem fins lucrativos em parceria com a Agência Nacional de Segurança de Sistemas de Informação (ANSSI) do governo francês e o *Computer Emergency Response Team for European Institutions* (CERT-EU) (56).

2.5 CRITÉRIOS PARA ENRIQUECIMENTO DOS DADOS

Para definir os critérios para enriquecimento dos dados foram considerados a usabilidade e a relevância da informação agregada. Lembrando que enriquecimento é o processo de agregação de informações ou dados adicionais externos (41) à rede da organização. A escolha dos dados a serem enriquecidos é estratégico para subsidiar tomadas de decisão em tempo-real, utilização em regras e políticas de defesa da rede, ou robustecer investigações posteriores. Assim foi criado um modelo de dados, priorizando o Endereço IP de origem do fluxo, o Domínio de DNS (*Domain Name System*) ou o endereço de *e-mail*, nesta ordem.

2.5.1 Enriquecimento Automatizado

Em se tratando de Indicadores de Ameaças existem dados básicos a serem avaliados como endereços IP, nomes de domínio, servidores de domínio, elementos comportamentais de malware (57), cabeçalhos de *e-mail*, dentre outros. Os indicadores contêm um ou mais elementos que contextualizam a ameaça. O contexto pode incluir carimbos de hora "*When*", por quanto tempo ficaram ativos "*How long*", indicação de gravidade do incidente, bem como informações sobre o mecanismo e a dinâmica de um ataque (por exemplo, processo de infecção, disseminação e atuação de um malware). Mas para agregar inteligência ao evento, necessitamos agregar informações sobre as Táticas, Técnicas e Procedimentos (TTPs) (26) para assim possibilitar a identificação dos atores de ameaças "*Who*" e possíveis campanhas em andamento (17) (58). Para que estas informações sejam produzidas é necessário o processo de enriquecimento dos dados antes que os analistas avaliem os Indicadores de Ameaças, e deve ser feito de forma o mais automatizada possível.

Quando tratamos do tema Ameaças Cibernéticas, a automação é essencial devido à evolução no número e na sofisticação de ameaças, a diversidade dos serviços a proteger e a falta de recursos especializados na área de segurança cibernética. Podemos elencar como as necessidades básicas em segurança cibernética no que se refere à automação (58) (41):

- Detecção de Indicadores de Ameaça,
- Enriquecimento das informações sobre ameaças,
- Detecção e prevenção de incidentes de segurança,
- Triagem no tratamento de incidentes em se tratando da sua gravidade, e

- Controle de compartilhamento de informações (5W3H).

O enriquecimento dos dados pode se utilizado como apoio a *frameworks* sofisticados de detecção de *malwares* que utilizam Aprendizado de Máquina (ML - Machine Learning) para geração de assinaturas (59). Há situações onde após a atuação do processo de ML, a informação ainda não é suficiente para a elaboração de assinaturas. Então, através do processo de enriquecimento, dados externos são agregados para subsidiar o processo de análise para criação das assinaturas.

Várias fontes de dados podem ser utilizadas para o enriquecimento de Indicadores de Ameaças, tais como redes sociais (60), registros de Sistema de Nomes de Domínio (DNS), identificação de prefixos de roteamento que identificam um sistema autônomo (AS - *Autonomous System*), *hashs* em repositórios de análise de *malwares*, dentre outras.

2.6 REDES DE COMPUTADORES E SEGURANÇA DA INFORMAÇÃO

A diversidade de tipos de redes e protocolos existentes na Internet fica evidenciada quando observamos a Internet das Coisas ou *Internet of Things* (IoT). A IoT é formada, na maioria das vezes, por tecnologias tais como redes de sensores sem fio (RSSF), comunicação móvel, identificação por radiofrequência ou *Radio Frenquency Identification* (RFID) e vários outros protocolos. A força das redes IoT está na interconexão dinâmica de bilhões de equipamentos em um ecossistema através de sensores inteligentes, atuadores e outros componentes. Estima-se que o mercado IoT é de aproximadamente 200 bilhões, dados de 2020 (61).

Outra vertente são as redes dos chamados Sistemas de Controle Industrial ou *Industrial Control Systems* (ICS) e as redes de Controle de Supervisão e Aquisição de Dados ou *Supervisory Control and Data Acquisition* (SCADA). Os sistemas SCADA modernos são essenciais para operar as estruturas de geração, distribuição e transmissão de energia elétrica. Atualmente, utilizando a metodologia da tecnologia IoT, esses sistemas foram integrados e funcionam como sistemas inteligentes e computação em nuvem. Sendo cada vez mais integrados á Internet para facilitar e integrar os controles. Entretanto, esta alta conectividade e integração resultam em novas vulnerabilidades e ameaças (62).

Como podemos observar, desde redes que controlam sistemas de transmissão de energia, passando por redes de controles industriais até às modernas redes IoT, estão se conectando com a Internet. Devido a essa conectividade em massa, a modernização de redes legadas levam ao compartilhamento de tecnologias de comunicação. Em alguns casos, a análise de uma infraestrutura já em operação leva a uma completa reorganização da topologia e redefinição dos parâmetros de segurança, possibilitando uma evolução contínua dos sistemas distribuídos em rede (63). Com o aprimoramento destas tecnologias de comunicação, ampliando a conectividade e a multiplicidade de plataformas de conexão, tornou a segurança de infraestrutura um elemento crucial no funcionamento ágil e correto dos sistemas. Um dos requisitos fundamentais para obter a ciência de situação em uma infraestrutura é o monitoramento contínuo dos eventos de segurança para detecção de incidentes. A detecção pode ser com base em conhecimento (assinaturas) ou por anomalias, sendo as abordagens totalmente complementares. Como vimos anteriormente, a detecção de anomalias faz parte de um sistema integrado de segurança denominado classicamente como sistema de *firewall* (64) (65).

Essencialmente, existem seis métodos básicos utilizados para invasão de uma rede: enumeração, descoberta de vulnerabilidade, inserção de vírus ou Trojans, infecções de *e-mail*, ataques de roteador e quebra de senha (66)(67). A enumeração ou varredura da rede para descobrir os protocolos existentes e vulnerabilidades associadas ao sistema. Se existir vulnerabilidade conhecida, esta pode ser explorada por vírus ou Trojans.

O planejamento de um ataque, após a obtenção das informações, segue os seguintes passos: Monitoração a rede; Penetração no sistema; Inserção códigos maliciosos ou informações falsas no sistema; Envio de uma enxurrada de pacotes, causando negação de serviço ou *Deny of Service* (DoS) (32) (68). Este último pode forçar o roteador ou um sistema que suporta um serviço a reiniciar ou entrar em situação inesperada, possibilitando uma invasão. Todas as invasões baseadas em rede possuem a característica de carregar em seus pacotes do protocolo internet os elementos do ataque, por exemplo, a utilização de redes IoT sendo exploradas por protocolos específicos em ataques de DoS (69) (70). As consequências de um ataque bem-sucedido a uma organização podem ser variadas: Monitoramento não autorizado; Descoberta e "vazamento" de informações confidenciais; Modificação não autorizada de servidores e da base de dados da organização, dentre outras (32). Os sistemas de proteção das organizações estão cada vez mais eficientes, mas sempre é necessário que adicionemos mais camadas para complementar a infraestrutura de segurança (33)(71).

Os *firewalls* são utilizados tradicionalmente para proteger as redes, mas estão configurados para permitir acesso a serviços públicos. Adicionalmente, nem todas as redes e protocolos podem ser protegidos por simples equipamentos comercialmente denominados *firewalls* (67) (72). Então, podemos concluir que o *firewall* é um ponto entre duas ou mais redes, formado por um conjunto de elementos de segurança ou um único elemento, por onde passa o tráfego, permitindo que o controle, a autenticação, a coleta e os registros do tráfego (32). Assim, os equipamentos de encaminhamento de tráfego, como o roteador, o autenticador de usuários, o coletor de registros dos sistemas de segurança, e qualquer analisador de rede, compõem o sistema de *firewall*. Comercialmente utilizam a denominação *firewall* para um único equipamento que pode executar estas funcionalidades, mas por definição essas funcionalidades podem ser exercidas por vários equipamentos e sistemas distintos (73).

2.6.1 Sistemas de Detecção de Intrusão ou Sistemas de Detecção de Ameaças

Para proteger as redes de computadores dos ataques de redes, descritos anteriormente, foram criados os sistemas de detecção de intrusão ou *Intrusion Detection Systems* (IDS) e os sistemas de prevenção de intrusão ou *Intrusion Prevention System* (IPS). Outro termo utilizado é Sistemas de Detecção de Ameaças ou *Threat Detection System* (TDS) (74), este possui uma abrangência maior, pois congrega todos os tipos de sistemas que podem detectar ameaças, inclusive *firewalls* comerciais modernos chamados de *Next Generation Firewalls* (NGFW) (75) e os de aplicação, também chamados de *Web Application Firewall* (WAF) (76). Lembrando que o IDS/IPS faz parte do sistema de *firewall* (31) (77).

O IDS é o mais indicado para a tarefa de coleta e classificação preliminar da informação, dentre os vários elementos que compõem o sistema de *firewall* (1). O IDS foi idealizado para apoiar os computadores que executavam o roteamento e o processamento dos pacotes conforme as políticas de segurança da organização, porque com a limitação de processamento das máquinas e a necessidade de decisões rápidas em

fluxos de rede, a análise do conteúdo dos pacotes era extremamente difícil de ser realizada em tempo real (1) (67). Então a coleta era realizada para que em uma análise posterior fosse realizada com identificação de possíveis de ameaças, metodologia utilizada até os dias atuais (2).

Um IDS "tem como objetivo detectar atividades suspeitas, impróprias, incorretas ou anômalas" (32). Ele coleta, organiza os dados e em seguida aplica um mecanismo de detecção, gerando apenas um alerta. Diferentemente, o IPS pode bloquear um ataque ao detectá-lo, mas o mecanismo de funcionamento básico é o mesmo (78). Os IDSs ainda são classificados como *Network* IDS (NIDS) e o *Host* IDS (HIDS). O HIDS é instalado nas máquinas e funciona como um agente de detecção local. O NIDS é instalado na rede e trabalha na coleta, organização e detecção de intrusão (79) (80). Assim, vamos nos referir aos NIDSs sendo eles IPS ou IDS de forma simplificada apenas como IDS, conforme ilustrado na Figura 2.7.

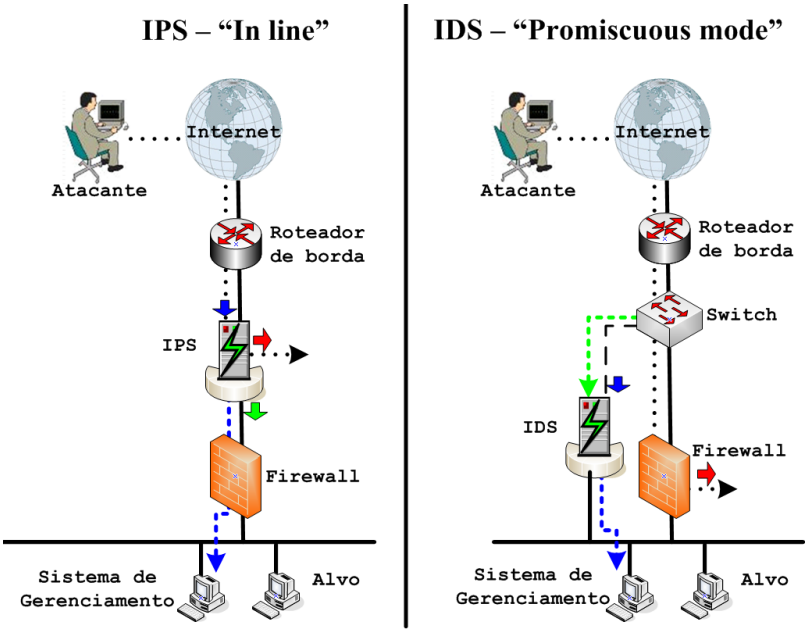


Figura 2.7: Topologia de emprego do IPS em comparação a IDS, adaptado de (81).

Os IDSs podem empregar diversos métodos de detecção (82):

- Algoritmos baseados em regras, que usam conhecimento prévio de ataques;
- Algoritmos baseados em estatísticas, que detectam anomalias construindo uma distribuição estatística de padrões de intrusão;
- Soluções baseadas em aprendizado de máquina ou *Machine Learn* (ML), que utiliza algoritmos de aprendizado para treinar classificadores que podem identificar os ataques.

O método mais simples e rápido de implementação de um IDS é baseado em regras, mas este se torna inútil para ataques ainda não conhecidos. O método estatístico e soluções baseadas em ML podem resolver este problema, mas exigem a coleta de grandes volumes de dados na coleta e um alto custo computacional para manipular esta massa de dados. Outra dificuldade é a análise de uma grande variedade de fontes de tráfego com diferentes formatos e graus de estruturação. Em um tráfego de rede temos pacotes de protocolos, fluxos de rede, mensagens, dentre outras informações. Os sistemas de IDS *open source* mais conhecidos, bem documentados e mais utilizados são Snort, Zeek (Bro) e Suricata (83).

2.6.2 *Honeynets* e *Honeypots*

Honeynets são com ambientes computacionais especialmente projetados onde sistemas e serviços são disponibilizados na Internet com as devidas monitorações e registros, mas sem nenhum bloqueio às ações de agentes maliciosos. Estes ambientes são uma ferramenta de pesquisa e acompanhamento das Técnicas, Táticas e Procedimentos (TTP) de intrusos cibernéticos. Os serviços disponibilizados dentro da *Honeynet* são chamados de *honeypots* (84).

Na arquitetura de *Honeynet* é geralmente composta por vários elementos de segurança de rede tais como *firewall* e IDS. O *firewall* fica responsável por bloquear atividades maliciosas a partir dos *honeypots*, protegendo a Internet dos sistemas comprometidos. Já o IDS tem a função de captura dos dados gerados pela atividade de rede nos *honeypots*.

Uma interessante arquitetura encontrada durante as pesquisas é o *HoneySELK* (85), conforme Figura 2.8. Nesta arquitetura proposta toda a infraestrutura da *honeynet* é montada em ambiente virtual. A solução ainda propõe um ambiente de visualização gráfica dos ataques que facilita a análise e identificação de ataques. Os gráficos da solução *HoneySELK* oferecem várias informações, tais como quantidade de conexões por intervalo de tempo, visualização geográfica em mapas das origens dos ataques, distribuição de ataques por países, IPs e serviços. O ambiente ainda possibilita a visualização detalhada de pacotes capturados pelo IDS no mesmo ambiente gráfico, a análise detalhada do *script* de *malware* coletado, oferece a função de construção de grafo com relacionamento dos ataques entre IPs e serviços.

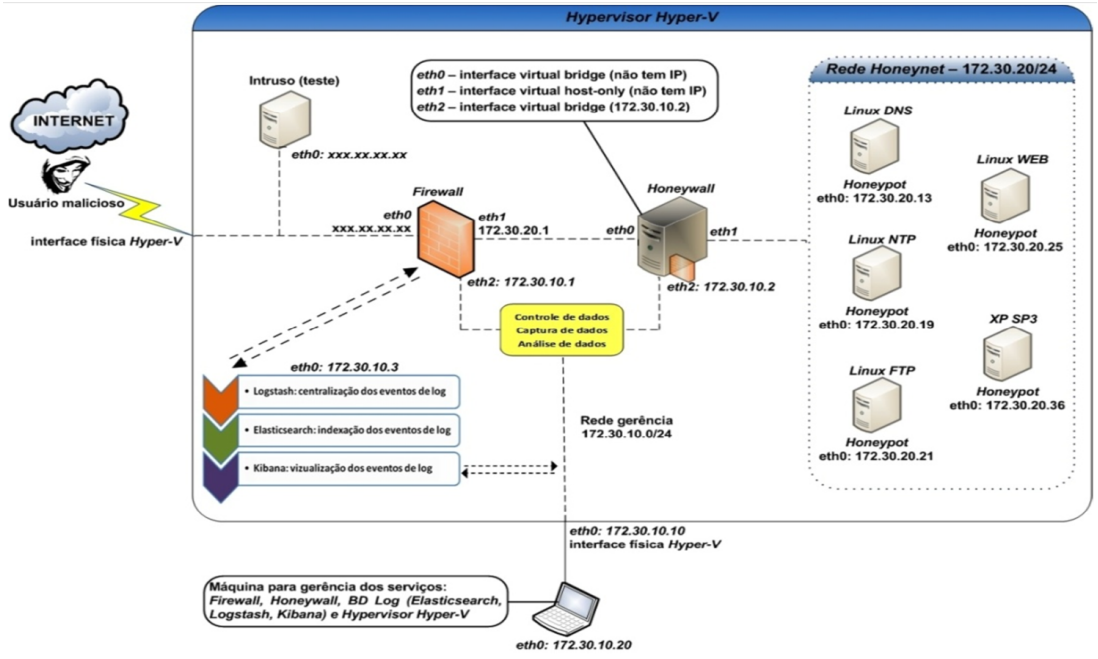


Figura 2.8: Arquitetura do ambiente *HoneySELK* (85).

2.6.3 Repositório de Assinaturas *Emerging Threats*

O *Bleeding Edge Threats* foi fundado por Matt Jonkman e James Ashton no início de 2003 para satisfazer a carência de assinaturas compatíveis com IDS *Open Source* (86). Antes da organização deste

repositório, os profissionais de segurança precisavam monitorar listas de discussão e sites de segurança para coletar novas assinaturas de IDS que estavam sendo discutidas e distribuídas. Outro problema era que não havia como garantir que essas assinaturas eram as mais recentes, não havia como contribuir com um ajuste para melhorar uma assinatura e não havia garantias de que a anomalia já tivesse sido alterada enganando a assinatura. Sendo desde o princípio um projeto executado de modo voluntário usando servidores e recursos doados.

No final de 2007 foi necessária uma mudança e a *Emerging Threats* surgiram para substituir as *Bleeding Edge Threats*. Em 2 de março de 2015, a empresa Proofpoint anunciou que assinou um contrato para adquirir a *Emerging Threats*. Apesar de ser adquirida por uma empresa, todo o repositório de assinaturas continua aberto para a comunidade de segurança cibernética, com atualizações diárias das assinaturas (87).

A empresa Proofpoint mantém, em complemento ao repositório aberto à comunidade, uma base de assinaturas chamada de "Pro", somente acessível através de compra e recebimento de um código de segurança. Esta compra pode ser feita por *e-mail* e no portal <https://etadmin.proofpoint.com/etpro>, apresentado na Figura 2.9.

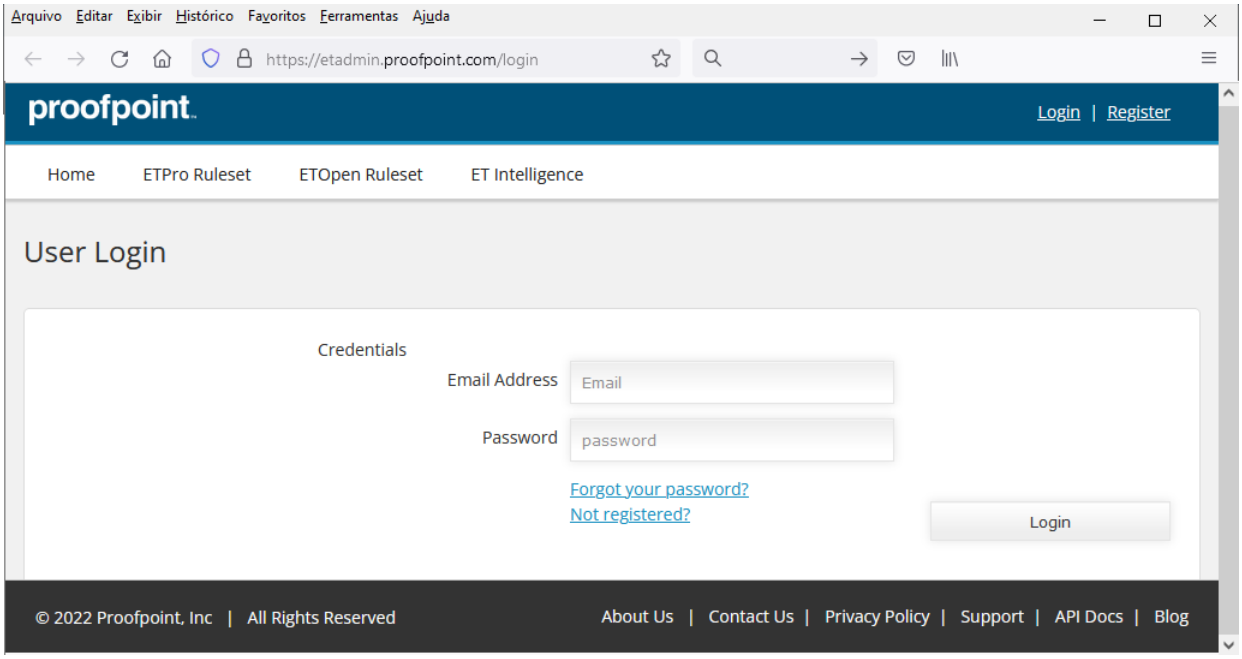


Figura 2.9: Portal para compra do acesso ao repositório "Pro".

2.7 TRABALHOS CORRELATOS

Nos textos pesquisados encontramos várias propostas de soluções recentes utilizando o IDS na proteção da infraestrutura de rede em diversos cenários de aplicação (62) (67) (68). Também encontramos a utilização de aprendizado de máquinas e inteligência artificial em análises de segurança em fluxos de redes (88) e em enriquecimento de dados. Entretanto, a metodologia proposta é explorar flexibilidade de utilização da detecção de incidentes em vários cenários, aliando a utilização de assinaturas com um método de enriquecimento dos dados do registro produzido e posterior armazenamento em Plataformas de Com-

partilhamento de Inteligência de Ameaças (TISPs). A Tabela 2.3 foi construída através de buscas em bases de artigos acadêmicos e selecionando os mais relevantes, relacionando o termo Suricata e o termo MISP.

Tabela 2.3: Resumo dos Trabalhos mais relevantes

Artigo	Resumo
(74)	Proposta de integração de Sistemas de Detecção de Ameaças com honeypots utilizando uma plataforma de TISP (MISP) como repositório de ameaças.
(89)	FISHY usa a coleta de IDS e um sistema para identificação, categorização, classificação e enriquecimento de IoCs usando ML (*Machine Learning*)para sistemas IoT.
(90)	ECAD apresenta um novo conceito para integrar ML (*Machine Learning*) e ferramentas analíticas em uma solução de prevenção e detecção de intrusão em tempo real.
(91)	INTIME é um *framework* integrado baseado em *Machine Learning* e *Deep Learning*.
(92)	A proposta iGen identifica IoCs usando uma Rede Neural Convolucional.
(93)	CyTIME é uma estrutura para gerenciar dados CTI e coletar dados de repositórios externos através de coletores padronizados. Automaticamente gerar regras de segurança.
(94)	A solução APIRO consiste em uma palavra específica da API modelo de incorporação e um modelo de Rede Neural Convolucional.

3 METODOLOGIA PROPOSTA

Neste capítulo descreveremos as características buscadas e as soluções encontradas ao longo da pesquisa bibliográfica. Após esta pesquisa, identificamos uma lacuna metodológica que possibilitou a definição do problema que este trabalho se propõe a solucionar, E ainda, como consequência, foi possível a definição dos requisitos desejáveis da nova metodologia proposta.

3.1 DESCRIÇÃO DO PROBLEMA

A heterogeneidade das topologias, tecnologias e protocolos de rede levam a um complexo cenário de ameaças cibernéticas, já explanadas na Introdução deste trabalho. Toda e qualquer adequação da rede instalada para implantação de sistemas de segurança ou monitoramento é trabalhosa, custosa em termos financeiros e arriscada em termos de disponibilidade.

Outra dificuldade é a construção correta de toda a terminologia que envolve a Inteligência Cibernética, pois é de fundamental importância a correta denominação e identificação assertiva de Indicadores de Comprometimento (IoC) e de Indicadores de Ataque (IoA). Além da determinação da superposição do considerado IoC e IoA, chamado de Indicador de Ameaça. Por este motivo, durante toda a pesquisa bibliográfica buscou-se o atendimento mútuo e simultâneo destes indicadores, pois são os pilares da Inteligência de Ameaça.

Uma preocupação também se reside na acessibilidade às tecnologias por gestores e analistas de segurança, pois em muitos casos estes não podem utilizar de sistemas proprietários por razões de Inteligência Estratégica e Segurança de Estado.

Em última instância, dentro do universo da Inteligência de Ameaças Cibernéticas, observa-se a necessidade de armazenamento e acompanhamento dos registros, além da correlação dos mesmos, com diversas bases de informações. Esta persistência é necessária para investigações futuras, bem como o compartilhamento de informações, muito comuns na Inteligência.

Assim sendo, podemos resumir o nosso problema propondo uma metodologia que atenda a integração de sensores com o mínimo de intervenção na estrutura da rede, que possa colher registros de vários elementos de segurança rede, que consiga identificar IoCs, IoAs e Indicadores de Ameaças, que não seja dependente de sistemas proprietários e, finalmente, contemple o armazenamento e compartilhamento de informações.

3.2 ANÁLISE DOS REQUISITOS

Diante do cenário definido com a exposição dos problemas e a definição dos requisitos, passaremos à análise de cada um dos requisitos identificados.

Para atendimento ao requisito sobre diversidade de complexidade das redes instaladas, devemos propor uma solução que cause uma mínima intervenção na topologia existente, com utilização de elementos modulares que possuam interfaces e acoplamentos bem definidos. Os elementos adicionados devem interagir com os sistemas existentes com ajustes pontuais utilizando mecanismos de leitura de registros já padronizados internacionalmente, conforme preconiza o MITRE (6)(10), citado no Capítulo 1 e, por conseguinte, resulta em registros como o modelo JSON (46), apresentado no Capítulo 2, seção 2.2.1.

Em relação à identificação simultânea de IoCs, IoAs e Indicadores de Ameaças, não podemos escolher modelos, arquiteturas ou *frameworks* que somente utilizem tecnologias de ML ou IA para identificação de Ameaças, pois tais ferramentas necessitam de bases de dados estruturadas de registros coletados em um tempo passado. Como descrito no Capítulo 2, seção 2.3 este tipo de registro é chamado de IoC (13) (49). Somente soluções que avaliem Ameaças em tempo real podem coletar IoAs (34).

No que se refere a não utilização de sistemas proprietários, devemos então restringir a solução para sistemas modulares de código aberto. Estes sistemas são de utilização comunitária, portanto de código aberto e auditável.

Finalmente, para atender o requisito de armazenamento e compartilhamento, a solução deve ser integrada à pelo menos uma Plataforma de Compartilhamento de Inteligência de Ameaças (TISP)(17), citada na Introdução deste documento.

3.3 DETALHAMENTO DA METODOLOGIA PROPOSTA

A proposta é a integração de sensores ativos para a coleta de anomalias utilizando assinaturas pré-selecionadas, alinhadas com a política de segurança e com a estratégia de negócios da organização. Conhecendo o padrão de tráfego na rede podemos escolher as categorias de assinaturas para identificação de anomalias, em conformidade com a política e com a estratégia citadas. Assim, todos os registros gerados são Indicadores de Ameaças ligados diretamente com as tecnologias expostas na rede da organização, pois as categorias de assinaturas escolhidas dependem diretamente dos sistemas e serviços mantidos pela organização. Exemplificado, quando a organização mantém sistemas construídos com um certo tipo de linguagem e banco de dados, podemos escolher categorias de regras que detectem Ameaças para o tipo de tecnologia utilizada. Em outra análise, os tipos de assinaturas de coleta já resultam na classificação dos Indicadores de Ameaças, pois existem assinaturas para detecção de exfiltração de informações ou atuação de malware, detecção de acesso originário de rede anonimizada, tentativas de abuso de servidores DNS ou e-mail, dentre outras categorias.

Basicamente, este trabalho propõe uma metodologia com um fluxo de trabalho, descrito na Figura 3.1, onde:

- no Estágio 1 tem-se a coleta de indicadores, realizada por sensores de monitoração;
- no Estágio 2 tem-se a extração, transformação com foco no enriquecimento dos dados dos registros e a carga na TSIP;
- no Estágio 3 tem-se o armazenamento na TISP;

- em seguida, existe a necessidade de análises dos registros feita pela Equipe de Tratamento e Resposta à Incidentes de Rede (ETIR) local; e
- como resultado, tem-se a produção de regras para continuação da monitoração e defesa da rede.

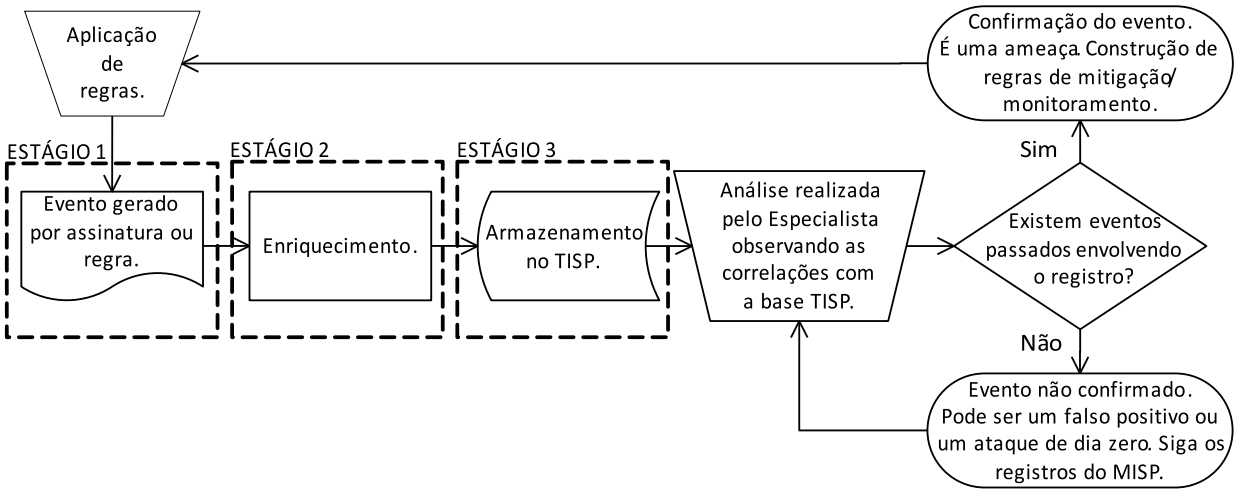


Figura 3.1: Fluxo proposto para a Gestão de Ameaças.

Cabe aqui destacar que os sensores tradicionais trabalham com a utilização de assinaturas, resultantes de estudos sobre vulnerabilidades e comportamento de sistemas. Estes estudos e análises são padrões genéricos que podem identificar ameaças a uma rede específica, mas esta ameaça pode ou não ser um IoC, ou um IoA. Assim, a atuação de analistas de segurança das infraestruturas são essenciais para a efetiva identificação como Indicador de Ameaça.

Outra dificuldade dos sensores ativos tradicionais, que utilizam IDS ou IPS, é que a quantidade de registros gerados pelas assinaturas leva à necessidade de análise posterior às ocorrências. Esta característica temporal da análise, leva a tratar de Indicadores de Comprometimento, pois a ação invasiva já aconteceu, com consequências que podem ou não ainda estar acontecendo. Na maioria dos trabalhos acadêmicos pesquisados encontramos arquiteturas e soluções para pesquisa em bases de dados formadas pelos registros e assim focam em IoCs ou em suas consequências, como veremos mais adiante neste trabalho.

Mas como vimos na seção 2.3, para a coleta de Indicadores de Ameaça necessitamos de um sensor ou coletor que consiga identificar ataques em tempo real. Propomos então a utilização de *honeypots*, ou um conjunto de *honeypots*, chamado de *Honeynet*. Estes sensores são configurados, preferencialmente, com serviços correlatos aos da organização instalados para registro em tempo real das ameaças às possíveis vulnerabilidades. Estes ambientes especiais de monitoração possibilitam um amplo mapeamento e acompanhamento situacional de segurança da organização pela ETIR local.

Tanto dos IDS/IPS ou os *honeypots* possuem a função de captura de informação e registros da rede. Por serem estruturas com propostas diferentes possibilitam uma variedade maior de elementos capturados. Nos IDS/IPS, são mais comuns a geração de registros através das assinaturas, já nos *honeypots* existe a capacidade intrínseca de análise de todo o tráfego com captura de pacotes e detalhamento das TTPs.

A internalização dos dois sistemas de monitoração também é semelhante, possibilitando a detecção no caso do IDS e da *Honeynet*, e o bloqueio no caso de IPS. Neste trabalho estamos mencionando o IPS, pois

muitas redes não possuem *Firewalls* sofisticados que possam bloquear tráfego com base no comportamento de aplicações, por ser configurado diretamente como ponte de acesso à rede de produção, este pode interferir ativamente no tráfego. Essas ações são derivadas de bases de assinaturas, nos caso do IDS/IPS e de regras e políticas configuradas conforme o comportamento de aplicações no caso da *Honeynet*. Cabe ressaltar que a *Honeynet*, apesar de se comportar como um se fosse uma rede em produção, ela está acoplada à rede como um anexo paralelo à rede de produção, não possibilitando a interferência ativa no funcionamento da mesma.

Para possibilitar uma análise rápida e efetiva pela ETIR, o registro gerado pelas regras deve mostrar informações sobre os sistemas efetivamente ameaçados ou possibilitar a caracterização da fonte de ameaça. Assim, quanto mais informações sobre as características do tráfego e dados dos serviços ameaçados forem agregados aos registros produzidos, mais simples será a identificação dos IoCs ou IoAs. Neste aspecto, o IDS/IPS sai na frente, pois as assinaturas já estão organizadas em grupos, quando postadas nos repositórios, e quando são construídas pelas ETIRs locais. A *Honeynet* se mostra especialmente útil na avaliação de regras produzidas pelas ETIRs, pois possibilita a construção e estudo das mesmas sem nenhuma interferência na rede de produção. Entretanto, para identificação rápida e eficiente de ataques, os Sistemas de Detecção de Ameaças são mais ágeis e eficientes.

Assim, os sensores IDS/IPS foram considerados neste trabalho como ativos e permanentes por estarem ativamente atuando na rede, enquanto a *Honeynet* é um tipo de sensor que tem papel mais investigativo. Os *Honeypots* são especialmente eficazes na detecção de ataques desconhecidos, chamados de *zero-day*, pois seu papel principal é monitorar anomalias produzidas na interação dos serviços na rede ou e no comportamento dos sistemas. Os *Honeypots* e os TDSs, além de enviar os eventos ao sistema de enriquecimento, em uma máquina processadora, podem receber novas regras resultantes das análises da ETIR, validando-as. As assinaturas utilizadas no IDS são armazenadas em um espelho na rede interna da organização que faz sincronização da base de assinaturas com bases externas localizadas na Internet, conforme proposto na Figura 3.2.

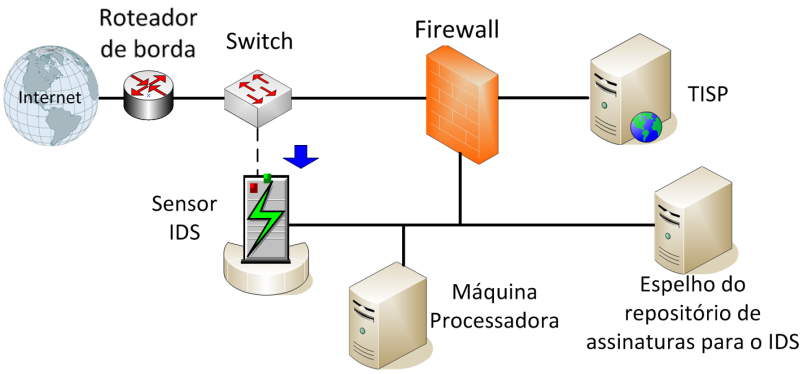


Figura 3.2: Arquitetura da proposta para prova de conceito.

Os dados dos registros dos sensores, são extraídos, transformados ou preparados e carregados em um sistema próprio, por exemplo, em uma máquina processadora dedicada,conforme proposto na Figura 3.2. Antes da manipulação destes registros, tem-se a necessidade de categorizar ou pré-analisar estes para elevar a qualidade das informações e facilitar as análises da ETIR. Assim, mesmo com as categorizações efetuadas pelas assinaturas, existe a necessidade da realização de uma filtragem para retirada de toda e qualquer

informação que não esteja diretamente relacionada com IoCs ou IoAs.

Alguns dados dos registros vindos dos sensores são complementados através de um processamento automatizado, em alguns casos, em apoio à ETIR. Este processamento agrega outras informações para melhor investigação da anomalia. Como exemplo podemos citar o endereço IP (*Internet Protocol*) de origem "*Who*". O enriquecimento desse dado pode resultar em um Nome de Domínio Completamente Qualificado (FQDN) através do acesso automatizado às bases do Sistema de Nomes de Domínio (DNS) armazenadas nos *root name servers*. O FQDN pode identificar imediatamente país de origem e sistema autônomo associado, acelerando a investigação ou a tomada de decisão no caso de ataques. Na avaliação de ataques com TTP´s específicas a serviços da organização, uma investigação mais detalhada deve ser feita pela ETIR sendo subsidiada pelo enriquecimento dos dados. O enriquecimento é a principal fase do tratamento dos dados dos registros.

Após o enriquecimento, o registro é carregado na TISP para verificação de outras ocorrências envolvendo o registro, sendo possível duas situações já explicitadas na Figura 3.1:

- Caso existam eventos já relatados, é uma confirmação de ameaça e a equipe de segurança cibernética passa a acompanhar e monitorar o evento como ataque, e se for o caso, ajustar as regras existentes; ou
- Caso não existam eventos anteriores na TISP, pode ser um falso positivo ou uma tentativa de ataque *Zero Day*. Então, é feito o acompanhamento dos registros na TISP aguardando possíveis outros eventos correlatos.

No caso da identificação de um ataque, podemos aplicar regras que podem ser construídas pela ETIR, formatadas e aplicadas automaticamente pelo sistema. Essas regras podem ser configuradas no *Firewall* da organização, ou no IPS, caso este esteja sendo utilizado na monitoração como um sensor. A Figura 3.3 detalha a metodologia proposta.

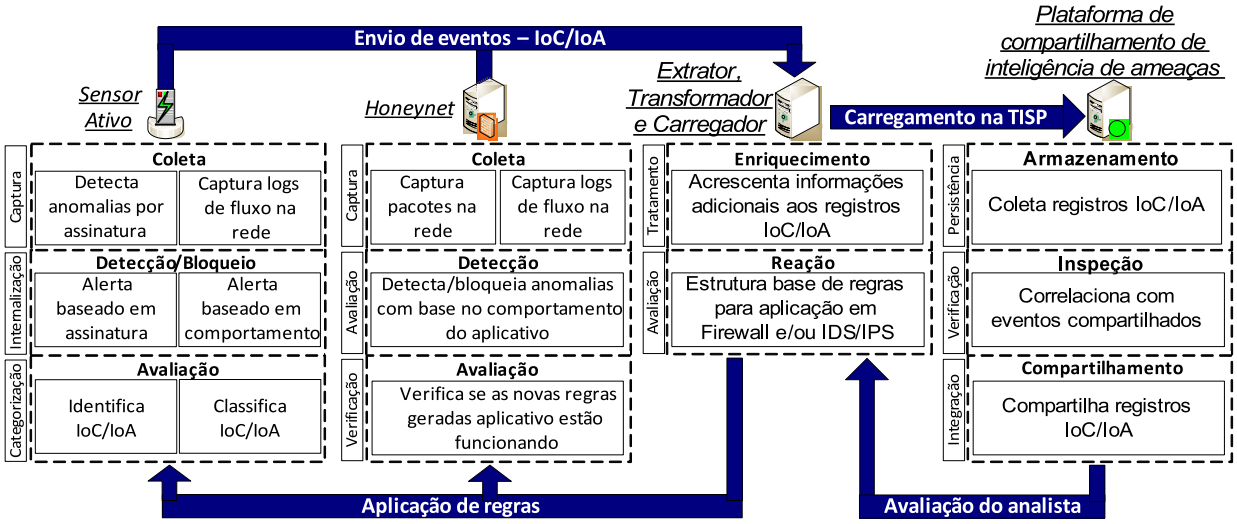


Figura 3.3: Metodologia Proposta.

Em uma última etapa, todos os registros devem ser armazenados em Plataformas de Compartilhamento

de Inteligência de Ameaças (TISPs). Este armazenamento tem a função principal de persistência do registro coletado de forma indexada e devidamente classificado. Entretanto, este armazenamento também propicia a verificação dos registros através da inspeção dos registros de ameaças na base de dados compartilhada por outras organizações. Os registros carregados na TISP devem ser acompanhados, pois eventos compartilhados por outras organizações podem tornar um registro inicialmente sem importância em IoC ou IoA com o passar do tempo. Assim, as TISPs possibilitam o armazenamento com acompanhamento do evento observando novas correlações obtidas dos compartilhamentos das informações de CTI.

Finalmente, através da avaliação do analista, as informações podem ser compartilhadas com outras organizações, bem como ser relevantes para geração e aplicação de regras e políticas na rede de produção.

3.4 METODOLOGIA PROPOSTA EM COMPARAÇÃO AOS TRABALHOS RELACIONADOS

A seguir faremos uma breve análise das técnicas utilizadas pelos principais trabalhos acadêmicos atuais no estudo do Suricata IDS combinado ou não com o TISP MISP. Para possibilitar a montagem da tabela comparativa, identificamos características específicas de uma solução de Detecção de Intrusão, considerando IoC e IoA, além da possibilidade de gerar regras de detecção em *Firewall* e IDS. Outra característica importante é o cenário de aplicação da solução, sendo importante a escalabilidade e flexibilidade de uso em diferentes cenários de rede. Os trabalhos analisados foram relacionados na Tabela 2.3.

No framework denominado INTIME (91) e na proposta iGen apresentada na tese (92), ambos não identificam IoA porque focam na identificação de IoCs. Esses trabalhos utilizam ML, *Deep Learning* e Rede Neural Convolucional para detectar IoCs, portanto, não utilizam assinaturas de sensores e não geram regras de bloqueio em sistemas de *Firewall*. No entanto, eles propõem integração com TISPs, conforme observado na Figura 3.4.

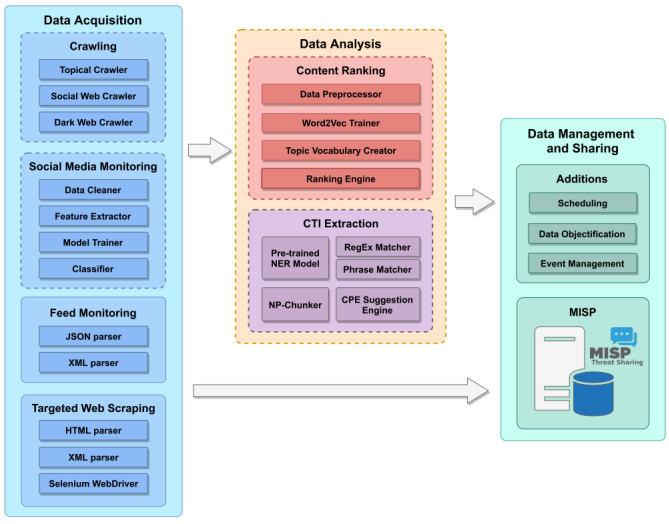


Figura 3.4: Uma visão de alto nível da arquitetura do INTIME (componentes em linhas tracejadas empregam técnicas de machine/deep learning) (91).

Outra proposta encontrada foi o ECAD apresentado no artigo (90). Esta proposta sugere um quadro

mais flexível semelhante à proposta apresentada neste artigo. Também é integrado a um TISP e possibilita a identificação de ataques com a sugestão de instalação de agentes em diversos ativos da infraestrutura de rede. No entanto, como qualquer solução de ML, não considera a possibilidade de adoção de assinaturas pelos sensores e não gera novas assinaturas para os sensores e sistemas de *Firewall*, conforme observado na Figura 3.5.

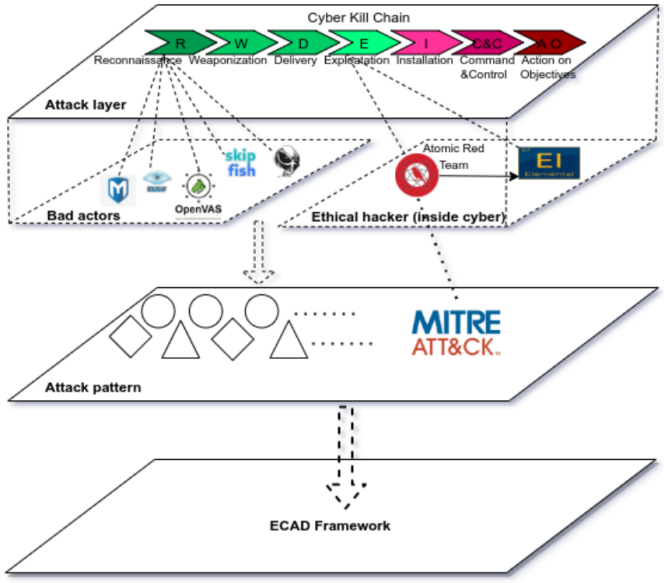


Figura 3.5: O contexto operacional da plataforma de testes para o framework ECAD (90).

No caso do APIRO (94), que também utiliza Rede Neural Convolucional, tem uma abordagem diferente. Baseia-se na construção de APIs (*Application Programming Interface*) para integração de plataformas SOAR (*Security Orchestration, Automation, and Response*). Por permitir a integração de diversas fontes de registros, eles identificam IoA, mas não propõem a geração de regras para bloquear sistemas de *Firewall* e não utilizam diretamente assinaturas de sensores, conforme observado na Figura 3.6.

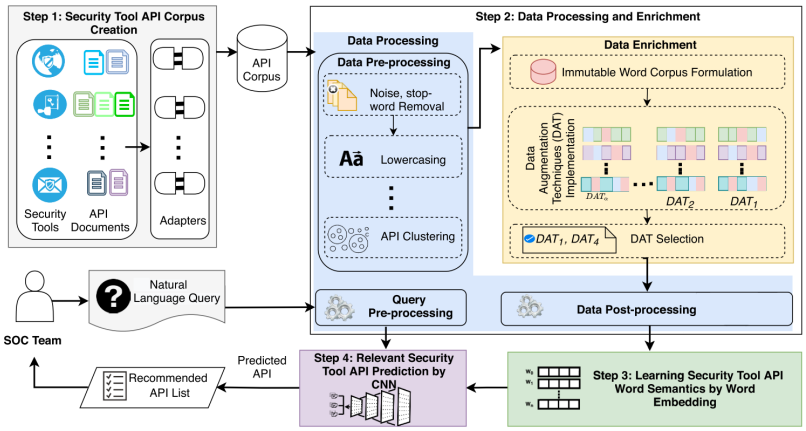


Figura 3.6: Visão geral de alto nível da estrutura APIRO (94).

Uma arquitetura interessante encontrada na pesquisa foi a FISHY apresentada no artigo (89). Esta proposta é bastante robusta e ampla, sendo bastante atual e inovadora, pois sugere uma plataforma que atuaria na nuvem envolvendo diversos protocolos e diferentes tipos de redes. Eles propõem cobrir toda uma cadeia

de suprimentos de forma estruturada, considerando a IoT. Como uma arquitetura baseada exclusivamente na atuação de ML em bases cadastrais, a proposta não contempla a possibilidade de detecção de ataques em tempo real e não utiliza bases de assinatura IDS para detecção. Além disso, não contempla a geração de regras para aplicação em Sistemas de *Firewall* existentes nas redes e não possui integração com TISPs, pois a proposta é para plataforma própria, conforme observado na Figura 3.7.

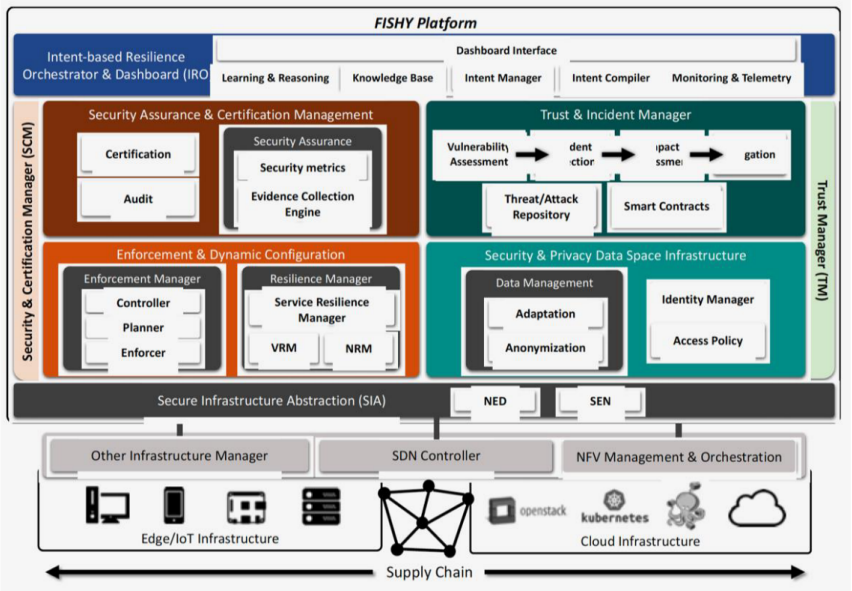


Figura 3.7: Arquitetura funcional FISHY em todo o sistema de TIC (89).

No trabalho (95) é apresentado o modelo ETIP (*Enriched Threat Intelligence Platform*), ou Plataforma de inteligência de ameaças enriquecida, que propõe o enriquecimento de dados coletados por OSINT (Open Source Intelligence), ou Inteligência de fontes abertas. Pressupõem a identificação de IoCs através destas coletas. Os registros são enriquecidos e carregados em TISPs, conforme observado na Figura 3.8.

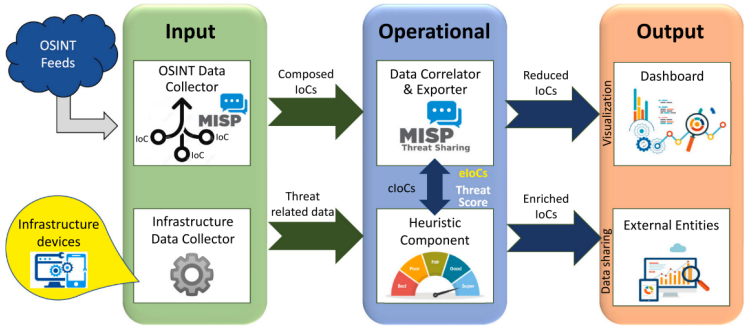


Figura 3.8: A arquitetura do ETIP (95).

No trabalho (74) é apresentada uma proposta de integração dos diversos Sistemas de Detecção de Ameaças (TDS - *Threat Detection System*), que carregam informações em TISPs (no caso foi proposto o MISP) que, se comunica com *honeypots*. A ideia fundamental é que os TDSs podem se beneficiar mutuamente compartilhando conhecimento, pois um conjunto de registros de ameaças compartilhado por um TDS pode ser utilizado por outro para melhorar suas técnicas de detecção de ameaças. Simultaneamente, os mesmos registros podem ser enriquecidos ao permitir a integração de Indicadores fornecidos por diferentes tipos de

TDSs, como conjuntos de *honeypots* trabalhando em conjunto com IDSs. Os *honeypots* podem ser ajustados para caracterizar ainda mais as ameaças subjacentes e fornecer informações importantes sobre elas. A base do trabalho está na utilização de uma TISP como catalogador de Técnicas, Táticas e Procedimentos (TTP) trabalhando como centralizador das ameaças catalogadas, conforme observado na Figura 3.9. Entretanto, a proposta não integra diretamente os TDSs aos *honeypots*, nem tampouco prevê a geração e testagem de novas regras para o sistema de *firewall*. Assim a dependência de inserção das informações no MISP antes do correlacionamento, tratamento e enriquecimento dos registros, não permite uma análise rápida e simples pelos analistas de segurança.

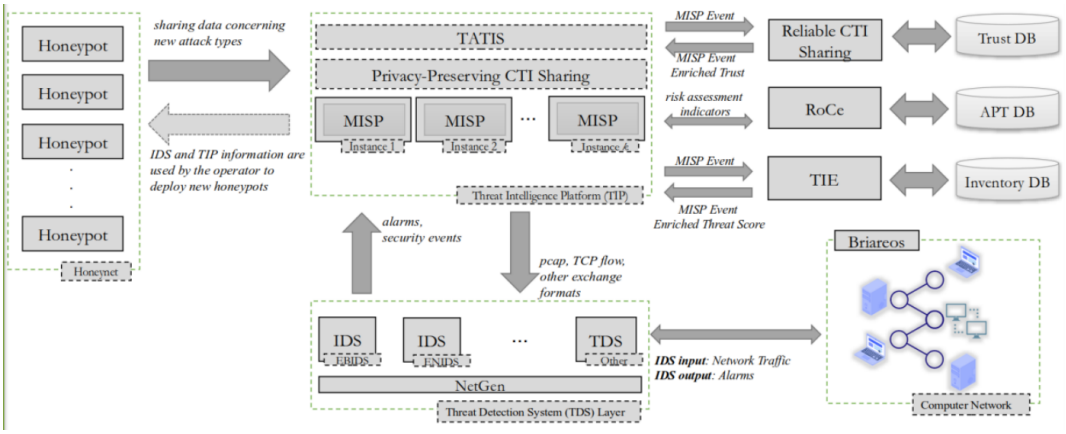


Figura 3.9: Estrutura geral (74).

O projeto Cyber-Trust (96) traz a abordagem interdisciplinar de captura das diferentes fases de ataques emergentes, antes e após vulnerabilidades conhecidas ou desconhecidas (*zero-day*) serem amplamente exploradas por criminosos cibernéticos para lançar o ataque. A ênfase é dada na construção de um sistema proativo de coleta e compartilhamento de inteligência de ameaças cibernéticas para evitar a exploração de vulnerabilidades e falhas de projeto encontradas em dispositivos IoT. Essas informações de inteligência são usadas para manter perfis de vulnerabilidade precisos de dispositivos IoT, conforme a proteção de dados, privacidade ou outros regulamentos, e alterar de maneira ideal sua superfície de ataque para minimizar os danos causados por ataques cibernéticos, conforme observado na Figura 3.10.

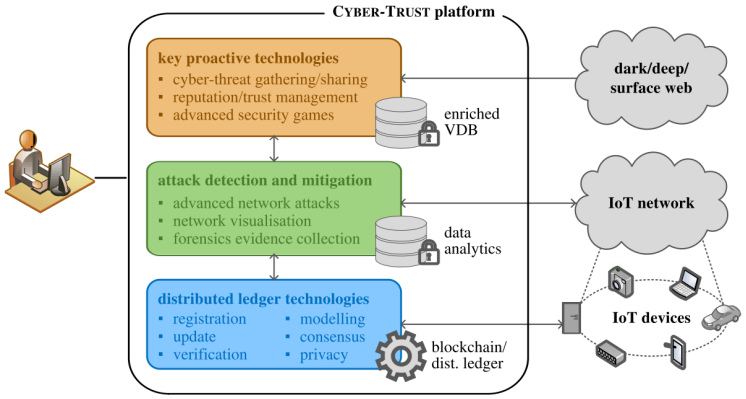


Figura 3.10: Diagrama de alto nível da arquitetura de referência da Cyber-Trust, onde são destacados os principais pilares e ferramentas (96).

CyTIME (93) é outro exemplo de framework que não identifica IoA, mas diferente de trabalhos an-

teriores, não utiliza ML ou AI. Também não usa seus próprios sensores com assinaturas como fonte. No framework proposto, a coleta de registros é feita em bases de *malware*, servidores TAXII e em TISP. Assim, a integração com TISP é para obtenção de IoCs. O objetivo final é gerar regras para os sensores e sistemas de *firewall* das organizações, conforme observado na Figura 3.11.

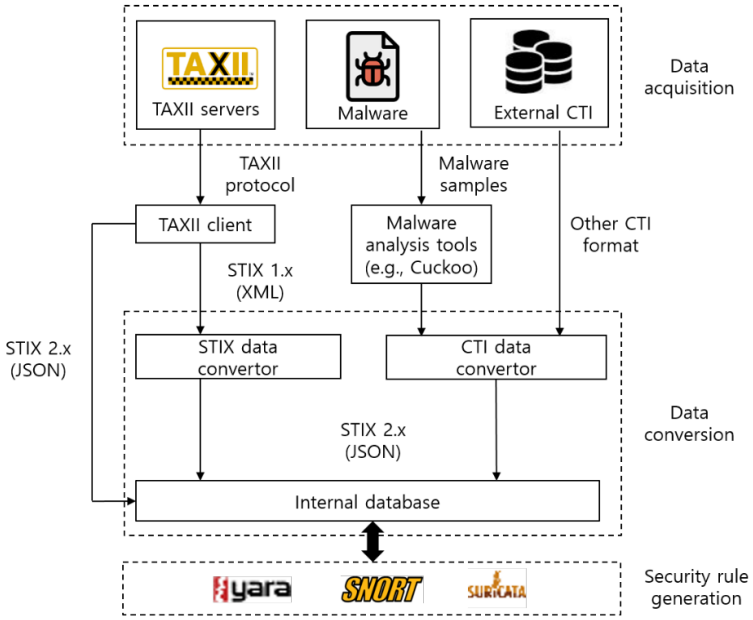


Figura 3.11: Visão geral do CyTIME (93).

No artigo (97) é apresentado o sistema HAVARO, sendo opcional para todas as organizações finlandesas. É um sistema que centraliza registros sobre segurança da informação ao nível nacional. O sistema produz informações, que permitem alertar todos os colaboradores sobre uma ameaça detectada e desenvolver melhores ferramentas de detecção. O trabalho propõe uma evolução do sistema chamado de E-EWS ou *ECHO Early Warning System* versão 2.0. O sistema funciona com diversos tipos de dados e tem como base a detecção de IoCs seguindo o modelo STIX (*Structured Threat Information Expression*), do MITRE, conforme observado na Figura 3.12.

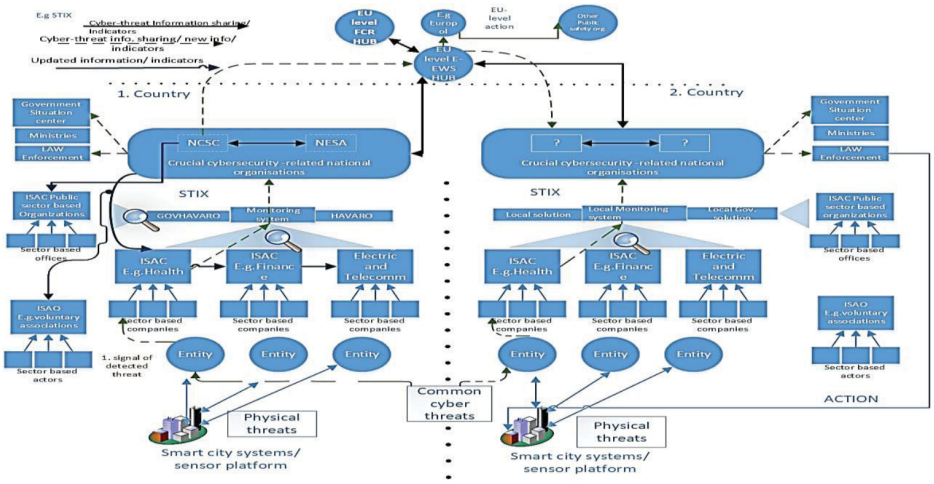


Figura 3.12: Modelo de compartilhamento de informações do E-EWS ou HAVARO 2.0 (97).

A Tabela 3.1 é a síntese das principais características da Metodologia Proposta em relação aos trabalhos pesquisados.

Tabela 3.1: Principais características da Metodologia Proposta.

Artigo	**(74)**	**(89)**	**(90)**	**(91)**	**(92)**	**(93)**	**(94)**	**(96)**	**(97)**	**(95)**	**Metodologia Proposta**
Identifica Ataques em Tempo Real	SIM	NÃO	SIM	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	NÃO	**SIM**
Identifica Comprometimento	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	**SIM**
Possibilita a identificação de APT	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	NÃO	**SIM**
Utiliza assinaturas de IDS	SIM	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	**SIM**
Reação em Tempo Real regras para IDS/*firewall*	NÃO	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	NÃO	NÃO	**SIM**
Integra com TISPs	SIM	NÃO	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	**SIM**

Na avaliação que fizemos dos trabalhos analisados na Tabela 3.1 foram selecionados levando-se em conta a atualidade, publicados os últimos dois anos. E ainda a relação direta com os temas IoC, IDS e TISP. Observamos que em sua maioria trabalham com identificação textual em relatórios ou diretamente na Internet com busca em redes sociais e sites especializados, para em seguida aplicar algoritmos de Inteligência Artificial. Os trabalhos que propuseram arquiteturas ou metodologias se limitaram a discutir teoricamente a possibilidade de inter-relação entre as diversas plataformas, e ainda com enfoque na Internet. Assim, pudemos analisar a tendências dos estudos acadêmicos e identificar a lacuna de conhecimento e o posicionamento desta monografia.

De uma forma geral, a maioria dos trabalhos não estuda a atuação e a integração de sensores ativos nas redes, que possibilita uma atuação rápida e proativa das ETIRs.

3.5 CONTRIBUIÇÕES

Uma característica que se destaca na metodologia proposta é que podemos identificar ataques em tempo real, pois consideramos qualquer fonte de registro, seja IDS ou mesmo uma *Honeynet*, como (90) (94). No entanto, observamos a complexidade da implementação das duas propostas. Além disso, consideramos a *Honeynet* uma excelente fonte de registros com possibilidade de identificação de Indicadores de Ataques (IoA) com implantação, operação e manutenção razoavelmente simples, pois as atividades diárias das equipes de resposta a incidentes de segurança já incluem estudos de TTP, análise de *malware* e computação forense.

Outra abordagem que simplifica a adoção da metodologia proposta é basear-se em registros no formato JSON dos sensores. Assim, não é necessário fazer nenhum interpretador do tipo API ou a construção de um framework específico, como proposto por (94) e (89).

Por fim, em quase todos os *frameworks* e propostas de arquitetura observamos o uso de ML, AI ou Rede Neural Convolucional para identificar ou correlacionar IoCs. A identificação de IoAs quando possível é feita através da adoção de estruturas complexas e com o uso de diversas fontes de registro. Como não usamos ML ou AI, consideramos que os sensores ativos estão usando assinaturas atualizadas de diversas fontes diferentes, tornando a operação, ajustes e manutenção muito ágeis. Outra necessidade presente é a integração com um TISP, pois as equipes de resposta a incidentes de segurança precisam confrontar e compartilhar os registros coletados.

4 PROVA DE CONCEITO

O objetivo pretendido é a construção de um modelo funcional da metodologia proposta que possa ser utilizada em qualquer rede que utilize protocolo TCP/IP. Para a montagem do sensor escolhemos um sistema de IDS/IPS, utilizando tecnologias de código aberto (*open source*) de IDS (ou IPS), associado a mecanismos para detecção de anomalias utilizando assinaturas e análise de fluxos já descritas anteriormente que fornecem registros de ameaças minimamente categorizados e organizados.

4.1 ARQUITETURA DA PROVA DE CONCEITO

Para uma atuação efetiva configuramos o sensor IDS coletando tráfego em um *switch* entre o roteador externo e o *firewall*. Assim a coleta ocorre antes de qualquer filtro ou intervenção. Entretanto, nessa posição o sensor IDS ficaria muito vulnerável a ataques, então configuramos o sensor para apenas executar a coleta tráfego em modo promíscuo, situação em que ele não responde a conexões. Colocamos uma máquina com serviço web como espelho do repositório de assinaturas protegida pelo *firewall*, atualizando as assinaturas diariamente. Assim o sensor busca estas assinaturas na *intranet* e atualiza seu contexto.

O sensor envia os indicadores de ameaças para um sistema de armazenamento de registros na *intranet*, também protegido pelo *firewall*, onde são enriquecidos. Em seguida, os indicadores de ameaça já enriquecidos seguem diretamente para o MISP ou podem ser aplicados no *firewall*. A arquitetura montada para a Prova de Conceito é ilustrada na Figura 4.1.

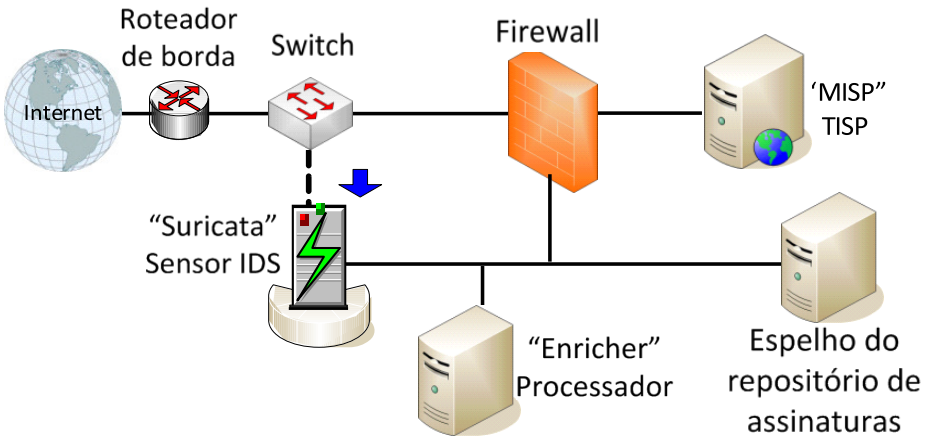


Figura 4.1: Arquitetura da prova de conceito.

O sensor escolhido para a coleta é o Suricata IDS (98). O Suricata pode realizar a coleta de todo o tráfego ou apenas o registro baseado em assinaturas. Considerando a agilidade e otimização das informações que serão produzidas, focaremos apenas nos registros baseados em assinaturas, pois as assinaturas já fornecem uma pré-classificação dos eventos. Assim, ficamos apenas com os registros da atividade já classificada como anômala e aderente à política de segurança da organização.

Em nossa proposta consideramos a base de assinaturas existentes no repositório *Emerging Threats* <https://rules.emergingthreats.net/>. Neste repositório as assinaturas são ofertadas, já classificadas e categorizadas por tipo de Indicador de Ameaça. Todos os dias o repositório é atualizado aproximadamente às 22:00 UTC, com todas as informações identificadas com carimbo de tempo no formato Universal *Sortable Date Time Pattern* "Z" e com registro de horário estendido "T", perfazendo o formado YYYY-MM-DDTHH:MM:SSZ (99). A Figura 4.2 ilustra o repositório de assinaturas.

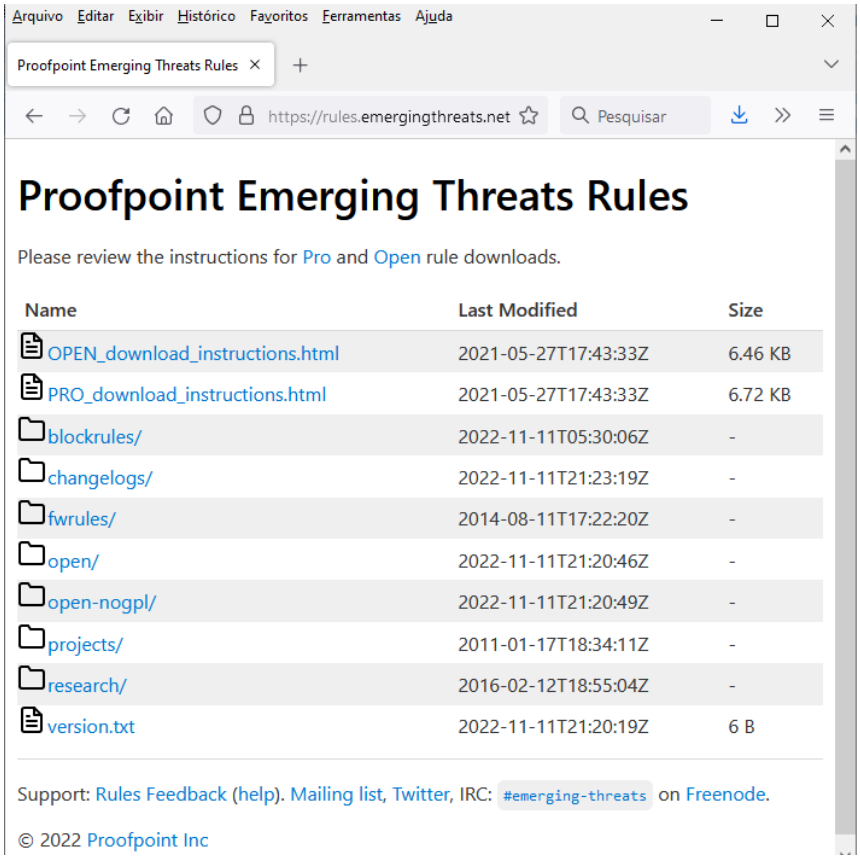


Figura 4.2: Página <https://rules.emergingthreats.net/>.

4.1.1 Sensor: Suricata e *Emerging Threats*

O repositório de assinaturas da *Emerging Threats* é totalmente compatível e configurável no IDS Suricata, contando com um conjunto de regras pré-classificadas em grupos de ameaças, tais como *hosts* identificados como participantes da rede TOR (100), regras de remoção de comando e controle de *botnet* (101), *strings* de ataques conhecidos de *Shell code* (102), dentre outros. Todas atividades, conhecidamente suspeitas, potencialmente maliciosas ou claramente hostis, pela comunidade de segurança cibernética. Assim, instala-se uma ferramenta de IDS/IPS, configura-se um mecanismo de *download* diário desta base de Inteligência de Ameaças no formato de regras de alerta e aplica-se as regras como assinaturas (103).

Na configuração de um IDS, basta ativar e atualizar estas regras, pois apenas há interesse de detectar atividades maliciosas. O resultado é a geração de uma base de registros dos eventos que coincidem com as regras. A escolha das classes de regras, que serão escolhidas para se transformarem em bloqueio, depende da política de segurança da informação e comunicações adotada pela organização.

4.1.2 Enriquecimento dos Dados com Enricher

Um mecanismo para enriquecimento de dados, que pode ser um programa com a função de adicionar informações aos dados dos registros, facilitando a interpretação e análise das informações. Na prova de conceito apresentada sugerimos o Enricher (104), mas poderia ser qualquer sistema que busque em repositórios informações complementares relevantes para os Indicadores de Ameaça, como o Cortex que compõem o projeto TheHive (105).

A opção pelo Enricher foi devido sua simplicidade na implantação no *framework* montado para a prova de conceito, não necessitando de nenhum outro mecanismo associado. Os dois enriquecedores de dados acima citados já fazem integração com o MISP. Iniciando o programa (enricher()) busca nos registros do Suricata em Formato *JavaScript Object Notation* (JSON), por um dos três tipos de parâmetros iniciais de busca:

- Endereço IP;
- Domínio de DNS; ou
- Endereço de *E-mail*.

Assim o programa segue os seguintes passos, conforme fluxograma mostrado na Figura 4.3 (104):

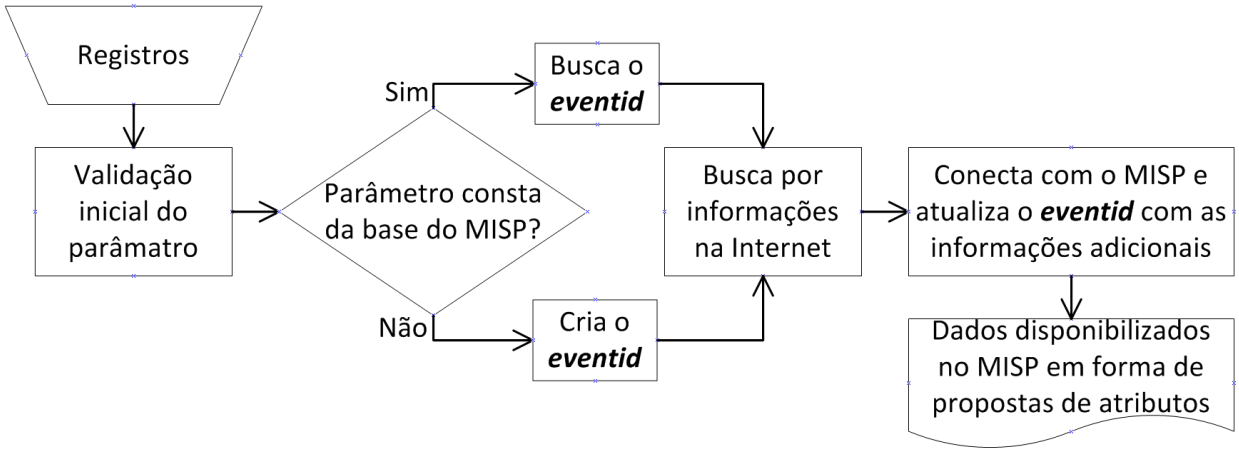


Figura 4.3: Fluxograma simplificado da ferramenta, adaptado de (104).

1. O programa busca um dos parâmetros do alvo e fará uma validação inicial;
2. Feita a validação, o programa fará a primeira conexão com a plataforma MISP para verificar se o parâmetro informado consta da base;
   (a) Caso o evento NÃO EXISTA, o programa criará um evento com o parâmetro informado e enviará para a plataforma recuperando o ***eventid*** para tratamento futuro;
   (b) Caso o evento EXISTA, a plataforma retornará para a ferramenta as informações disponíveis, bem como o ***eventid*** do evento.

3. A ferramenta iniciará uma busca com base nas ferramentas integradas por informações sobre o alvo selecionado. Tal busca se dará de forma cruzada, sendo que, obtendo-se o IP de um Domínio, acionará a busca por informações desse IP, e vice-versa;

4. A busca por *e-mail* gerará também uma busca pelo nome de usuário em sites e rede conhecidas.

5. Finalizada a busca, o programa fará nova conexão com a plataforma, atualizando as informações do evento com os dados encontrados;

6. Os dados serão disponibilizados na plataforma em forma de propostas de atributos. O analista terá a responsabilidade de analisar quais informações são ou não relevantes.

Na prova de conceito implementada, buscamos apenas por endereços IPs dentro dos registros gerados pelo IDS, pois as assinaturas configuradas para a rede de teste não contempla domínio de DNS ou endereço de *e-mail*.

4.1.3 TISP: MISP

O último elemento configurado é o MISP como Plataforma de Compartilhamento de Inteligência de Ameaças (TISPs). O software Suricata e o MISP foram localizados em documentos acadêmicos atuais, sendo este o motivo da escolha (22) (61) (79) (89) (90) (91) (92). O MISP pode ser buscado na página do projeto <https://www.misp-project.org/> Figura 4.4, assim como toda a documentação necessária para sua implantação.

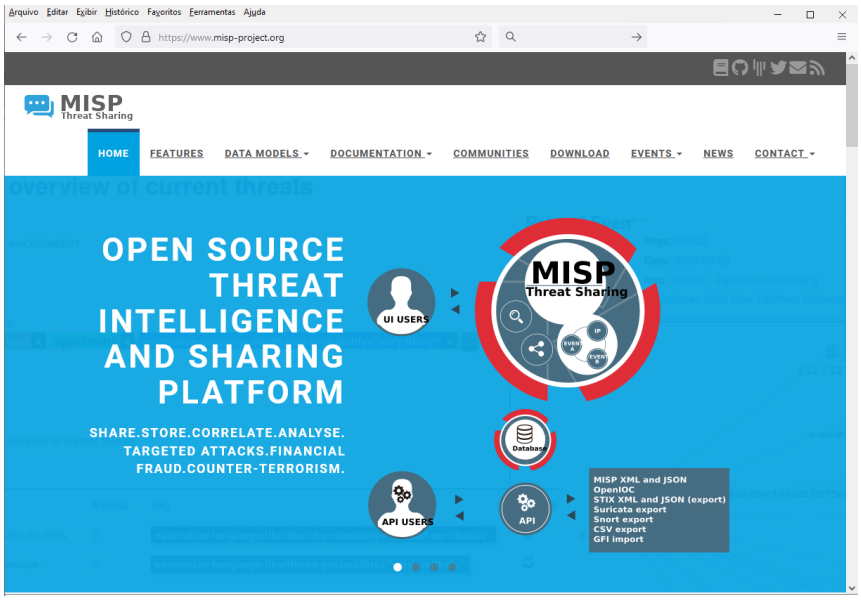


Figura 4.4: Página <https://www.misp-project.org/>.

O CERT.BR também oferece muita documentação, além de cursos e trocas de *scripts* para manuseio de informações na base de dados do MISP.

Assim, a prova de conceito atende a todos os elementos propostos na metodologia, contemplando a coleta, avaliação, enriquecimento, estruturação e compartilhamento dos Indicadores de Ameaças.

4.2 RESULTADOS DA PROVA DE CONCEITO

Na apresentação dos resultados da prova de conceito vamos também descrever os procedimentos executados seguindo o Fluxograma apresentado na Figura 3.1.

Assim, como destaque da Figura 3.1, o primeiro Estágio sendo a geração e armazenamento de registros de eventos gerados por assinatura ou regra, conforme apresentado na Figura 4.5.

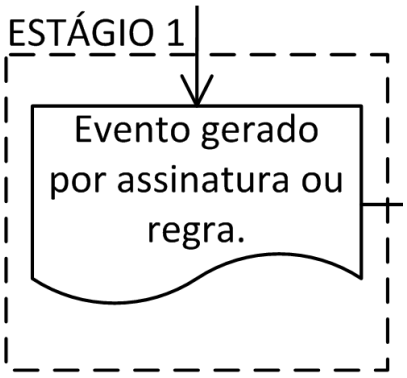


Figura 4.5: Detalhamento da Figura 3.1, Estágio 1.

Os registros são produzidos e armazenados diariamente no IDS em arquivos no formato JSON. Para melhor otimização da arquitetura, o IDS apenas gera os registros sendo os mesmos transferidos para a máquina do Processador onde está implementado o software Enricher, conforme observamos na Figura 4.1. Dentro do Processador que é feita a manipulação dos registros. Assim passamos ao Estágio 2, conforme detalhamento apresentado na Figura 4.6.

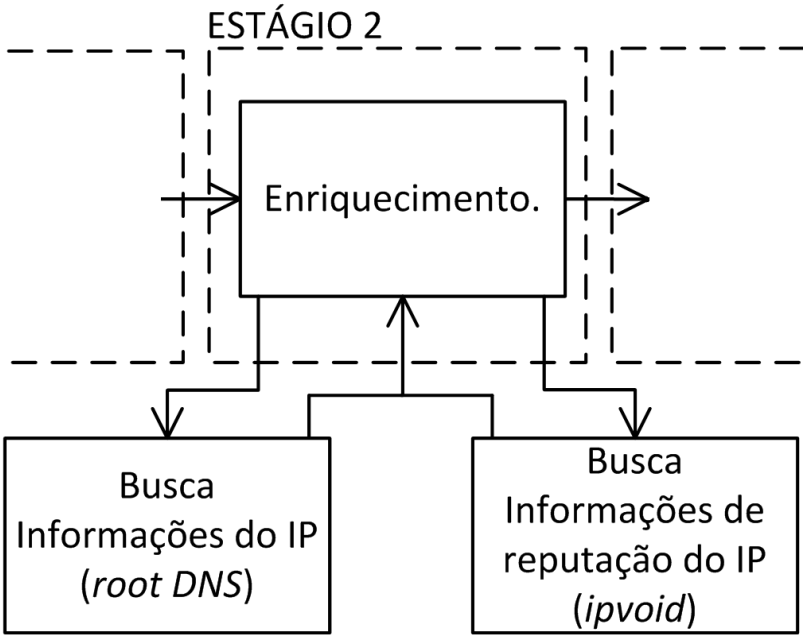
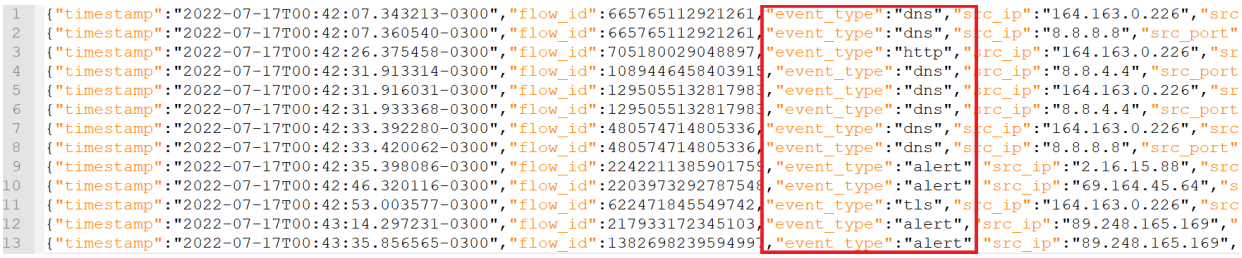


Figura 4.6: Detalhamento da Figura 3.1, Estágio 2.

Após a implementação da prova de conceito em laboratório obtivemos muitos registros, mas vários desses registros eram de rastreamento das comunicações DNS e alertas de monitoração para controle de

TLS e conexões HTTP. Todos misturados com as verdadeiras assinaturas com alertas de possíveis ameaças, como observamos na Figura 4.7.

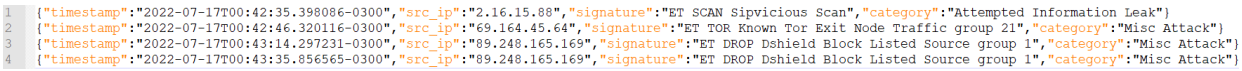


```
{"timestamp":"2022-07-17T00:42:07.343213-0300","flow_id":665765112921261,"event_type":"dns","src_ip":"164.163.0.226","src
{"timestamp":"2022-07-17T00:42:07.360540-0300","flow_id":665765112921261,"event_type":"dns","src_ip":"8.8.8.8","src_port"
{"timestamp":"2022-07-17T00:42:26.375458-0300","flow_id":705180029048897,"event_type":"http","src_ip":"164.163.0.226","sr
{"timestamp":"2022-07-17T00:42:31.913314-0300","flow_id":1089446458403919,"event_type":"dns","src_ip":"8.8.4.4","src_port
{"timestamp":"2022-07-17T00:42:31.916031-0300","flow_id":1295055132817983,"event_type":"dns","src_ip":"164.163.0.226","sr
{"timestamp":"2022-07-17T00:42:31.933368-0300","flow_id":1295055132817983,"event_type":"dns","src_ip":"8.8.4.4","src_port
{"timestamp":"2022-07-17T00:42:33.392280-0300","flow_id":480574714805336,"event_type":"dns","src_ip":"164.163.0.226","src
{"timestamp":"2022-07-17T00:42:33.420062-0300","flow_id":480574714805336,"event_type":"dns","src_ip":"8.8.8.8","src_port"
{"timestamp":"2022-07-17T00:42:35.398086-0300","flow_id":2242211385901759,"event_type":"alert","src_ip":"2.16.15.88","src
{"timestamp":"2022-07-17T00:42:46.320116-0300","flow_id":2203973292787548,"event_type":"alert","src_ip":"69.164.45.64","s
{"timestamp":"2022-07-17T00:42:53.003577-0300","flow_id":622471845549742,"event_type":"tls","src_ip":"164.163.0.226","src
{"timestamp":"2022-07-17T00:43:14.297231-0300","flow_id":217933172345103,"event_type":"alert","src_ip":"89.248.165.169","
{"timestamp":"2022-07-17T00:43:35.856565-0300","flow_id":138269823959499?,"event_type":"alert","src_ip":"89.248.165.169",
```


Figura 4.7: Registro gerado pelo IDS.

Para uma melhor análise das ameaças, dentro do Processador, realizamos uma filtragem nos registro, buscando apenas as entradas com alertas gerados pelas assinaturas, e as informações importantes do registro, tais como ***timestamp***, ***src-ip***, ***signature*** e ***category***. Estas informações são as mais relevantes para a análise de um alerta, pois oferece a possibilidade de verificação de todas as dimensões discutidas no Modelo de Dados 5W3H, apresentado no Capítulo 2, sendo *What, Who, Why, When, Where, How, How much* e *How long*, com a observação de poucos campos do registro gerado.

Este pré-processamento possibilitou uma melhor observação dos alertas, resultando no formato de registro apresentado na Figura 4.8.

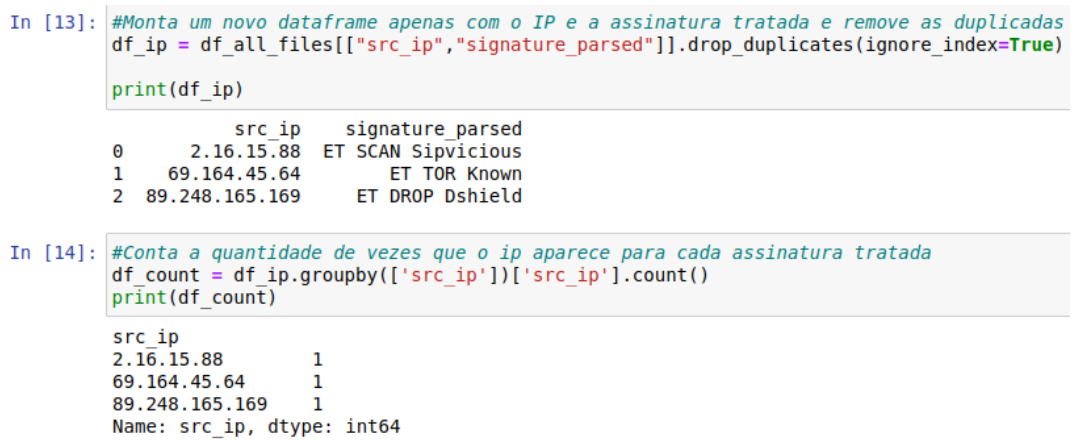


```
{"timestamp":"2022-07-17T00:42:35.398086-0300","src_ip":"2.16.15.88","signature":"ET SCAN Sipvicious Scan","category":"Attempted Information Leak"}
{"timestamp":"2022-07-17T00:42:46.320116-0300","src_ip":"69.164.45.64","signature":"ET TOR Known Tor Exit Node Traffic group 21","category":"Misc Attack"}
{"timestamp":"2022-07-17T00:43:14.297231-0300","src_ip":"89.248.165.169","signature":"ET DROP Dshield Block Listed Source group 1","category":"Misc Attack"}
{"timestamp":"2022-07-17T00:43:35.856565-0300","src_ip":"89.248.165.169","signature":"ET DROP Dshield Block Listed Source group 1","category":"Misc Attack"}
```


Figura 4.8: Registro após a filtragem.

A observação de um registro JSON completo pode ser feita na Tabela 2.2, onde apresentamos um dado coletado por assinatura gerado pelo IDS Suricata implementado.

A seguir, passamos a analisar visualmente os registros, classificando-o por ***signature*** e por IP utilizando a linguagem de programação *python3*, por um ambiente de programação instalado na máquina Processador. A Figura 4.9 mostra o resultado da classificação.



```
In [13]: #Monta um novo dataframe apenas com o IP e a assinatura tratada e remove as duplicadas
         df_ip = df_all_files[["src_ip","signature_parsed"]].drop_duplicates(ignore_index=True)

         print(df_ip)

                src_ip    signature_parsed
         0      2.16.15.88  ET SCAN Sipvicious
         1    69.164.45.64        ET TOR Known
         2  89.248.165.169     ET DROP Dshield

In [14]: #Conta a quantidade de vezes que o ip aparece para cada assinatura tratada
         df_count = df_ip.groupby(['src_ip'])['src_ip'].count()
         print(df_count)

         src_ip
         2.16.15.88        1
         69.164.45.64      1
         89.248.165.169    1
         Name: src_ip, dtype: int64
```


Figura 4.9: Classificação do registro filtrado.

Assim, pudemos observar os alertas com mais entradas nos registros, que em seguida submetemos ao

enriquecimento, conforme ilustrado na Figura 4.10.

```
In [15]: # Código do enriquecedor de IPs

         # Definição de variáveis e desativação do WARNING sobre conexão insegura.
         urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

         # The URL of the MISP instance to connect to
         misp_url = "https://misp.[redacted].br"

         # Can be found in the MISP web interface under
         # http://+MISP_URL+/users/view/me -> Authkey
         misp_key = "HD06Xnhi[redacted]"

         # Should PyMISP verify the MISP certificate
         misp_verifycert = False

         #Conexão com a Plataforma MISP
         misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert)
```

Figura 4.10: Dados para execução do Enricher e carga no MISP (imagem sanitizada por se tratar de sistema em produção).

Esta etapa de visualização dos registros serve ao analista de segurança para analisar imediatamente alguma possível origem de IP que esteja executando mais de uma atividade considerada ameaça pelas assinaturas instaladas no IDS, portanto elevando seu grau de suspeição. Esta classificação pode ser considerada parte do Enriquecimento apresentado na Metodologia Proposta, Figura 3.3.

Finalmente, o Estágio 3 contempla a carga dos registros já enriquecidos para armazenamento no MISP. A seguir destaca-se a Figura 4.11 que apresenta o detalhamento da Figura 3.1, Estágio 3 com análise do Especialista e tomada de decisão.

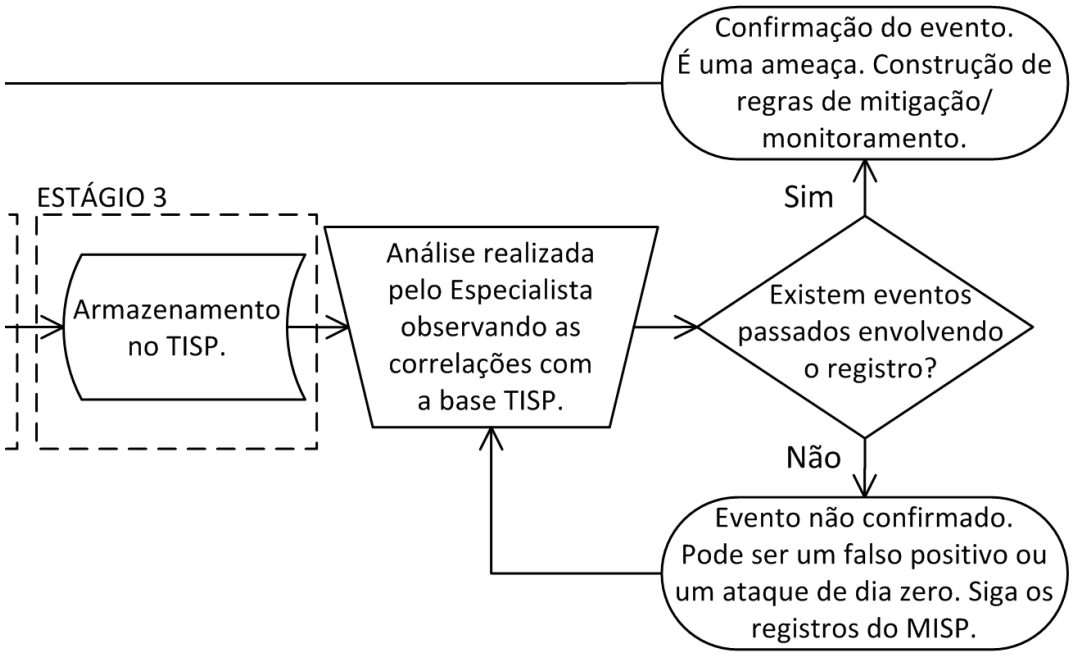


Figura 4.11: Detalhamento da Figura 3.1, Estágio 3 com análise do Especialista e tomada de decisão.

Após a carga no MISP, no dia seguinte observamos, que um endereço IP foi correlacionado com outros

sete eventos já relatados por outras organizações que executam o compartilhamento de registros com nosso CTIR. Outros registros com uma correlação, são inicialmente deixados de lado, pois buscamos endereços IP com registros já constantes no MISP. A identificação de A Figura 4.12 mostra um recorte da tela dos Alertas no MISP de produção.

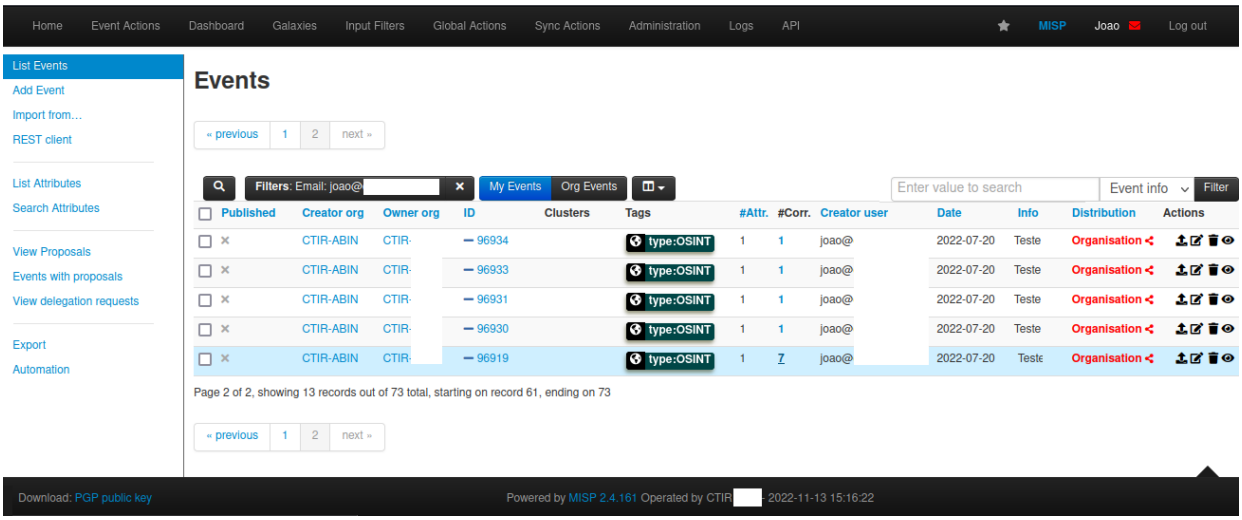


Figura 4.12: Alertas transformados em eventos no MISP (imagem sanitizada por se tratar de sistema em produção).

Assim, observamos que as correlações dos registros enriquecidos são efetuadas automaticamente na base do MISP, como podemos observar na porção direita superior da Figura 4.13. Em nossa prova de conceito, o MISP teve como base o endereço IP para a realização das correlações. Cabe salientar que os eventos encontrados no MISP relacionado com o endereço IP em questão datam de outubro de 2021 e junho de 2019. Um analista de segurança seguramente não considerará estes registros para a classificação do IP como IoA, mas certamente o catalogará como possível IoC, com a devida severidade.

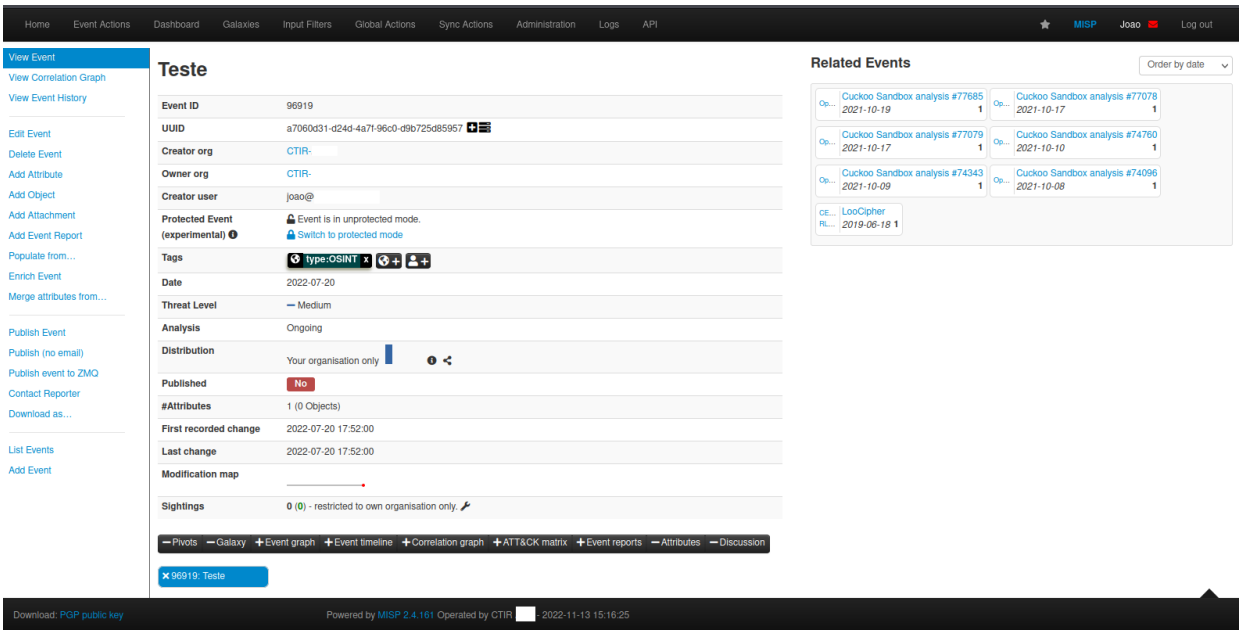


Figura 4.13: Detalhamento dos eventos correlacionados no MISP (imagem sanitizada por se tratar de sistema em produção).

A Figura 4.14 mostra a parte inferior da tela de detalhamento dos eventos correlacionados ao IP de origem "**ip-src**"além dos números identificadores dos eventos já cadastrados no MISP.

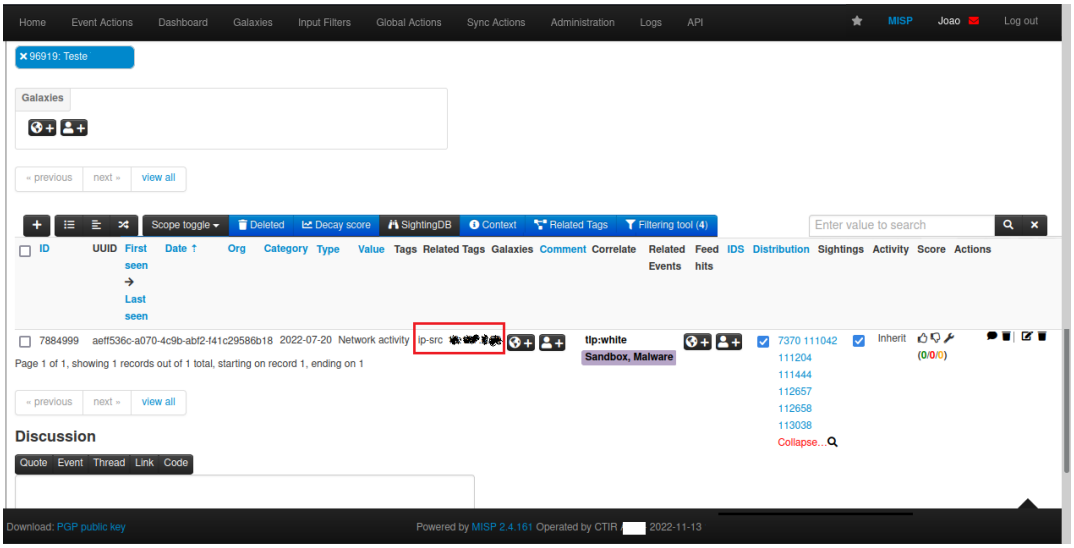


Figura 4.14: Detalhamento dos eventos correlacionados no MISP (imagem sanitizada por se tratar de sistema em produção).

4.2.1 Discussão dos resultados

Em nossa proposta consideramos a base de assinaturas existentes em *Emerging Threats* <https://rules.emergingthreats.net/> para IDSs, onde os IoCs são ofertados já classificados e categorizados. Diante deste artifício, é retirado de mecanismos de ML para enriquecimento de dados dos registros, pois como as assinaturas já identificam corretamente os IoCs, não havendo necessidade de se realizar um enriquecimento para identificá-los. Apenas aplicamos filtros para singularizar eventos.

Conforme o fluxo da Figura 3.1, no primeiro Estágio, o uso de dados de sensores (coletor IDS/IPS) com assinaturas atualizadas acelerou a coleta de informações de qualidade, por meio de regras com assinaturas que fornecem registros de Indicadores de Ameaça minimamente categorizados e organizados. Por envolver coleta e análise em tempo real, foi possível identificar ataques em andamento. Ressalta-se que ao filtrar os registros produzidos pelo IDS, os possíveis IoCs e IoAs foram imediatamente identificados. Assim, houve um ganho de eficiência no processo. A implementação de *Honeypots* permitiria identificar mais facilmente os Indicadores.

A estrutura montada conforme a Figura 4.1 não alterou o funcionamento da rede e possibilitou a coleta transparente de registros. Os equipamentos utilizados no sensor e no enriquecimento dependem apenas da capacidade de armazenamento dos registros necessários para processar a filtragem e o enriquecimento. A filtragem antes do enriquecimento é necessária, pois os logs têm vários dados de sincronização e logs habilitados para auditoria do sistema. Assim, o volume de dados para enriquecimento diminuiu consideravelmente. A máquina com maior capacidade de armazenamento deve ser a TISP, pois funciona como ponto de persistência de dados.

No segundo Estágio, foi realizado o processamento para enriquecimento desses registros com a coleta

de informações complementares relevantes, o que facilitou a identificação de ataques por parte dos analistas. Neste estágio, não houve filtragem de qualidade das informações obtidas no enriquecimento, pois se optou por carregar todos os dados obtidos no TISP para posterior avaliação.

Por fim, no terceiro estágio, os dados foram carregados no MISP. Ficou evidente que a decisão de não realizar a filtragem foi acertada, pois a base de eventos do MISP identificou imediatamente os registros que já possuíam histórico. Assim, foram identificados indicadores e possíveis falsos positivos. Essa identificação é visual e muito simples no MISP. A decisão de compartilhar os registros com outros parceiros MISP é de responsabilidade do analista de segurança, assim como a criação ou aprimoramento de regras para aplicação em sistemas de *firewall*.

Observa-se que a metodologia proposta é facilmente adotada independente das ferramentas utilizadas como sensores e também se adapta bem a qualquer topologia de rede. Outra característica interessante é a possibilidade de montagem de diversos sensores em diversas redes na Internet com a finalidade de produzir Inteligência de Ameaças ao nível setorial ou mesmo nacional, atividade essencial realizada pelos CSIRTs. No entanto, a mesma metodologia pode ser facilmente adotada por uma única organização, onde sua equipe de resposta a incidentes de segurança pode montar vários sensores para identificar ataques, auditorias e tentativas de exfiltração de informações.

5 CONCLUSÃO

A arquitetura proposta desenvolve de um framework metodológico para a geração e análise sistemática dos registros com identificação de padrões anômalos e a derivação de regras de detecção codificadas por meio de assinaturas. Os registros terão a forma de metadados de fluxos que serão enriquecidos, utilizando tecnologias de código aberto (*open source*) de detecção e prevenção de intrusão (IDS - *Intrusion Detection System* e o IPS - *Intrusion Prevention System*).

Caber ressaltar que os metadados utilizados na prova de conceito desta monografia não são considerados dados pessoais, tais como endereços de *e-mail*. Os endereços de *e-mail* podem ser enriquecidos por buscas em bases de informações como repositórios e redes sociais. Esta ressalva é muito importante no cenário brasileiro devido à Lei Geral de Proteção de Dados (LGPD) (106), que entrou em vigor no ano de 2020. Como o tema LGPD é transversal a todo tipo de armazenamento de dados pessoais, o autor desta monografia, durante a construção deste trabalho, fez um estudo mais aprofundado do assunto e publicou o artigo "Mitigação dos Riscos à Privacidade após Anonimização de Dados"(107).

A prova de conceito demonstrou que a arquitetura proposta permite acelerar a identificação de ameaças e possíveis incidentes antes que sejam amplamente reportados pela comunidade, contribuindo para a antecipação de ações de segurança e inteligência de ameaças cibernéticas.

Todos os sistemas utilizados em nossa prova de conceito são *Open Source*, adotando padrões e formatos de protocolos padronizados pela comunidade de Inteligência de Ameaças. Estas características facilitam seu emprego e flexibiliza sua utilização. A sua simplicidade de arquitetura possibilita a adoção em redes de quaisquer tamanhos, desde redes de governo, passando por corporações privadas até pequenas redes com IoT. Assim a metodologia pode ser adotada por qualquer organização, sendo adaptativa a ferramentas e soluções já instaladas, possibilitando a composição sem alteração de *design* da rede com custos reduzidos. A adaptabilidade do sistema de IDS aos diversos protocolos e redes já constituídas incentivam sua adoção.

As organizações modernas possuem em suas estruturas de Tecnologia da informação, equipes de resposta a incidentes de rede CTIR (Centro de Tratamento e Resposta a Incidentes) (108). Essa equipe tem atuação na gestão de incidentes e mantém troca de informações sobre incidentes de rede com outras Equipes de Tratamento de Incidentes, além de alimentar a área de Inteligência Cibernética para a produção de alertas identificando ameaças. O modelo proposto neste trabalho possibilita a aceleração de identificação de ameaças e possíveis incidentes antes que os mesmos sejam reportados pela comunidade, contribuindo para antecipação de ações de segurança e inteligência de ameaças cibernéticas. Atualmente a comunidade dos CTIRs utiliza uma Plataforma de Compartilhamento de Inteligência de Ameaças (TISP) denominada *MISP Threat Sharing* (18). Esta plataforma compartilha ameaças detectadas por sistemas de *firewall* (109) e pode ser alimentada por softwares IDS.

Como resultado desta monografia foram gerados dois artigos apresentados em conferências internacionais. O primeiro publicado foi da Conferência IADIS Ibero-Americana de Computação Aplicada 2022 - CIACA 2022, em Lisboa, artigo com mesmo título da monografia (110), ganhando prêmio de melhor artigo da Conferência. O segundo foi no IV Congreso de Ciencia de la Computacion, Electronica e Industrial,

artigo apresentado e em fase de publicação. Será publicado no *Book series, Lecture Notes in Networks and Systems*, Editora Springer, ISSN Eletrônico 2367-3389.

Para trabalhos futuros, pode-se considerar alguns desdobramentos imediatos, tais como a inclusão da *honeynet* como fonte de registros de eventos, a análise de desempenho dos *scripts* utilizados neste trabalho para avaliar o emprego da arquitetura em escala, mensurando capacidades de hardware e comunicação conforme o volume de dados tratados, e ainda, avaliar ganhos na automação do processo. Por outro lado, pode-se avaliar a integração com outras TISPs, que podem resultar em outros benefícios e implicações.

REFERÊNCIAS BIBLIOGRÁFICAS

1 MCAULIFFE, N.; WOLCOTT, D.; SCHAEFER, L.; KELEM, N.; HUBBARD, B.; HALEY, T. Is your computer being misused? A survey of current intrusion detection system technology. In: *[1990] Proceedings of the Sixth Annual Computer Security Applications Conference*. IEEE Comput. Soc. Press, 1990. December, p. 260–272. ISBN 0-8186-2105-2. ISSN 10639527. Disponível em: <http://ieeexplore.ieee.org/document/143785/>.

2 KALOGERAKI, E.-M.; PAPASTERGIOU, S.; PANAYIOTOPOULOS, T. An Attack Simulation and Evidence Chains Generation Model for Critical Information Infrastructures. *Electronics*, v. 11, n. 3, p. 404, jan 2022. ISSN 2079-9292. Disponível em: <https://doi.org/10.3390/electronics11030404https://www.mdpi.com/2079-9292/11/3/404>.

3 ABDULLAHI, M.; BAASHAR, Y.; ALHUSSIAN, H.; ALWADAIN, A.; AZIZ, N.; CAPRETZ, L. F.; ABDULKADIR, S. J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics*, v. 11, n. 2, p. 198, jan 2022. ISSN 2079-9292. Disponível em: <https://www.mdpi.com/2079-9292/11/2/198>.

4 ALSHBOUL, Y.; BSOUL, A. A. R.; AL Zamil, M.; SAMARAH, S. Cybersecurity of Smart Home Systems: Sensor Identity Protection. *Journal of Network and Systems Management*, Springer, v. 29, n. 3, jul 2021. ISSN 15737705.

5 ZHOU, Y.; TANG, Y.; YI, M.; XI, C.; LU, H. CTI View: APT Threat Intelligence Analysis System. *Security and Communication Networks*, v. 2022, p. 1–15, jan 2022. ISSN 1939-0122. Disponível em: <https://doi.org/10.1155/2022/9875199https://www.hindawi.com/journals/scn/2022/9875199/>.

6 ELMELLAS, J. Knowledge is power: the evolution of threat intelligence. *Computer Fraud and Security*, Elsevier Ltd, v. 2016, n. 7, p. 5–9, 2016. ISSN 13613723. Disponível em: <http://shorturl.at/FIJMT>.

7 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*, Hindawi Limited, v. 2021, p. 1–21, dec 2021. ISSN 2090-715X. Disponível em: <https://www.hindawi.com/journals/jcnc/2021/1302999/>.

8 SCHLETTE, D.; BÖHM, F.; CASELLI, M.; PERNUL, G. Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, Springer Science and Business Media Deutschland GmbH, v. 20, n. 1, p. 21–38, feb 2021. ISSN 1615-5262. Disponível em: <https://link.springer.com/article/10.1007/s10207-020-00490-y?utm_source=getftr&utm_medium=getftr&utm_campaign=getftr_pilothttp://link.springer.com/10.1007/s10207-020-00490-y>.

9 MARCHIO, J. Analytic Tradecraft and the Intelligence Community: Enduring Value, Intermittent Emphasis. *Intelligence and National Security*, Routledge, v. 29, n. 2, p. 159–183, 2014. ISSN 17439019.

10 MITRE Corporation. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). 2012. Disponível em: <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pd>.

11 FIRST. *Version 2 (April 202 Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1 TLP:WHITE Computer Security Incident Response Team (CSIRT) Services Framework*. [S.l.], 2019. Disponível em: <https://www.first.org>.

12 MITRE Corporation. *ATT&CK content available in STIX 2.0 via public TAXII 2.0 server | The MITRE Corporation*. 2012. Disponível em: <https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck-content-available-in-stix-20-via>.

13 SKOPIK, F.; SETTANNI, G.; FIEDLER, R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, Elsevier Ltd, v. 60, p. 154–176, jul 2016. ISSN 01674048. Disponível em: <http://dx.doi.org/10.1016/j.cose.2016.04.003https://linkinghub.elsevier.com/retrieve/pii/S0167404816300347>.

14 THOMSON, A.; KEIRSTEAD, J. *STIX/TAXII™ 2.0 Interoperability Test Document: Part 2 Version 1.0 | Enhanced Reader*. Woburn, MA: OASIS Open, 2018. 85 p. Disponível em: <https://docs.oasis-open.org/cti/stix-taxii-2-interop-p2/v1.0/stix-taxii-2-interop-p2-v1.0.pdf>.

15 JORDAN, B.; PIAZZA, R.; DARLEY, T.; STRUSE, R.; DARLEY, T. *STIX™ Version 2.1*. OASIS Open, 2021. 313 p. Disponível em: <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.docxhttps://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.htmlhttps://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.pdfPreviousstage:https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.>

16 JORDAN, B.; VARNER, D.; STRUSE, R.; DARLEY, T. *TAXII Version 2.1 | Enhanced Reader*. OASIS Open, 2021. 79 p. Disponível em: <https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.pdf>.

17 SANDER, T.; HAILPERN, J. UX Aspects of Threat Information Sharing Platforms. In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. New York, NY, USA: ACM, 2015. p. 51–59. ISBN 9781450338226. Disponível em: <http://dx.doi.org/10.1145/2808128.2808136https://dl.acm.org/doi/10.1145/2808128.2808136>.

18 PROJECT, M. *MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (formely known as Malware Information Sharing Platform)*. MISP project, 2021. Disponível em: <https://www.misp-project.org/>.

19 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*, MDPI AG, v. 13, n. 2, p. 40, feb 2021. ISSN 1999-5903. Disponível em: <https://www.mdpi.com/1999-5903/13/2/40>.

20 HAASTRECHT, M. van; GOLPUR, G.; TZISMADIA, G.; KAB, R.; PRIBOI, C.; DAVID, D.; RăCăTăIAN, A.; BAUMGARTNER, L.; FRICKER, S.; RUIZ, J.; ARMAS, E.; BRINKHUIS, M.; SPRUIT, M. A Shared Cyber Threat Intelligence Solution for SMEs. *Electronics*, v. 10, n. 23, p. 2913, nov 2021. ISSN 2079-9292. Disponível em: <https://doi.org/10.3390/electronics10232913https://www.mdpi.com/2079-9292/10/23/2913>.

21 FERNANDES, R.; PINTO, P.; PINTO, A. Controlled and Secure Sharing of Classified Threat Intelligence between Multiple Entities. In: *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. IEEE, 2021. p. 525–530. ISBN 978-1-6654-4505-4. Disponível em: <https://ieeexplore.ieee.org/document/9647616/>.

22 STOLERIU, R.; PUNCIOIU, A.; BICA, I. Cyber Attacks Detection Using Open Source ELK Stack. In: *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2021. p. 1–6. ISBN 978-1-6654-2534-6. Disponível em: <https://ieeexplore.ieee.org/document/9515120/>.

23 SHOLIHAH, I. M.; SETIAWAN, H.; NABILA, O. G. Design and Development of Information Sharing and Analysis Center (ISAC) as an Information Sharing Platform. In: *2021 Sixth International Conference on Informatics and Computing (ICIC)*. IEEE, 2021. p. 1–6. ISBN 978-1-6654-2155-3. Disponível em: <https://ieeexplore.ieee.org/document/9632989/>.

24 CHRISTIAN, R.; DUTTA, S.; PARK, Y.; RASTOGI, N. An Ontology-driven Knowledge Graph for Android Malware. In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: ACM, 2021. p. 2435–2437. ISBN 9781450384544. Disponível em: <https://doi.org/10.1145/3460120.3485353https://dl.acm.org/doi/10.1145/3460120.3485353>.

25 MENGES, F.; PUTZ, B.; PERNUL, G. DEALER: decentralized incentives for threat intelligence reporting and exchange. *International Journal of Information Security*, v. 20, n. 5, p. 741–761, oct 2021. ISSN 1615-5262. Disponível em: <https://doi.org/10.1007/s10207-020-00528-1https://link.springer.com/10.1007/s10207-020-00528-1>.

26 NASH, A. *Demystifying Cyber Threat Intelligence Sharing Platforms: An evaluation of data quality issues and their effects on cyber attribution*. 58 p. Tese (Master Degree in Science) — Faculty of Utica College, 2021. Disponível em: <https://www.proquest.com/dissertations-theses/demystifying-cyber-threat-intelligence-sharing/docview/2518209169/se-2?accountid=26646>.

27 COLLEN, A.; NIJDAM, N. A. Can I Sleep Safely in My Smarthome? A Novel Framework on Automating Dynamic Risk Assessment in IoT Environments. *Electronics*, v. 11, n. 7, p. 1123, apr 2022. ISSN 2079-9292. Disponível em: <https://www.mdpi.com/2079-9292/11/7/1123>.

28 ALAM, M. T.; BHUSAL, D.; PARK, Y.; RASTOGI, N. CyNER: A Python Library for Cybersecurity Named Entity Recognition. apr 2022. Disponível em: <http://arxiv.org/abs/2204.05754>.

29 SILVA, A. de Melo e; GONDIM, J. J. C.; ALBUQUERQUE, R. de O.; VILLALBA, L. J. G. A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. *Future Internet*, v. 12, n. 6, p. 108, jun 2020. ISSN 1999-5903. Disponível em: <https://www.mdpi.com/1999-5903/12/6/108>.

30 CHESWICK, W. R.; BELLOVIN, S. M. *Firewalls and Internet security : repelling the wily hacker*. Addison-Wesley, 1994. 394 p. ISBN 9788129702074. Disponível em: <https://archive.org/details/firewallsinterne00ches>.

31 CHAPMAN, D. B.; ZWICKY, E. D. *Building Internet Firewalls*. 2. ed. Newton, Massachusetts, EUA: O'Reilly, 1995. 517 p. ISBN 9788173661013. Disponível em: <https://docstore.mik.ua/orelly/networking/firewall/index.htm>.

32 NAKAMURA, E. T.; GEUS, P. L. de. *Segurança de Redes em Ambientes Cooperativos*. 1. ed. São Paulo, SP: Novatec, 2007. 488 p. ISBN 9788575221365. Disponível em: <https://novatec.com.br/livros/seguranca-redes-ambientes-cooperativos/>.

33 BEGLI, M.; DERAKHSHAN, F.; KARIMIPOUR, H. A Layered Intrusion Detection System for Critical Infrastructure Using Machine Learning. In: *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, 2019. p. 120–124. ISBN 978-1-7281-2440-7. Disponível em: <https://ieeexplore.ieee.org/document/8859950/>.

34 ALBASHEER, H.; Md Siraj, M.; MUBARAKALI, A.; Elsier Tayfour, O.; SALIH, S.; HAMDAN, M.; KHAN, S.; ZAINAL, A.; KAMARUDEEN, S. Cyber-Attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey. *Sensors*, v. 22, n. 4, p. 1494, feb 2022. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/22/4/1494>.

35 SIEBERT, E. *Indicadores de ataque versus indicadores de comprometimento*. Austin, Texas, 2020. 11 p. Disponível em: <http://shorturl.at/bru49>.

36 NAM, K.; KIM, K. A Study on SDN security enhancement using open source IDS/IPS Suricata. In: *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2018. p. 1124–1126. ISBN 978-1-5386-5041-7. Disponível em: <https://ieeexplore.ieee.org/document/8539455/>.

37 HOEPERS, C.; STEDING-JESSEN, K.; MONTES, A. Honeynets Applied to the CSIRT Scenario. In: *FIRST*. [s.n.], 2003. p. 9. Disponível em: <http://www.honeynet.org/alliance/>.

38 VANDERGRIFF, L. J. Welcome to the Intelligence Age: an examination of intelligence as a complex venture emergent behavior. *VINE*, v. 38, n. 4, p. 432–444, oct 2008. ISSN 0305-5728. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/03055720810917697/full/html>.

39 SONG, J. The analysis of military intelligence early warning based on open source intelligence. In: *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 2011. p. 226–226. ISBN 978-1-4577-0082-8. Disponível em: <http://ieeexplore.ieee.org/document/5984775/>.

40 JOHNSON, C.; BADGER, L.; WALTERMIRE, D.; SNYDER, J.; SKORUPKA, C. Guide to Cyber Threat Information Sharing. *NIST Special Publication*, v. 800, n. 150, p. 35, 2016. Disponível em: <http://dx.doi.org/10.6028/NIST.SP.800-150>.

41 RIESCO, R.; VILLAGRÁ, V. A. Leveraging cyber threat intelligence for a dynamic risk framework. *International Journal of Information Security*, Springer Berlin Heidelberg, v. 18, n. 6, p. 715–739, dec 2019. ISSN 1615-5262. Disponível em: <http://link.springer.com/10.1007/s10207-019-00433-2>.

42 BLANK, R. M.; GALLAGHER, P. D. *Guide for conducting risk assessments*. Gaithersburg, MD, 2012. Disponível em: <http://csrc.nist.gov/publications.https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

43 MAVROEIDIS, V.; JØSANG, A. Data-Driven Threat Hunting Using Sysmon. In: *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy*. New York, NY, USA: ACM, 2018. p. 82–88. ISBN 9781450363617. Disponível em: <https://dl.acm.org/doi/10.1145/3199478.3199490>.

44 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. p. 51–60. ISBN 9781450331517. Disponível em: <http://dx.doi.org/10.1145/2663876.2663883http://dl.acm.org/citation.cfm?doid=2663876.2663883>.

45 de Oliveira Júnior, G. A.; de Oliveira Albuquerque, R.; Borges de Andrade, C. A.; SOUSA, R. T. de; Sandoval Orozco, A. L.; García Villalba, L. J. Anonymous Real-Time Analytics Monitoring Solution for Decision Making Supported by Sentiment Analysis. *Sensors*, v. 20, n. 16, p. 4557, aug 2020. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/20/16/4557>.

46 STANDARD, J. *The JSON Data Interchange Standard.* 1999. Disponível em: <https://www.json.org/json-en.html>.

47 YOU, Y.; JIANG, J.; JIANG, Z.; YANG, P.; LIU, B.; FENG, H.; WANG, X.; LI, N. TIM: threat context-enhanced TTP intelligence mining on unstructured threat data. *Cybersecurity*, v. 5, n. 1, p. 3, dec 2022. ISSN 2523-3246. Disponível em: <https://doi.org/10.1186/s42400-021-00106-5https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00106-5>.

48 CHO, H.; LEE, S.; KIM, N.; KIM, B.; PARK, J. Method of Quantification of Cyber Threat Based on Indicator of Compromise. In: *2018 International Conference on Platform Technology and Service (PlatCon)*. IEEE, 2018. p. 1–6. ISBN 978-1-5386-4710-3. Disponível em: <https://ieeexplore.ieee.org/document/8472733/>.

49 WAGNER, C.; DULAUNOY, A.; WAGENER, G.; IKLODY, A. MISP. In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. New York, NY, USA: ACM, 2016. p. 49–56. ISBN 9781450345651. Disponível em: <https://dl.acm.org/doi/10.1145/2994539.2994542>.

50 COMISSION, E. *Connecting Europe Facility | Innovation and Networks Executive Agency*. 2021. Disponível em: <https://ec.europa.eu/inea/en/connecting-europe-facility>.

51 CIRCL Luxemburg. *CIRCL » MISP - Open Source Threat Intelligence Platform*. 2022. Disponível em: <https://www.circl.lu/services/misp-malware-information-sharing-platform/>.

52 BOTACIN, M.; CESCHIN, F.; GRÉGIO, A. Corvus: Uma solução Sandbox e de Threat Intelligence para Identificação e Análise de Malware. In: *Anais Estendidos do XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg Estendido 2021)*. Sociedade Brasileira de Computação - SBC, 2021. p. 50–57. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/17339>.

53 W3C. *Extensible Markup Language (XML) 1.0 (Fifth Edition)*. 2008. Disponível em: <https://www.w3.org/TR/REC-xml/>.

54 FILIGRAN. *OpenCTI - Open platform for cyber threat intelligence*. 2022. Disponível em: <https://www.opencti.io/en/>.

55 LUATIX. *Luatix - Cybersecurity and crisis management*. 2022. Disponível em: <https://www.luatix.org/en/>.

56 ANSSI. *OpenCTI – The open source solution for processing and sharing threat intelligence knowledge | Agence nationale de la sécurité des systèmes d'information*. 2022. Disponível em: <https://www.ssi.gouv.fr/en/actualite/opencti-the-open-source-solution-for-processing-and-sharing-threat-intelligence-knowledge/>.

57 BOTACIN, M.; GEUS, P. de; GRÉGIO, A. On the Malware Detection Problem: Challenges & Novel Approaches. In: *Anais Estendidos do XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg Estendido 2022)*. Sociedade Brasileira de Computação - SBC, 2022. p. 25–32. Disponível em: <https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/21688>.

58 WENDT, D. W. *Exploring The Strategies Cybersecurity Specialists Need To Improve Adaptive Cyber Defenses Within The Financial Sector: An Exploratory Study*. 148 p. Tese (D.C.S) — Colorado Technical University, 2019. Disponível em: <https://www.proquest.com/dissertations-theses/exploring-strategies-cybersecurity-specialists/docview/2293040399/se-2?accountid=26646>.

59 IRFAN, A. N.; ARIFFIN, A.; MAHRIN, M. N.; ANUAR, S. A Malware Detection Framework Based on Forensic and Unsupervised Machine Learning Methodologies. In: *Proceedings of the 2020 9th International Conference on Software and Computer Applications*. New York, NY, USA: ACM, 2020. p. 194–200. ISBN 9781450376655. Disponível em: <https://dl.acm.org/doi/10.1145/3384544.3384556>.

60 KRISTIANSEN, L. M.; AGARWAL, V.; FRANKE, K.; SHAH, R. S. CTI-Twitter: Gathering Cyber Threat Intelligence from Twitter using Integrated Supervised and Unsupervised Learning. *Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020*, p. 2299–2308, 2020.

61 MALHOTRA, P.; SINGH, Y.; ANAND, P.; BANGOTRA, D. K.; SINGH, P. K.; HONG, W.-C. Internet of Things: Evolution, Concerns and Security Challenges. *Sensors*, v. 21, n. 5, p. 1809, mar 2021. ISSN 1424-8220. Disponível em: <https://doi.org/10.3390/s21051809https://www.mdpi.com/1424-8220/21/5/1809>.

62 FERRAG, M. A.; BABAGHAYOU, M.; YAZICI, M. A. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications*, v. 52, p. 102500, jun 2020. ISSN 22142126. Disponível em: <https://doi.org/10.1016/j.jisa.2020.102500https://linkinghub.elsevier.com/retrieve/pii/S2214212619311408>.

63 MOREIRA, F. R.; NUNES, R. R.; GIOZZA, W. F.; NZE, G. A. Optimization of the performance of an online payment application by the improviment of its infrastructure. In: *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2020. v. 2020-June, n. June, p. 1–2. ISBN 978-989-54659-0-3. ISSN 21660735. Disponível em: <https://ieeexplore.ieee.org/document/9140895/>.

64 SINGH, V. K.; GOVINDARASU, M. Cyber Kill Chain-Based Hybrid Intrusion Detection System for Smart Grid. In: *Wide Area Power Systems Stability, Protection, and Security*. Springer, Cham, 2021. p. 571–599. Disponível em: <http://link.springer.com/10.1007/978-3-030-54275-7_22>.

65 BOHARA, A. *Information-fusion-based methods to improve the detection of advanced cyber threats*. Tese (Thesis Ph. D.) — University of Illinois, 2020. Disponível em: <http://hdl.handle.net/2142/108614>.

66 BORKAR, A.; DONODE, A.; KUMARI, A. A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS). In: *2017 International Conference on Inventive Computing and Informatics (ICICI)*. IEEE, 2017. p. 949–953. ISBN 978-1-5386-4031-9. Disponível em: <https://ieeexplore.ieee.org/document/8365277/>.

67 BHATI, N. S.; KHARI, M.; GARCÍA-DÍAZ, V.; VERDÚ, E. A Review on Intrusion Detection Systems and Techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, World Scientific, v. 28, n. Supp02, p. 65–91, dec 2020. ISSN 0218-4885. Disponível em: <https://www.worldscientific.com/doi/abs/10.1142/S0218488520400140>.

68 ROOPAK, M.; TIAN, G. Y.; CHAMBERS, J. An Intrusion Detection System Against DDoS Attacks in IoT Networks. In: *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2020. p. 0562–0567. ISBN 978-1-7281-3783-4. Disponível em: <https://ieeexplore.ieee.org/document/9031206/>.

69 Costa Gondim, J.; de Oliveira Albuquerque, R.; Clayton Alves Nascimento, A.; García Villalba, L.; KIM, T.-H. A Methodological Approach for Assessing Amplified Reflection Distributed Denial of Service on the Internet of Things. *Sensors*, v. 16, n. 11, p. 1855, nov 2016. ISSN 1424-8220. Disponível em: <http://www.mdpi.com/1424-8220/16/11/1855>.

70 PINCOVSCY, J. A.; MOURA, A. L. A. *Ataques de negação de serviço por reflexão amplificada utilizando o protocolo SSDP*. 49 p. Tese (Especialização em Guerra Cibernética) — Departamento de Ciência e Tecnologia do Exército Brasiliero, 2016. Disponível em: <https://bdex.eb.mil.br/jspui/handle/1/1012>.

71 SANTOS, P. L. B. dos. *Implementação de plataforma integrada de técnicas de exfiltração de dados*. 74 p. Tese (Especialização em Guerra Cibernética) — Departamento de Ciência e Tecnologia do Exército Brasileiro, Brasília, 2018. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/4202/1/2018CCIBEROF_TENLOAMI.pdf>.

72 THAMES, J. L.; ABLER, R.; KEELING, D. A distributed firewall and active response architecture providing preemptive protection. In: *Proceedings of the 46th Annual Southeast Regional Conference on XX - ACM-SE 46*. New York, New York, USA: ACM Press, 2008. p. 220. ISBN 9781605581057. Disponível em: <http://portal.acm.org/citation.cfm?doid=1593105.1593162>.

73 BOSIRE, S. Information security management. In: *2009 Information Security Curriculum Development Conference on - InfoSecCD '09*. New York, New York, USA: ACM Press, 2009. p. 121. ISBN 9781605586618. Disponível em: <http://portal.acm.org/citation.cfm?doid=1940976.1941000>.

74 GUARASCIO, M.; MANCO, G. *Cooperation with Threat Intelligence Services for deploying adaptive honeypots*. [S.l.], 2019. 61 p. Disponível em: <moz-extension://52af6013-1315-4d55-a889-44aaa2add586/enhanced-reader.

html?openApp&pdf=https://cybersec4europe.eu/wp-content/uploads/2021/10/D3.14-Cooperation-with-Threat-Intelligence-Services-for-deploying-adaptive-honeypots_2.05_submitted>.

75 UCTU, G.; ALKAN, M.; DOGRU, I. A.; DORTERLER, M. A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls. *Future Generation Computer Systems*, v. 124, p. 56–67, nov 2021. ISSN 0167739X. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0167739X21001631>.

76 LEWANDOWSKI, P.; JANISZEWSKI, M.; FELKNER, A. SpiderTrap—An Innovative Approach to Analyze Activity of Internet Bots on a Website. *IEEE Access*, v. 8, p. 141292–141309, 2020. ISSN 2169-3536. Disponível em: <https://ieeexplore.ieee.org/document/9152976/>.

77 ASIF, M. K.; KHAN, T. A.; TAJ, T. A.; NAEEM, U.; YAKOOB, S. Network Intrusion Detection and its strategic importance. In: *2013 IEEE Business Engineering and Industrial Applications Colloquium (BEIAC)*. IEEE, 2013. p. 140–144. ISBN 978-1-4673-5968-9. Disponível em: <http://ieeexplore.ieee.org/document/6560100/>.

78 FARES, A. A. Y. R.; de Caldas Filho, F. L.; GIOZZA, W. F.; CANEDO, E. D.; Lopes de Mendonca, F. L.; Amvame Nze, G. D. DoS Attack Prevention on IPS SDN Networks. In: *2019 Workshop on Communication Networks and Power Systems (WCNPS)*. IEEE, 2019. p. 1–7. ISBN 978-1-7281-2920-4. Disponível em: <https://ieeexplore.ieee.org/document/8896233/>.

79 Hardy Major, R. N.; HANEY, M.; SOULE, T. *Network Security Monitoring for Cyber Situational Awareness*. 75 p. Tese (Doutorado) — University of Idaho, 2020. Disponível em: <https://www.proquest.com/dissertations-theses/network-security-monitoring-cyber-situational/docview/2502196639/se-2>.

80 WANG, X.; LU, X. A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices. *Wireless Communications and Mobile Computing*, v. 2020, p. 1–13, oct 2020. ISSN 1530-8669. Disponível em: <https://doi.org/10.1155/2020/8838571https://www.hindawi.com/journals/wcmc/2020/8838571/>.

81 BORGES, R. *Sistemas de detecção de intrusos e sistemas de prevenção de intrusos: princípios e aplicação de entropia*. 2020. Disponível em: <https://medium.com/mobicareofficial/sistemas-de-detec{ç}{~{a}}o-e-de-preven{ç}{~{a}}o-de-intrusos-princ{í}pios-e-apli>.

82 GUMUSBAS, D.; YLDRM, T.; GENOVESE, A.; SCOTTI, F. A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems. *IEEE Systems Journal*, v. 15, n. 2, p. 1717–1731, jun 2021. ISSN 1932-8184. Disponível em: <https://ieeexplore.ieee.org/document/9099844/>.

83 SCHREIBER, J.; MEEHAN, M.; LANGSTON, R. *2021 Open Source IDS Tools: Suricata vs Snort vs Bro (Zeek) | AT&T Cybersecurity*. 2020. 1 p. Disponível em: <https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview>.

84 HOEPERS, C.; STEDING-JESSEN, K.; CHAVES, M. H. P. C. *Honeypots e Honeynets: Definições e Aplicações*. 2007. Disponível em: <https://www.cert.br/docs/whitepapers/honeypots-honeynets/>.

85 JÚNIOR, G.; Timoteo De Sousa Junior, R.; ALBUQUERQUE, R.; CANEDO, E. D. HoneySELK: Um Ambiente para Pesquisa e Visualização de Ataques Cibernéticos em Tempo Real. In: *Anais do XVI Simpósio em Segurança da Informação e de Sistemas Computacionais - SBSeg 2016*. Sociedade Brasileira de Computação, 2016. p. 697–706. Disponível em: <https://www.researchgate.net/publication/311796391>.

86 COMMUNITY. *Emerging Threats*. 2007. Disponível em: <https://rules.emergingthreats.net/>.

87 PROOFPOINT. *Emerging Threats - now part of Proofpoint | LinkedIn*. 2015. Disponível em: <https://www.linkedin.com/company/emerging-threats>.

88 SHAFIQ, M.; YU, X.; BASHIR, A. K.; CHAUDHRY, H. N.; WANG, D. A machine learning approach for feature selection traffic classification using security analysis. *The Journal of Supercomputing*, Springer New York LLC, v. 74, n. 10, p. 4867–4892, oct 2018. ISSN 0920-8542. Disponível em: <https://link.springer.com/article/10.1007/s11227-018-2263-3http://link.springer.com/10.1007/s11227-018-2263-3>.

89 MASIP-BRUIN, X.; MARÍN-TORDERA, E.; RUIZ, J.; JUKAN, A.; TRAKADAS, P.; CERNIVEC, A.; LIOY, A.; LÓPEZ, D.; SANTOS, H.; GONOS, A.; SILVA, A.; SORIANO, J.; KALOGIANNIS, G. Cybersecurity in ict supply chains: Key challenges and a relevant architecture. *Sensors*, MDPI, v. 21, n. 18, sep 2021. ISSN 14248220.

90 MIRONEANU, C.; ARCHIP, A.; AMARANDEI, C.-M.; CRAUS, M. Experimental Cyber Attack Detection Framework. *Electronics*, MDPI AG, v. 10, n. 14, p. 1682, jul 2021. ISSN 2079-9292. Disponível em: <https://www.mdpi.com/2079-9292/10/14/1682>.

91 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*, v. 10, n. 7, p. 818, mar 2021. ISSN 2079-9292. Disponível em: <https://doi.org/10.3390/electronics10070818https://www.mdpi.com/2079-9292/10/7/818>.

92 PANWAR, A.; AHN, G.-J.; DOUPÉ, A.; ZHAO, Z. *iGen: Toward Automatic Generation and Analysis of Indicators of Compromise (IOCs) using Convolutional Neural Network*. Tese (Master of Science) — Arizona State University, 2017. Disponível em: <https://hdl.handle.net/2286/R.I.44216>.

93 KIM, E.; KIM, K.; SHIN, D.; JIN, B.; KIM, H. CyTIME: Cyber Threat Intelligence ManagEment framework for automatically generating security rules. In: *Proceedings of the 13th International Conference on Future Internet Technologies*. New York, NY, USA: ACM, 2018. Part F1377, p. 1–5. ISBN 9781450364669. Disponível em: <https://dl.acm.org/doi/10.1145/3226052.3226056>.

94 SWORNA, Z. T.; ISLAM, C.; BABAR, M. A. APIRO: A Framework for Automated Security Tools API Recommendation. *ACM Transactions on Software Engineering and Methodology*, p. 41, mar 2022. ISSN 1049-331X. Disponível em: <https://arxiv.org/abs/2201.07959v1http://arxiv.org/abs/2201.07959https://dl.acm.org/doi/10.1145/3512768>.

95 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, v. 58, p. 102715, may 2021. ISSN 22142126. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S2214212620308589>.

96 KOLOKOTRONIS, N.; SHIAELES, S.; BELLINI, E.; CHARALAMBOUS, L.; KAVALLIEROS, D.; GKOTSOPOULOU, O.; PAVUE, C.; BELLINI, A.; SARGSYAN, G. Cyber-trust: The shield for IoT cyber-attacks. *Resilience and Hybrid Threats: Security and Integrity for the Digital World*, Amsterdam, The Netherlands, p. 76–93, 2019. Disponível em: <https://books.google.com.br/books?id=zGTIDwAAQBAJ&pg=PA76&dq=Resilience+and+Hybrid+Threats:+Security+and+Integrity+for+the+Digital+World&lr=&hl=pt-BR&source=gbs_toc_r&cad=3#v=onepage&q=ResilienceandHybridThreats%3ASecurityandIntegrityfortheDigita>.

97 SIMOLA, J.; LEHTO, M. J. National cyber threat prevention mechanism as a part of the E-EWS. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, Acpil, Norfolk, Virginia, p. 539–548, 2020. Disponível em: <https://doi.org/10.34190/ICCWS.20.106>.

98 OISF. *Suricata | Open Source IDS / IPS / NSM engine*. Open Information Security Foundation, 2020. Disponível em: <https://suricata-ids.org/https://github.com/OISF/suricata/>.

99 DTF. *Date Time Format Info. Universal Sortable Date Time Pattern*. 2022. Disponível em: <http://shorturl.at/gKX27>.

100 ALHARBI, A.; FAIZAN, M.; ALOSAIMI, W.; ALYAMI, H.; AGRAWAL, A.; KUMAR, R.; KHAN, R. A. Exploring the Topological Properties of the Tor Dark Web. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 21746–21758, 2021. ISSN 2169-3536. Disponível em: <https://ieeexplore.ieee.org/document/9340182/>.

101 SHINAN, K.; ALSUBHI, K.; ALZAHRANI, A.; ASHRAF, M. U. Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review. *Symmetry*, Multidisciplinary Digital Publishing Institute, v. 13, n. 5, p. 866, may 2021. ISSN 2073-8994. Disponível em: <https://www.mdpi.com/2073-8994/13/5/866/htmhttps://www.mdpi.com/2073-8994/13/5/866>.

102 LEE, J.; LEE, Y.; LEE, D.; KWON, H.; SHIN, D. Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 80866–80872, 2021. ISSN 2169-3536. Disponível em: <https://ieeexplore.ieee.org/document/9444397/>.

103 ALCANTARA, L.; PADILHA, G.; ABREU, R.; D'AMORIM, M. Syrius: Synthesis of Rules for Intrusion Detectors. *IEEE Transactions on Reliability*, v. 71, n. 1, p. 370–381, mar 2022. ISSN 0018-9529. Disponível em: <https://ieeexplore.ieee.org/document/9380789/>.

104 SOUSA, C. E. de; GONDIM, J. J. C.; ALBUQUERQUE, R. d. O. *ENRICHER:ferramenta de enriquecimento de dados integrada à plataforma MISP*. 31 p. Tese (Dissertation completion graduation) — Universidade de Brasília, 2021.

105 ADOUANI, N.; FRANCO, T.; KADHI, S.; LEONARD, J.; CO, D.; KUHNERT, N. *TheHive Project*. 2022. Disponível em: <https://thehive-project.org/>.

106 Lei nº 13.709, d. . d. A. d. . *Lei Geral de Proteção de Dados Pessoais (LGPD)*. 2018. Disponível em: <http://shorturl.at/tzCW9>.

107 FERREIRA, J. R.; PINCOVSCY, J. A.; RIBEIRO, C. d. M.; CANEDO, E. D.; MENDONÇA, F. L. L. de. Mitigação dos Riscos à Privacidade através da Anonimização de Dados. *Revista Ibérica de Sistemas e Tecnologias de Informação - RISTI*, Rio Tinto, Portugal, p. 573–585, Apr 2022. ISSN 1646-9895. Disponível em: <http://www.risti.xyz/issues/ristie49.pdf>.

108 TANCZER, L. M.; BRASS, I.; CARR, M. CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, v. 9, n. November, p. 60–66, nov 2018. ISSN 17585880. Disponível em: <https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12625>.

109 ALSHEHRI, M. Generic Attribute Scoring for Information Decay in Threat Information Sharing Platform. *Computers, Materials & Continua*, v. 67, n. 1, p. 917–931, 2021. ISSN 1546-2226. Disponível em: <https://www.techscience.com/cmc/v67n1/41224>.

110 PINCOVSCY, J. A.; GONDIM, J. J. C. Metodologia para Inteligência de Ameaças Cibernéticas com Integração de Sensores. In: *Conferência Ibero-Americana Computação Aplicada 2022 - CIACA 2022*. Lisboa: IADIS Press, 2022. p. 75–82. ISBN 978-989-8704-45-0. Disponível em: <https://ciaca-conf.org/wp-content/uploads/2022/11/3_CIACA2022_PT_F_047.pdf>.