Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

ENRICHER: ferramenta de enriquecimento de dados integrada à plataforma MISP

Carlos Eduardo de Sousa

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Orientador
Prof. Dr. João José Costa Gondim

Coorientador
Prof. Dr. Robson de Oliveira Albuquerque

Brasília
2021

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

ENRICHER: ferramenta de enriquecimento de dados integrada à plataforma MISP

Carlos Eduardo de Sousa

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Prof. Dr. João José Costa Gondim (Orientador)
CIC/UnB

Prof. Dr. Robson de Oliveira Albuquerque
ENE/UnB

Prof. Dr. Marcos Fagundes Caetano
CIC/UnB

Prof. Dr. João José Costa Gondim
Coordenador do Curso de Engenharia da Computação

Brasília, 18 de novembro de 2021

Dedicatória

À minha querida mãe e meus amados filhos.

Agradecimentos

Aos *Orixás*, por me suprirem de sabedoria, iluminação e persistência. *Eparrey oyá! Laroyé!*

À *minha mãe, Dona Dilma*, pelo apoio irrestrito e exemplo de luta e determinação. Muito obrigado mãe guerreira!!

Aos *meus filhos queridos*, pelo sacrifício da minha ausência em alguns momentos durante todo o curso.

Aos *meus irmãos, familiares e amigos*, pelo apoio constante, mesmo inconsciente.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

Este trabalho propõe a implementação de uma ferramenta integrada com a plataforma MISP para enriquecimento de Inteligência de ameaças cibernéticas (CTI). A funcionalidade da ferramenta, implementada em Python, consiste em se conectar com a plataforma MISP e realizar buscas de informações sobre alvos específicos com auxílio de ferramentas integradas disponibilizadas por terceiros.

Palavras-chave: Segurança cibernética, Inteligência de ameaças cibernéticas, MISP

Abstract

This work proposes the implementation of a tool integrated with the MISP platform to enrich Cyber Threat Intelligence (CTI). The tool's functionality, implemented in Python, consists of connecting to the MISP platform and searching for information about specific targets with the help of integrated tools made available by third parties.

Keywords: Cybersecurity, Cyber Threat Intelligence, MISP

Sumário

Lista de Figuras

Capítulo 1

Introdução

O presente trabalho tem como intuito apresentar aspectos sobre Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI), bem como propor um modelo de enriquecimento de inteligência integrado à plataforma de Inteligência de Ameaças MISP e seus padrões.

1.1 Motivação

No ano de 2020, os protocolos, técnicas, práticas e estratégias de segurança se viram sob forte ataque, sendo extremamente testados como nunca antes. Somadas às oportunidades de violação apresentadas pela pandemia do Coronavírus, operações de baixo risco e alta recompensa tem atraído novos criminosos cibernéticos [1]. Além das ameaças que visam lucro, como sequestro de dados e invasão de bases para roubo de informações, tem-se ainda ameaças político-ideológicas como por exemplo o cyberterrorismo. São inúmeras as possibilidades de ameaças, de forma que os procedimentos para detecção, prevenção e difusão das informações deva ser constantemente otimizado.

O conhecimento prévio de ameaças cibernéticas tem sido buscado de maneira incessante por analistas, equipes de segurança cibernética, CSIRTs, dentre outros profissionais. Ter a inteligência certa no momento certo pode fazer toda a diferença. E umas das informações iniciais numa análise/detecção de ameaças são o endereço IP, Domínio e email de um possível atacante.

Desta forma, uma proposta de enriquecimento de informações referentes a um endereço IP, Domínio ou Email, com base em padrões amplamente utilizados pode representar um ganho considerável na produção de conhecimento referente a um possível ataque.

1.2 Objetivos

O presente trabalho visa desenvolver uma ferramenta em PYTHON capaz de enriquecer dados de CTI referente a um endereço IPv4, URL ou Email e retroalimentar uma plataforma de MISP com base nos principais padrões utilizados.

1.2.1 Objetivo Geral

Propor e implementar uma ferramenta de enriquecimento integrada à plataforma MISP.

1.2.2 Objetivo Específico

- Apresentar definições de Cyber Threat Intelligence (CTI);
- Apresentar de forma sintética a plataforma MISP e seus os padrões utilizados;
- Definir enriquecimento e sua interação com outras fases do ciclo de inteligência;
- Apresentar a ferramenta de enriquecimento integrada com os resultados de algumas simulações.

1.3 Organização do texto

Este trabalho foi ordenado em quatro capítulos, sendo este primeiro o de Introdução.

O Capítulo 2 trata sobre o referencial teórico relativo a Inteligência, Inteligência de Ameaças Cibernéticas (CTI), à plataforma MISP e seus padrões e definições sobre enriquecimento, que serão implementados no presente trabalho.

O Capítulo 3 traz informações referentes à concepção e implementação da ferramenta, apresentando sua arquitetura e tecendo comentários sobre sua utilização.

O Capítulo 4 apresenta casos de uso da ferramenta com resultados experimentais de buscas realizadas e seus respectivos enriquecimentos.

O Capítulo 5 conclui este trabalho, com considerações sobre seus resultados.

Capítulo 2

Referencial Teórico

Neste capítulo serão apresentados os principais conceitos referentes à inteligência de ameaças cibernéticas (CTI), à plataforma de inteligência de ameaças MISP e aos padrões, protocolos e linguagens utilizados.

2.1 Conceitos Relacionados

2.1.1 Inteligência

Ao abordar o tema se faz necessário explanar conceitos relativos à atividade de produção de conhecimento, inteligência e ameaças, uma vez que são os aspectos principais tratados no presente projeto.

Considerando que a necessidade de conhecimento é inerente à humanidade desde os primórdios, a produção deste conhecimento acompanha a história do homem inicialmente sendo realizada de forma instintiva. Era necessário conhecer o comportamento de suas presas e seus predadores para melhor chance de sobrevivência. Com o passar dos tempos essas atividades foram tomando forma com base na intelectualidade da sociedade e variações de objetivos.

Nos dias atuais, são muitas as definições de **Inteligência** de acordo com os contextos aos quais a atividade está inserida. Para o presente contexto, será considerada a Inteligência como sendo a atividade de coleta de dados e produção de conhecimentos, disponibilizando-os aos tomadores de decisão, não antes de determinar o valor, a veraci-

Figura 2.1: Fases da Produção de Inteligência

dade e a importância dos dados colhidos. Tal atividade necessita seguir uma metodologia bem definida para garantia de um resultado eficaz e oportuno. A figura 2.1 apresenta as fases dessa metodologia.

Assim como a Inteligência, o conceito de **Ameaça** pode possuir diversas definições conforme o contexto a que é exposto. Definiremos Ameaça como sendo o agente capaz de gerar um incidente e comprometer os ativos por meio da exploração de vulnerabilidades.

Desta forma, chega-se ao termo **Inteligência de Ameaças**. O National Institute of Standards and Technology (NIST) traz a definição de Inteligência de Ameaça como sendo "toda informação sobre uma ameaça que foi agregada, transformada, analisada, interpretada ou enriquecida para prover o contexto necessário para os processos de tomada de decisão".(tradução nossa)[2]

2.1.2 CTI

Restringindo o escopo de análise para o ambiente cibernético, pode se definir Cyber Threat Intelligence - CTI (Inteligência de Ameaças Cibernéticas) como sendo todo conhecimento sobre o que seus adversários fazem e o uso desse conhecimento para subsidiar a tomada de decisões[3]. Outra definição para CTI é apresentada por Friedman et Bouchard (2015, p. 6) como sendo o “Conhecimento sobre adversários e suas motivações, intenções e métodos que são coletados analisados e disseminados por meios que auxiliam as equipes

de segurança de todos os níveis a protegerem os ativos críticos da empresa."[4]

Segundo a SYNNEX WESTCON-COMSTOR [5], CTI refere-se à área da segurança cibernética focada na análise e coleta de informações relativas a ataques cibernéticos recentes e potenciais que ameaçam a segurança de uma organização ou de seus ativos. As informações necessárias podem ser coletadas em uma comunidade global que se utiliza de protocolos pré-estabelecidos para um compartilhamento eficiente. SILVA (2020, p. 9) nos traz que "Pode ser considerada uma inteligência acionável gerada com base em evidências de mecanismos, indicadores, implicações e contextos relativos a ameaças ou incidentes no domínio cibernético. Fornece conhecimento sobre adversários e métodos que podem auxiliar no processo de tomada de decisão de resposta a ameaças"[6]. Tal definição mostra-se mais completa para o presente trabalho.

O objetivo principal da CTI é, de fato, proporcionar um conhecimento prévio e avançado das ameaças e seus propagadores, ou até mesmo identificar padrões já conhecidos por ataques sofridos. Nos níveis tático e operacional, a CTI otimiza a prévia detecção de um comportamento malicioso, preferencialmente antes que a ameaça venha a se concretizar. No nível estratégico, a CTI provê insights de ameaças relevantes para os tomadores de decisão. [7]

Para que o resultado proposto possa ser alcançado, padrões e boas práticas foram propostos aos longo dos anos. No presente trabalho focaremos na plataforma MISP e seus padrões utilizados para encaminhamento e compartilhamento dos dados buscados.

2.1.3 MISP

MISP-PROJECT[8]

O CERT.br descreve o MISP tanto como uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças, quanto um conjunto de padrões abertos para o compartilhamento dessas informações[9]. A utilização de padrões específicos é de extrema importância para integração e compartilhamento de informações entre diversos atores do cenário de segurança e inteligência cibernética.

De acordo com o site do projeto **MISP**[10], a plataforma de compartilhamento de ameaças MISP (Malware Information Sharing Platform) é um software free e open source que auxilia no compartilhamento de informações de inteligência de ameaças incluindo indicadores de cibersegurança. Uma plataforma de reunião, compartilhamento, armazenamento e correlacionamento de indicadores de comprometimento de ataques direcionados, inteligência de ameaças, informações de fraudes financeiras, informações de vulnerabilidade ou até mesmo de contra-terrorismo. Mas não apenas um software, mas também uma série de modelos de dados criados pela comunidade MISP. O MISP inclui um formato de compartilhamento de informações simples e prático expresso em JSON que pode ser usado com o software MISP ou por qualquer outro software. Os formatos MISP agora são padrões tratados pelo MISP-STANDARD.ORG (https://www.misp-standard.org).

MISP-STANDARD[11]

O padrão MISP é um padrão de inteligência colaborativa, potencializando a inteligência e a troca, compartilhamento e modelagem de informações. O misp-standard.org é um órgão de padrões que desenvolve padrões livres e abertos por meio de colaboração sã de código aberto.

O formato principal do MISP é um formato JSON simples usado pelo MISP e outras ferramentas para trocar eventos e atributos. O esquema JSON 2.4 é descrito no software principal MISP e muitos arquivos de amostra estão disponíveis no feed OSINT.

O formato MISP é descrito como Internet-Draft[1] em MISP-RFC[2], e é descrito para oferecer suporte ao desenvolvedor ou organização que deseja construir sua própria ferramenta de suporte ao formato MISP (como importação ou exportação). O padrão é construído a partir de casos de uso práticos e referências de implementação dentro do

[1]Por definição, um Internet-Draft é um documento de curta duração, geralmente produzido pelos grupos de trabalho da IETF, mas também divulgado por outros. Eles são trabalhos em andamento e, a menos que sejam atualizados, são removidos do arquivo de Rascunhos da Internet seis meses após sua publicação. Embora alguns eventualmente se tornem RFCs e sigam o formato RFC geral, os rascunhos da Internet não devem ser considerados fontes oficiais. Para ler os rascunhos atuais da Internet ou para encontrar mais informações, visite a página de Rascunhos da IETF na Internet em: http://www.ietf.org/ID.html

[2]Os **Requests for Comments** (RFC) são de natureza mais formal e permanente do que os Internet Draft. Depois que um RFC recebe um número e é distribuído, ele nunca pode ser alterado. Se uma revisão for necessária, um novo RFC é lançado, tornando-o obsoleto ou ampliando o documento original. Nem todas as RFCs necessariamente descrevem um padrão ou são até mesmo uma trilha padrão. Alguns são informativos ou descrevem tecnologias desenvolvidas por fornecedores que não passaram pela IETF. Todos os RFCs, entretanto, são publicados pelo Editor de RFC. Para obter mais informações sobre RFCs, bem como links para espelhos de arquivo RFC, visite a página do Editor RFC em: http://www.rfc-editor.org/

projeto MISP. O padrão está evoluindo rapidamente após a implementação do MISP.

MISP core format

Trata-se de um documento que descreve o formato principal do MISP usado para troca de indicadores e informações sobre ameaças entre as instâncias do MISP. O formato JSON inclui a estrutura geral junto com a semântica associada a cada chave respectiva. Tal formato é descrito para suportar outras implementações, visando reutilizar o formato e garantindo a interoperabilidade com o software MISP existente e outras Plataformas de Inteligência de Ameaças.

MISP object template format

Documento que descreve o formato do modelo de objeto MISP, um formato JSON simples para representar os vários modelos usados para construir objetos MISP. Um diretório público de modelos de objeto MISP comuns está disponível e depende do formato de referência de objeto MISP.

MISP taxonomy format

Documento que descreve o formato de taxonomia MISP, um formato JSON simples para representar vocabulários de tag de máquina (também chamada de tag tripla). Um diretório público de vocabulários comuns chamado taxonomias MISP está disponível e depende do formato de taxonomia MISP. Taxonomias MISP são usadas para classificar eventos de segurança cibernética, ameaças, eventos suspeitos ou indicadores .

MISP galaxy format

Documento que descreve o formato de galáxias MISP, um formato JSON simples para representar galáxias e aglomerados que podem ser anexados a eventos ou atributos MISP. Um diretório público de galáxias MISP está disponível e depende do formato de galáxias MISP. Galáxias MISP são usadas para anexar estruturas de informações adicionais, como eventos ou atributos MISP. MISP galaxy é um repositório público de malware conhecido, agentes de ameaças e várias outras coleções de dados que podem ser usados para marcar, classificar ou rotular dados no compartilhamento de informações de ameaças.

Sighting DB format

Documento que descreve o formato usado pelo SightingDB para fornecer contexto automatizado a um determinado Atributo, contando ocorrências e rastreando os tempos de observabilidade. SightingDB foi projetado para fornecer ao MISP e outras ferramentas uma maneira interoperável, escalonável e rápida de armazenar e recuperar visões de atri-

butos.

2.1.4 Enriquecimento

O que é Enriquecimento?

Segundo o site da LGPDBrasil[12], enriquecimento de bases de dados, de forma simples, é a captação de informações que a empresa ainda não tem em sua base para complementar um banco de dados existente. Por exemplo: a empresa tem o nome e o CPF, mas deseja enriquecer o seu banco de dados com o telefone de contato do cliente/consumidor. No contexto do presente trabalho, o enriquecimento de dados se refere ao processo de anexar ou de outra forma aprimorar os dados coletados com o contexto relevante obtido de fontes adicionais acerca de uma ameaça.[13]

As equipes de segurança agora têm uma ampla variedade de fontes de inteligência contra ameaças alimentadas com indicadores de comprometimento. No entanto, saber um endereço IP ou nome de domínio é apenas o primeiro passo para evitar uma ameaça ou responder a ela. Enriquecer o contexto em torno das IOCs aumenta drasticamente seu valor para os analistas.

Por que Enriquecer?

O enriquecimento da inteligência contra ameaças é um componente crítico de qualquer processo de investigação de incidentes ou ameaças. O processo de enriquecimento ajuda a remover falsos positivos e deduzir inteligência acionável para resposta a ameaças e outras operações de segurança.

Como se insere o enriquecimento no ciclo de inteligência?

Dentro do ciclo de produção de inteligência (Figura 2.1), o enriquecimento está inserido na fase de Reunião/coleta de dados. No entanto, nada impede que ao se chegar na fase de formalização se possa regressar à reunião para novo enriquecimento.

2.2 Síntese

No presente capítulo foram apresentados os principais conceitos relacionados ao tema do trabalho. Tais conceitos envolvem Inteligência e as fases de produção, Ameaças, Inteligência de Amaeças e CTI. Procurou-se também explanar sobre a plataforma e padrões MISP e seus formatos e ainda sobre Enriquecimento de dados.

Capítulo 3

Implementação da Integração

A proposta do projeto é de uma ferramenta modular, onde a mesma se conecta tanto com outras feramentas existentes bem como com a plataforma MISP. As respectivas arquiteturas são apresentadas e explanadas nas subseções que se seguem.

3.1 Ferramenta de Enriquecimento

A ferramenta proposta foi desenvolvida em Python, de forma moduarizada, com uso de algumas bibliotecas, dentre elas a PyMISP[1] que é uma biblioteca Python para acesso a plataformas MISP via REST API. Tal biblioteca permite a busca de eventos, adição ou atualização de eventos/atributos, adição ou atualização de amostras ou pesquisa de atributos.

Além disso, foram utilizadas ferramentas de terceiros, todas Open Source ou com versões para uso gratuito. Todas as ferramentas são chamadas por funções criadas dentro do Enricher e tratadas para envio à plataforma MISP criada especificamente para este trabalho.

Devido a modularidade da ferramenta, é possível a utlização da mesma com retorno das informações na tela sem a necessidade de instalação de uma plataforma MISP. No entanto esta forma de implementação não será tratada no presente projeto por fugir do escopo do mesmo.

A idéia principal do programa consiste nos seguintes passos:

[1](https://www.circl.lu/doc/misp/pymisp/)

- Iniciado o programa (***enricher()***) , o usuário opta por um dos tipos de busca disponibilizados, a saber: *IP*, *Domain* ou *Email*;
- O programa solicitará o parâmetro do alvo e fará uma validação inicial.
- Feita a validação, o programa fará a primeira conexão com a plataforma MISP para verificar se o parâmetro informado consta da base.
  - Caso o evento **NÃO EXISTA**, o programa criará um novo evento com o parâmetro informado e enviará para a plataforma recuperando o $event_id$ para tratamento futuro.
  - Caso o evento **EXISTA**, a plataforma retornará para a ferramenta as informações disponíveis, bem como o $event_id$ do evento.
- 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.
- a busca por email gerará também uma busca pelo nome de usuário em sites e rede conhecidas.
- finalizada a busca o programa fará nova conexão com a plataforma, atualizando as informações do evento com os dados encontrados.
- 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.

A figura 3.1 apresenta o fluxograma da implementação.

3.1.1 Arquitetura da Ferramenta

A figura 3.2 apresenta a arquitetura da ferramenta proposta, onde é possível identificar as funções específicas do programa, os momentos de acesso à plataforma implementada e as chamadas das ferramentas de terceiros integradas.

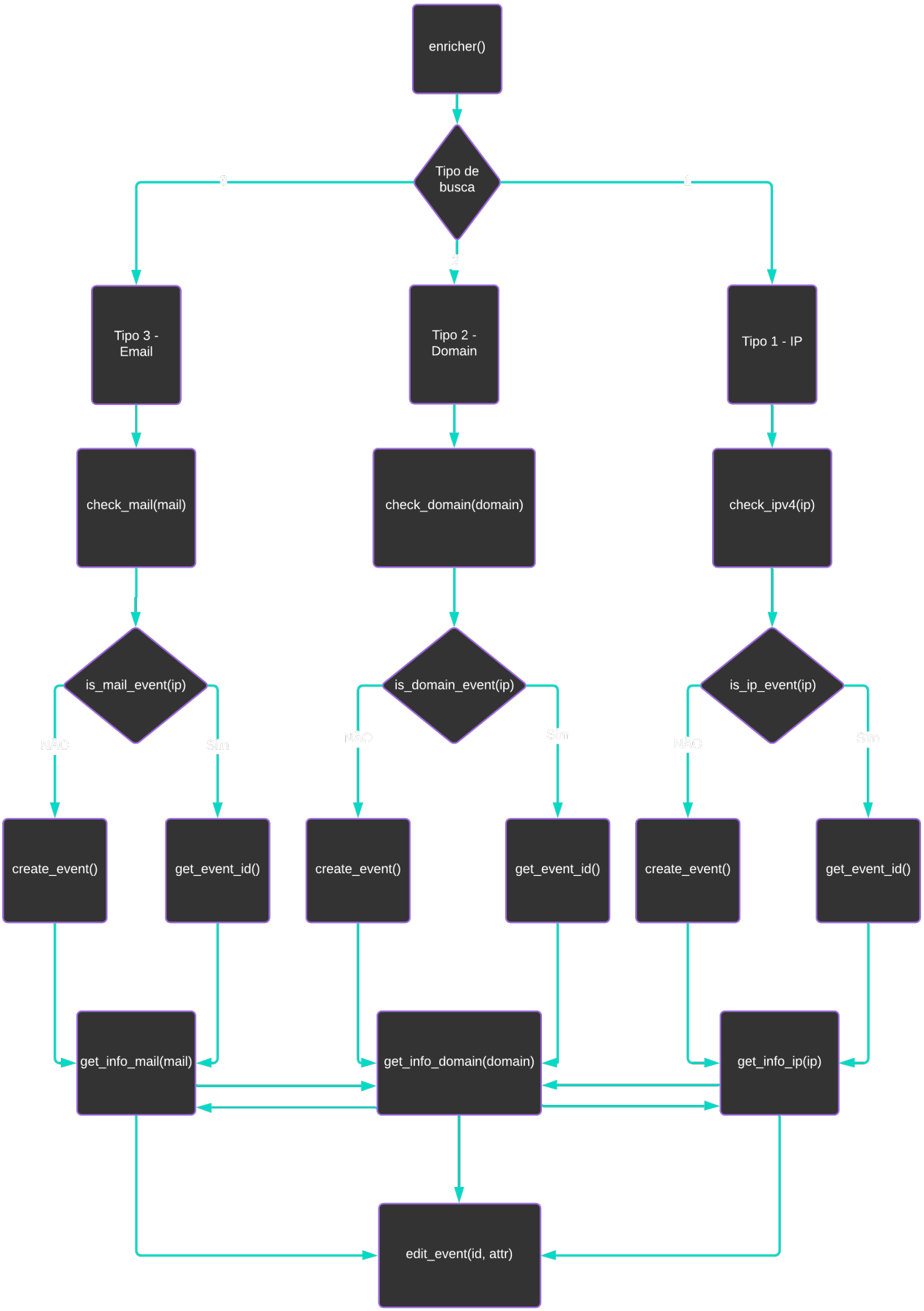

Figura 3.1: Fluxograma da implementação

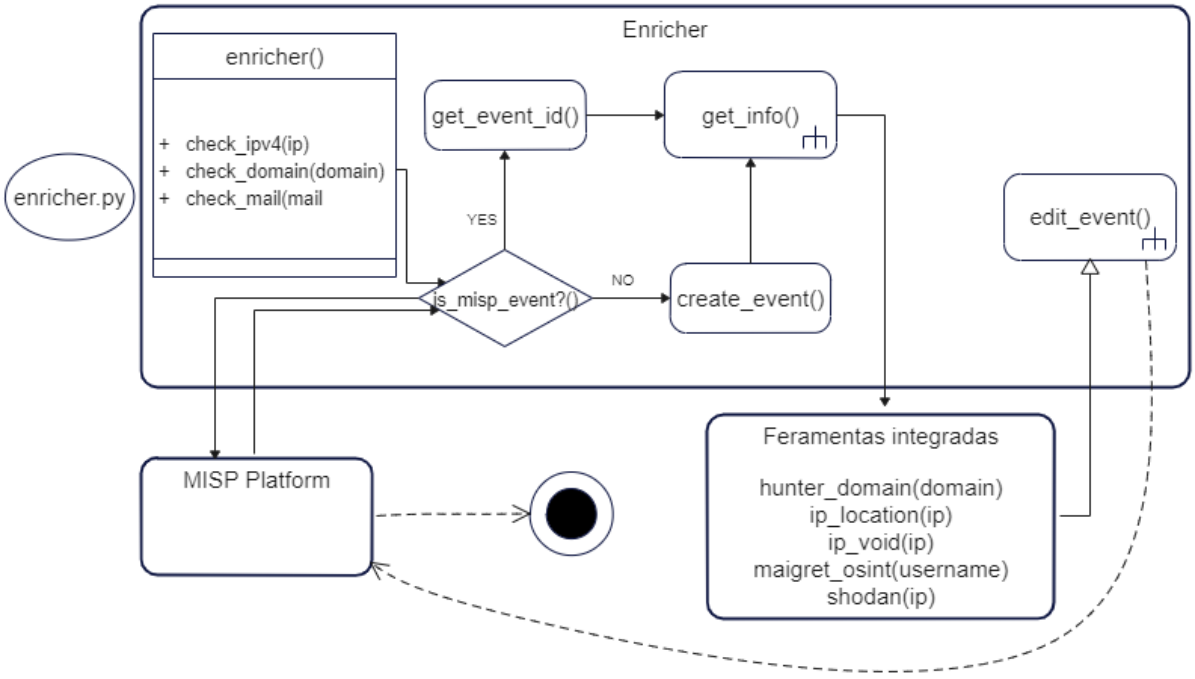

Figura 3.2: Arquitetura da Ferramenta proposta

3.2 Plataforma MISP

Para a execução do presente projeto foi necessário realizar a instalação de uma Plataforma MISP. Os passos para instalação e configuração foram seguidos da página do projeto https://misp.github.io/MISP/.

A plataforma foi instalada e configurada em uma VM Ubuntu 20.04 LTS na Google Cloud.

Para integração com a ferramenta *Enricher*, os requisitos necessários foram supridos com a utilização da biblioteca PYMISP.

A figura 3.4 mostra a arquitetura entre a ferramenta Enricher e a plataforma MISP. Na arquitetura é possível perceber quais funções são as responsáveis pela conexão com a plataforma, sendo elas:

- check_domain() - que se conecta com a plataforma pelas funções
  - is_domain_event() - Busca pelo evento.
  - get_event_id() - retorna o ID do evento (caso seja encontrado ou quando criado).

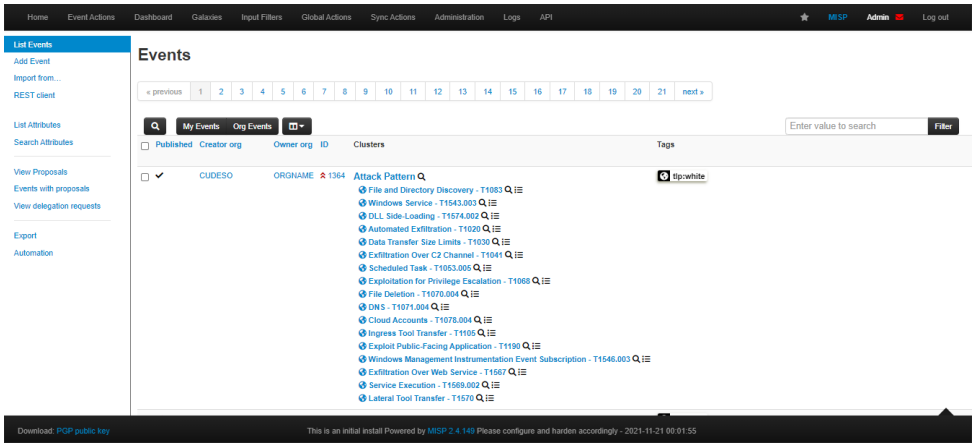

Figura 3.3: Tela inicial da plataforma MISP instalada

  - create_event() - cria o evento.
  - edit_event() - envia os dados da ferramenta para a plataforma.

- check_ipv4() - que se conecta com a plataforma pelas funções
  - is_ip_event() - Busca pelo evento.
  - get_event_id() - retorna o ID do evento (caso seja encontrado ou quando criado).
  - create_event() - cria o evento.
  - edit_event() - envia os dados da ferramenta para a plataforma.

- check_mail() - que se conecta com a plataforma pelas funções
  - is_mail_event() - Busca pelo evento.
  - get_event_id() - retorna o ID do evento (caso seja encontrado ou quando criado).
  - create_event() - cria o evento.
  - edit_event() - envia os dados da ferramenta para a plataforma.

3.2.1 PYMISP

PyMISP é uma biblioteca Python para acesso a plataformas MISP por meio de sua API REST, distribuída sob licença Open Source. Ela permite que se busque eventos,

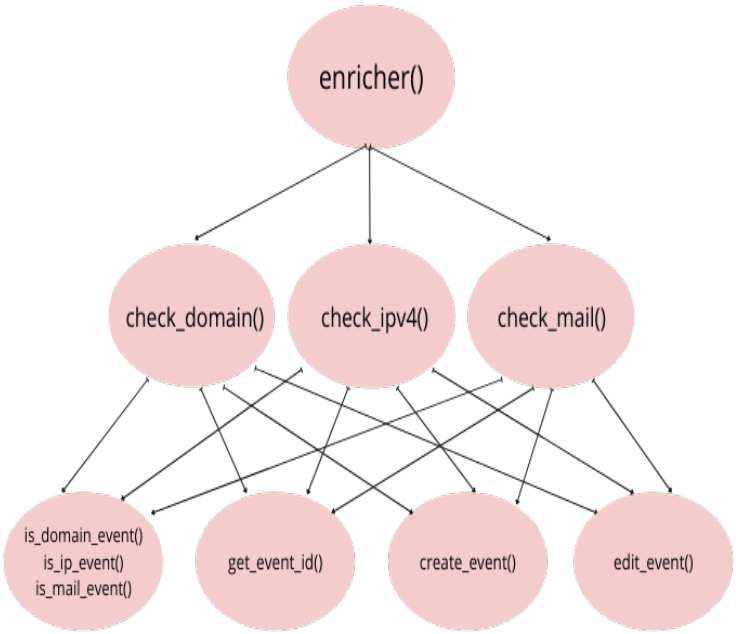

Figura 3.4: Arquitetura entre a Ferramenta Enricher e a plataforma MISP

adicione ou atualize eventos/atributos, adicione ou atualize amostras ou pesquise atributos. Sua documentação pode ser consultada em https://pymisp.readthedocs.io/en/latest/

3.3 Ferramentas integradas

A ferramenta proposta se conecta, para algumas coletas, à ferramentas de terceiros existentes e com licença Open Source ou versão gratuita, o que auxilia em um retorno de resultados mais amplo. Tais ferramentas são as que se seguem:

- Hunter - Busca de emails por domínio - (https://hunter.io/)
  A ferramenta Hunter fornece uma busca por emails vinculados a um domínio específico.
- Maigret OSINT
  A ferramenta Maigret OSINT traz informações sobre pessoas com base no username,

buscando em mais de 500 sites e web pages as existentes com o username relacionado - https://github.com/soxoj/maigret

- IP-Location
  IP-Location é uma API que provê geolocation de um IP - (https://api.iplocation.net/)

- IP-Void IP-Void é uma API que busca a reputação de um determinado IP. (https://www.ipvoid.com

A figura 3.5 apresenta a arquitetura existente entre a Ferramenta Enricher e as ferramentas de terceiros. Na arquitetura é possível perceber quais funções são as responsáveis pela conexão com as ferramentas, sendo elas:

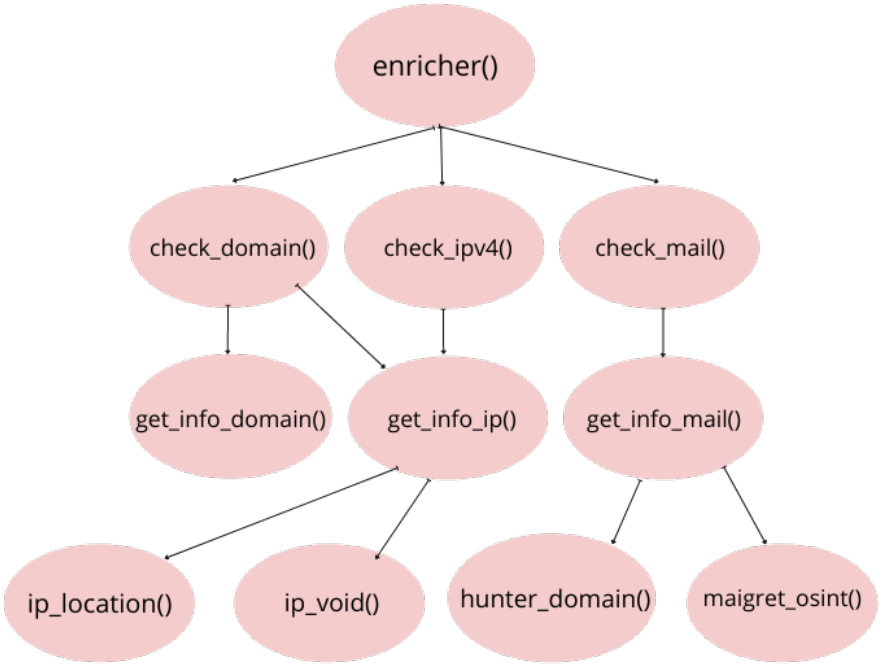

Figura 3.5: Arquitetura entre a Ferramenta Enricher e as Ferramentas de terceiros

- get_info_ip() - que se conecta com as ferramentas pelas funções
  - ip_location()
  - ip_void()

- get_info_mail() - que se conecta com as ferramentas pelas funções
  - hunter_domain().
  - maigret_osint().

3.4 Síntese

No presente capítulo foram apresentados os aspectos da implementação da ferramenta *Enricher*, a arquitetura da ferramenta e seu fluxograma. Foram também apresentadas as configurações da plataforma MISP e a biblioteca PYMISP, com a qual se tornou possível a comunicação da ferramenta com a plataforma. Arquitetura entre a ferramenta *Enricher* e a plataforma foi apresenta na Figura 3.4.

Por fim foram apresentadas as ferramentas de terceiros que se integraram ao projeto para realização das buscas de dados e retorno ao *Enricher*. A arquitetura entre esta e as ferramentas integradas foi apresentada na 3.5.

Capítulo 4

Testes, Resultados e Discussões

Para a avaliação da presente ferramenta foram propostos alguns casos de teste, os quais serão apresentados juntamente com seus resultados e discussões. Os testes realizados foram:

- Teste 1 - Evento de IP inexistente na plataforma MISP
- Teste 2 - Evento de IP existente na plataforma MISP
- Teste 3 - Evento de Domínio inexistente na plataforma MISP
- Teste 4 - Evento de E-mail inexistente na plataforma MISP

4.1 Teste 1 - Evento de IP inexistente na plataforma MISP

Este teste tem como objetivos principais verificar as funcionalidades do Enricher de **busca** e **criação** de eventos na plataforma MISP. Para isso foi realizada uma busca com base no endereço IP (162.241.203.131) (Figura 4.1).

Espera-se como comportamento da ferramenta que seja apresentada, após a busca, a mensagem "*Evento não consta como ORIGEM! Criar evento para IP de origem?*". Após selecionar a opção **1** deve ser apresentada a mensagem "*Informe a descrição do evento:*". Por fim o evento deve ser criado na plataforma MISP.

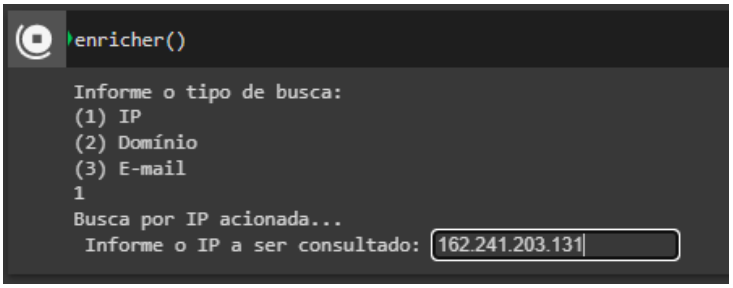

Figura 4.1: Início da ferramenta Enricher

No momento da busca o evento relativo a tal parâmetro não constava da plataforma, conforme se verifica na Figura 4.2.

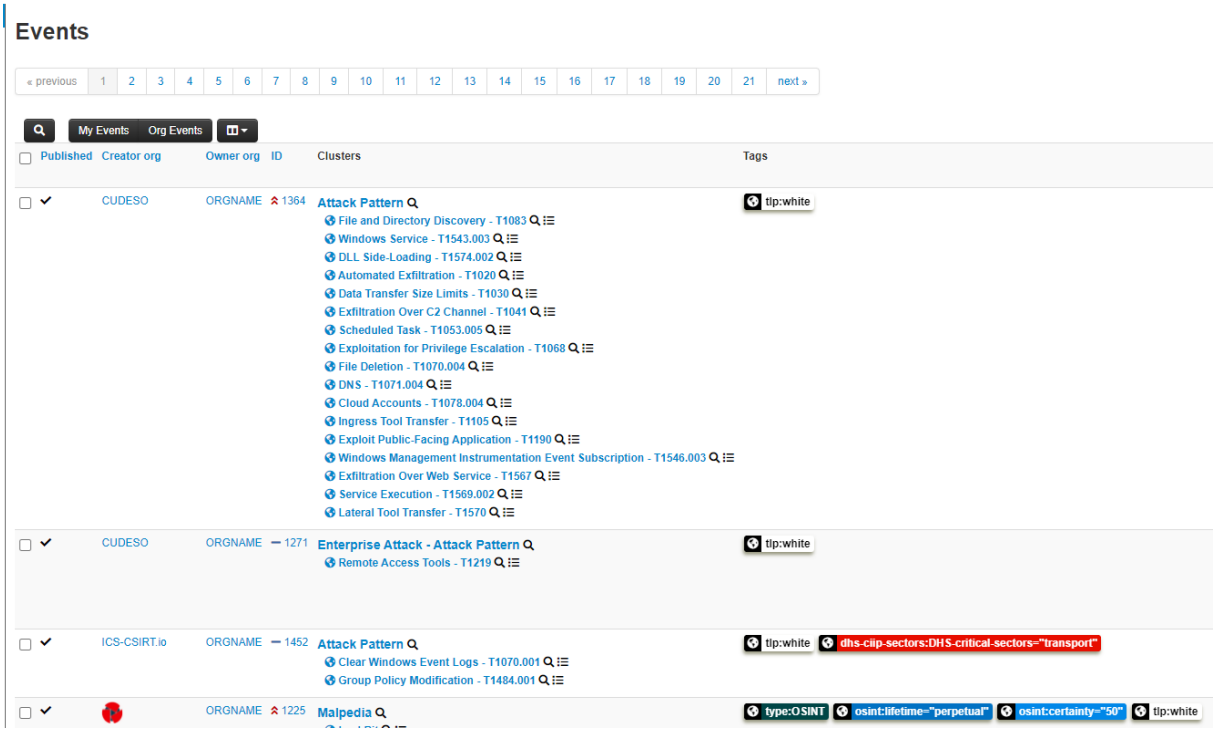

Figura 4.2: Eventos existentes na plataforma MISP

Após a realização da busca o evento foi criado com as informações inseridas conforme a Figura 4.3 e pôde ser visualizado na plataforma MISP (Figura 4.4), conforme era esperado.

As informações obtidas com base nas buscas feitas pela ferramenta são visualizadas na plataforma marcadas de laranja (Figura 4.5) como propostas de enriquecimento. O analista nesse momento deve selecionar as que desejar e aceitar as propostas ou não (Figura 4.6).

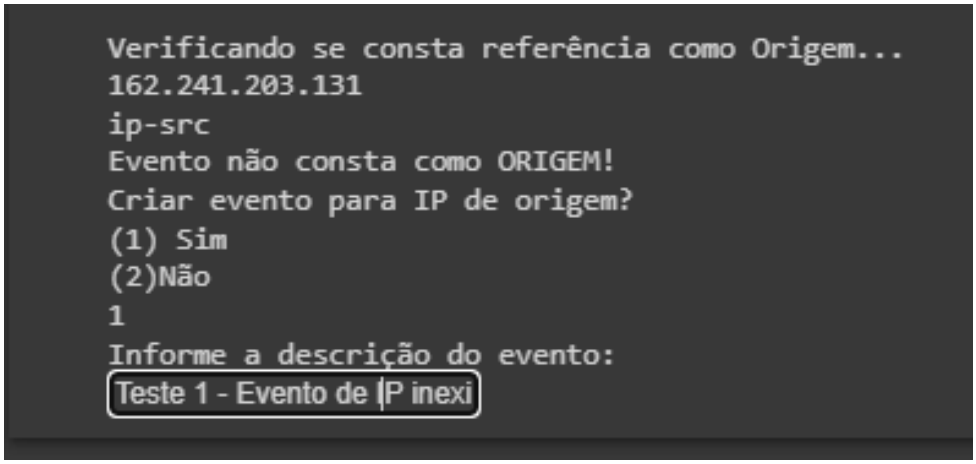

Figura 4.3: Criação do evento via ferramenta Enricher

Figura 4.4: Evento criado na plataforma MISP

Neste Teste foi possível verificar que o funcionamento da ferramenta para busca e criação de eventos na plataforma se deu de forma adequada. As buscas nas bases externas (OSINT) também retornou resultado satisfatório, trazendo informações de registro relativas ao IP informado.

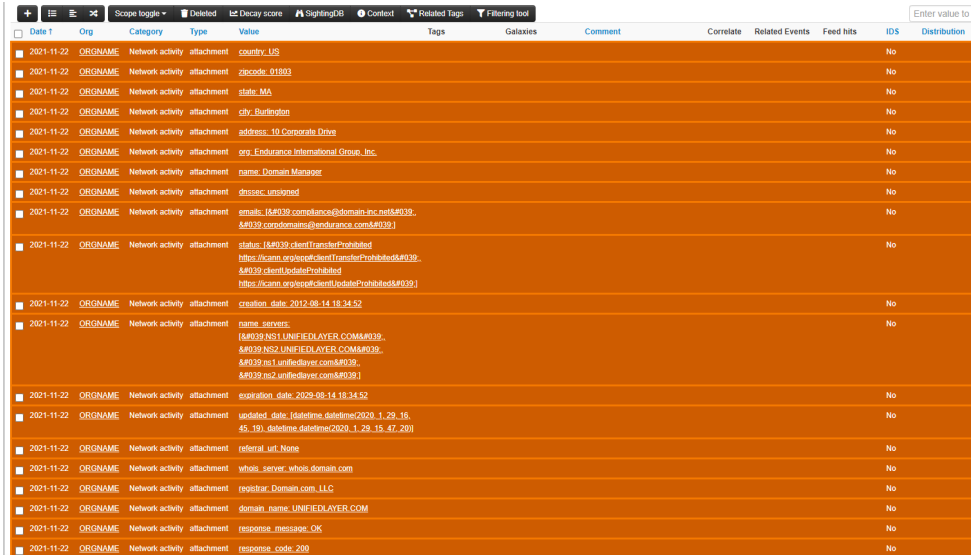

Figura 4.5: Informações coletadas enviadas à plataforma

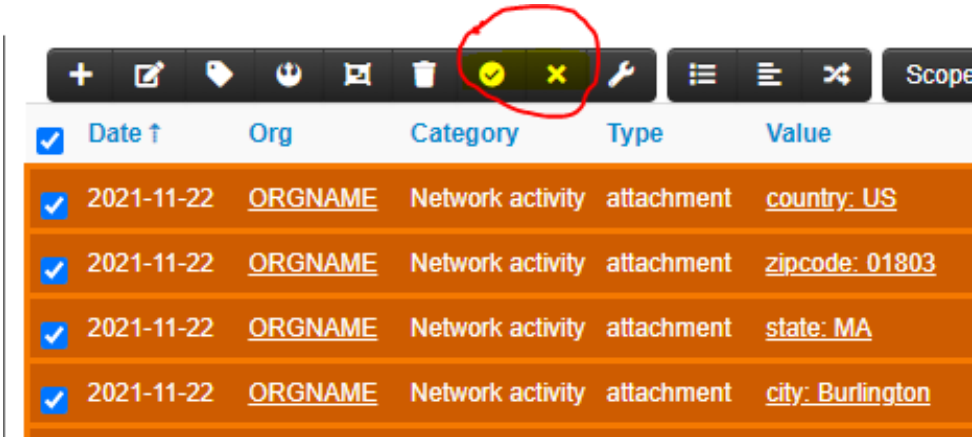

Figura 4.6: Confirmação ou exclusão de proposta

4.2 Teste 2 - Evento de IP existente na plataforma MISP

Este teste tem como objetivos principais verificar as funcionalidades do Enricher de **busca** e **edição** de eventos na plataforma MISP. Para isso foi realizada uma busca com base no endereço IP (144.217.81.160).

Espera-se como comportamento da ferramenta que NÃO seja apresentada, após a busca, nenhuma mensagem, pois o evento exite na plataforma. Adicionalmente, após as buscas sobre o parâmetro relativo, o evento existente na plataforma MISP deve ser editado com os novos dados recebidos como propostas.

Foi realizada a busca com base no endereço IP desejado. Como informado, no momento da busca o evento relativo a tal parâmetro **constava** na plataforma, conforme se verifica na Figura 4.7.

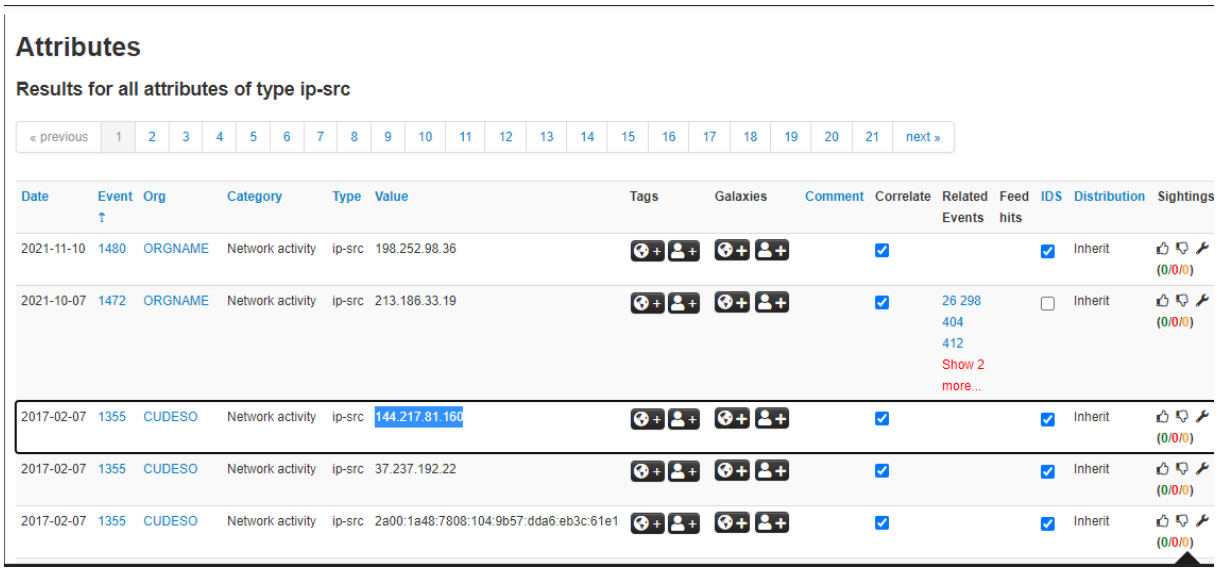

Figura 4.7: Lista de eventos com evento existente

Os atributos existentes no evento antes da execução da ferramenta são mostrados na Figura 4.8, onde é possível observar que apenas 1 (um) dos atributos ali existentes necessita de confirmação ou exclusão.

Após a realização da busca o evento foi atualizado e pôde ser visualizado na plataforma MISP com os novos atributos inseridos, a serem confirmados ou excluídos (Figura 4.9).

Neste Teste foi possível verificar que o funcionamento da ferramenta para busca e **edição** de eventos na plataforma se deu de forma adequada, sendo encontrado o evento e editado com novas informações, como era esperado.

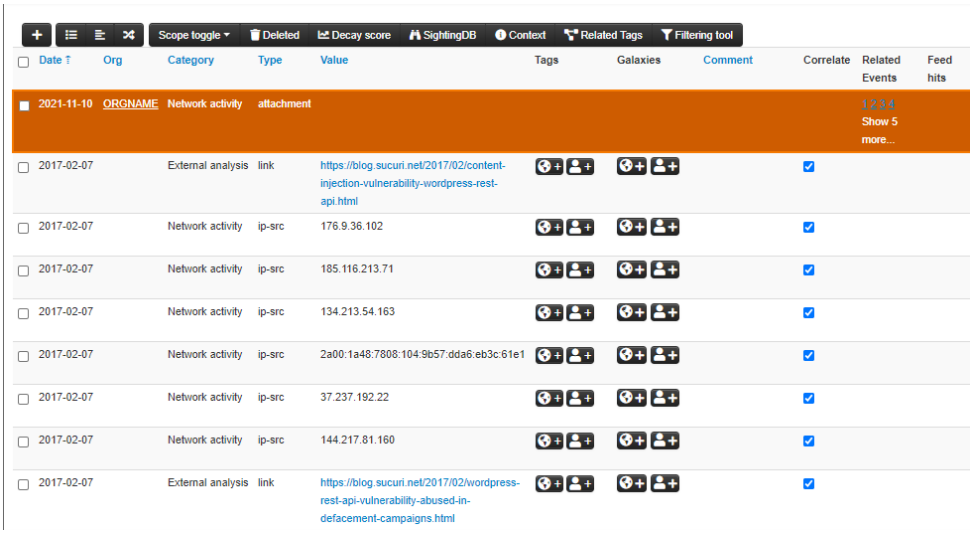

Figura 4.8: Atributos existentes do evento em referência

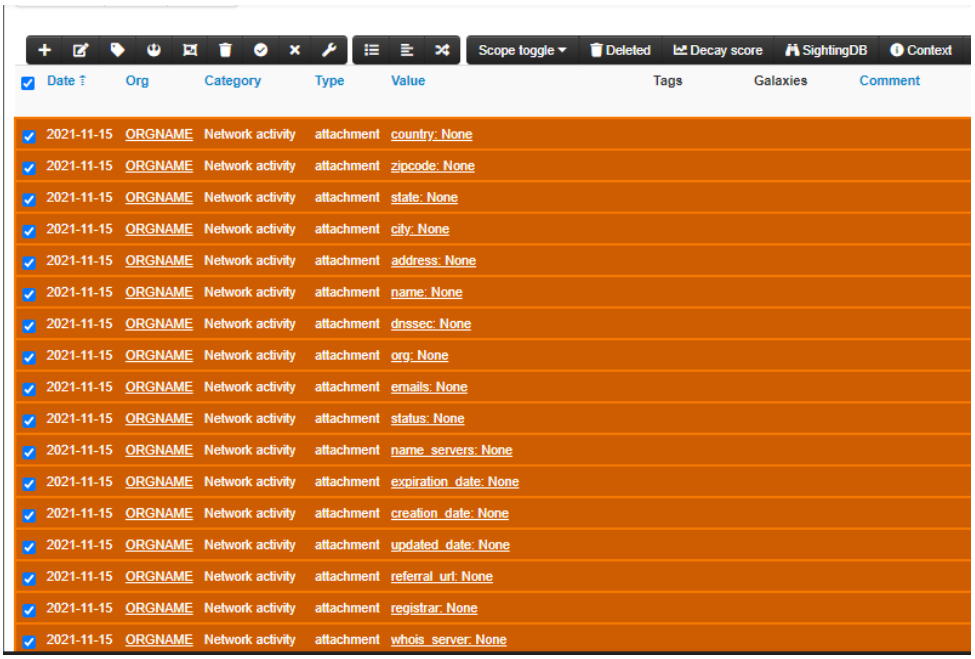

Figura 4.9: Atributos inseridos no evento em referência

4.3 Teste 3 - Evento de Domínio inexistente na plataforma MISP

Este teste tem como objetivos principais verificar as funcionalidades do Enricher de

busca e **criação** de eventos na plataforma MISP tendo como parâmetro um **Domínio**.

Espera-se como comportamento da ferramenta que seja apresentada, após a busca, a mensagem *"Não consta registro do evento. Criar evento para o Domínio?"*. Após ser selecionada a opção **1** deve ser apresentada a mensagem "*Informe a descrição do evento:*". Por fim o evento deve ser criado na plataforma MISP e apresentada a mensagem *"BUSCANDO INFORMAÇÕES OSINT FRAMEWORK..."*.

Foi realizada a busca com base no Domínio **"enigmaker.com.br"**, inexistente na plataforma. No momento da busca o evento relativo a tal parâmetro não constava da mesma. Após a realização da busca o evento foi criado com as informações inseridas e pôde ser visualizado na plataforma MISP (Figura 4.10).

Figura 4.10: Evento criado na plataforma MISP

As informações obtidas com base nas buscas feitas pela ferramenta são visualizadas na plataforma marcadas de laranja (Figura 4.11) como propostas de enriquecimento.

Neste Teste foi possível verificar que o funcionamento da ferramenta para busca e criação de eventos na plataforma com base em um **Domínio** se deu de forma adequada, sendo criado o evento após a busca inicial não ter encontrado referência ao mesmo na plataforma MISP e ainda editado com novas informações, como era esperado.As buscas nas bases externas (OSINT) também retornou resultado satisfatório, trazendo informações de

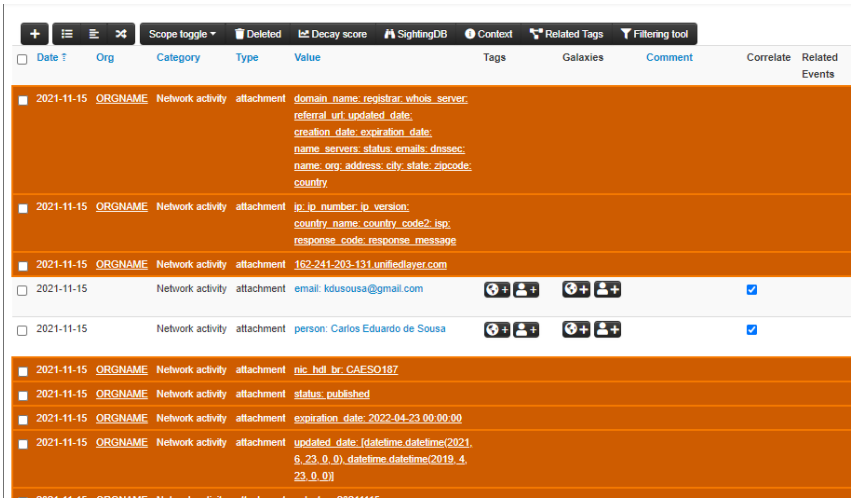

Figura 4.11: Informações coletadas enviadas à plataforma

registro relativas ao IP referente ao domínio informado.

4.4 Teste 4 - Evento de E-mail inexistente na plataforma MISP

Este teste tem como objetivos principais verificar as funcionalidades do Enricher de **busca** e **criação** de eventos na plataforma MISP tendo como parâmetro um **Email**.

Espera-se como comportamento da ferramenta que seja apresentada, após a busca, a mensagem *"Não foram localizados eventos para o e-mail informado. Deseja criar um novo evento?"*. Após ser selecionada a opção **1** deve ser apresentada a mensagem "*Informe a descrição do evento:*". Por fim o evento deve ser criado na plataforma MISP e apresentada a mensagem *"BUSCANDO INFORMAÇÕES OSINT FRAMEWORK..."*.

Foi realizada a busca com base no Email inexistente na plataforma **cyar-project@gmail.com**. No momento da busca o evento relativo a tal parâmetro não constava da plataforma. Após a realização da busca o evento foi criado com as informações inseridas (Figura 4.12) e pôde ser visualizado na plataforma MISP (Figura 4.13).

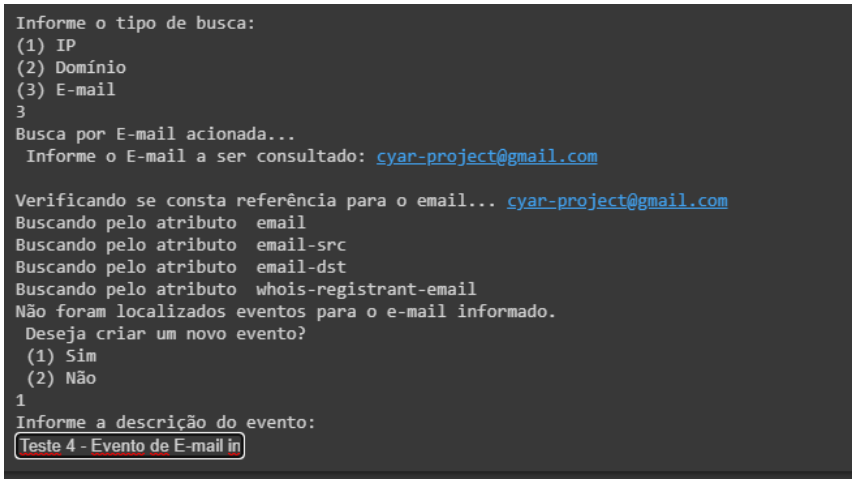

Figura 4.12: Criação do evento pela ferramenta

Figura 4.13: Evento criado na plataforma MISP

As informações obtidas com base nas buscas feitas pela ferramenta são visualizadas na plataforma marcadas de laranja (Figura 4.14) como propostas de enriquecimento.

Neste Teste foi possível verificar que o funcionamento da ferramenta para busca e criação de eventos na plataforma com base em um **Email** se deu de forma adequada, tendo sido criado o evento após nada ter sido encontrado na Plaaforma referente ao parâmetro. As buscas nas bases externas (OSINT) também retornaram resultados satisfatórios, trazendo informações relativas ao Username referente ao email informado e editadas na

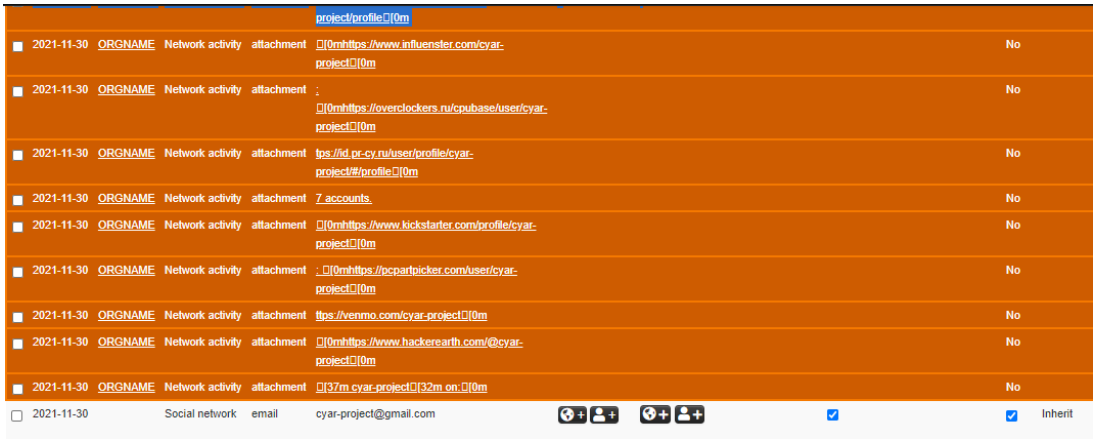

Figura 4.14: Informações coletadas enviadas à plataforma

plataforma MISP.

4.5 Síntese

Neste capítulo foram realizados testes de utilização da ferramenta para verificação e validação de suas funcionalidades, quais sejam, busca, criação e edição de eventos, busca e retorno de dados para enriquecimento.

No Teste 1 buscou-se por um evento com o parâmetro IP inexistente na plataforma. Como esperado o evento não foi encontrado e solicitou-se ao usuário decidir pela criação, informando a descrição do mesmo. O evento foi criado e em seguida enriquecido com dados buscados.

No Teste 2 a busca foi por um IP existente na plataforma, o qual foi encontrado e em seguida enriquecido como era esperado. Os dados foram enviados à plataforma e adicionados como *proposes* (propostas), para que o analista possa decidir qual informação é relevante.

O Teste 3 apresenta uma busca por Domínio inexistente na plataforma. Como esperado a ferramenta não encontrou evento relacionado ao parâmetro e solicitou a decisão do usuário pela criação ou não do evento. Após a opção pela criação o evento foi criado e enriquecido pela ferramenta.

Por fim, no Teste 4, foi feita uma busca pelo parâmetro Email por um evento inexistente no MISP. Novamente o evento não foi encontrado, sendo criado na plataforma e realizado o enriquecimento com base no username. Foi feita também uma busca pelo domínio relacionado ao Email.

Todos os testes apresentaram resultados satisfatórios, com retorno de informações relevantes ao enriquecimento dos parâmetros inseridos.

Capítulo 5

Considerações Finais

Neste projeto foi proposta uma ferramenta integrada com a plataforma MISP para enriquecimento de Inteligência de ameaças cibernéticas. A funcionalidade da ferramenta, feita em Python, consistia em se conectar com a plataforma MISP e realizar buscas de informações sobre alvos específicos.

Na fase de planejamento do projeto, desejava-se realizar algumas implementações, tais como indexação de relatórios de incidentes baseados em IPs para correlacionamento com a base. Infelizmente limitações surgiram impossibilitando tal implementação neste projeto.No entanto, devido a modularidade da ferramenta, é possível e viável que se realize no futuro.

Outro fato a observar para ajustes futuros refere-se ao ajuste dos atributos recebidos para comparação com existentes e remoção automática das redundâncias. Existe, ainda, a possibilidade de utilização da ferramenta de modo separado da plataforma MISP (standalone), de forma que possa atender a necessidades diversas.

O projeto foi apresentado como Prova de conceito, sendo que a ferramenta demosntrou resultados satisfatórios. Durante a criação do trabalho surgiu uma necessidade real de uso na qual foi utilizada a ferramenta e retornado um resultado extremamente útil para a situação apresentada.

Em linhas gerais, a ferramenta proposta demosntrou funcionamento adequado, com resultados reais úteis e oportunos, proporcionando a analistas de segurança cibernética e até mesmo analistas de inteligência auxílio na busca pelo enriquecimento dos dados disponíveis.

Referências

[1] CTI, Accenture: *Cyber threat intelligence report.* https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence, 2021. Acessado em 18-08-2021. 1

[2] Chris Johnson, Larry Feldman e Greg Witte: *Cyber-threat intelligence and information sharing.* https://tsapps.nist.gov/publication/get$_p df.cfm?pub_i d$ = 923332, 2021. $Acessadoem 17-08-2021$. 4

[3] ATTCK, MITTRE: *Getting started with attck: Threat intelligence.* https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f, 2021. Acessado em 18-08-2021. 4

[4] Friedman, Jon e Mark Bouchard: *Defnitive Guide to Cyber Threat Intelligence.* CyberEdge Group, LLC, MD, USA, 2015. 5

[5] WESTCON-COMSTOR, SYNNEX: *InteligÊncia de ameaÇas cibernÉticas: O que É e qual a importÂncia para empresas?* http://digital.br.synnex.com/pt/inteligencia-de-ameacas-ciberneticas, 2021. Acessado em 29-09-2021. 5

[6] SILVA, ALESSANDRA DE MELO E: *Metodologia integrativa para produÇÃo de inteligÊncia de ameaÇas cibernÉticas utilizando plataformas de cÓdigo aberto.* 2020. 5

[7] Oosthoek, Kris e Christian Doerr: *Cyber threat intelligence: A product without a process?* International Journal of Intelligence and CounterIntelligence, 2020. 5

[8] MISP-PROJECT: *Misp - open source threat intelligence platform open standards for threat information sharing.* https://www.misp-project.org/, 2021. Acessado em 10-09-2021. 5

[9] CERT.br: *Misp cert.br.* https://www.cert.br/misp/, 2021. Acessado em 29-09-2021. 5

[10] MISP-PROJECT: *Misp threat sharing.* https://www.misp-project.org/index.html, 2021. Acessado em 29-09-2021. 6

[11] Standard, MISP: *The collaborative intelligence standard powering intelligence and information exchange, sharing and model.* https://www.misp-standard.org, 2021. Acessado em 10-09-2021. 6

[12] Brasil, LGPD: *Lgpd e o enriquecimento de base de dados.* https://www.lgpdbrasil.com.br/lgpd-e-o-enriquecimento-de-base-de-dados/, 2021. Acessado em 15-09-2021. 8

[13] Knapp, Eric D. e Joel Thomas Langill: *Chapter 11 - exception, anomaly, and threat detection*. Em Knapp, Eric D. e Joel Thomas Langill (editores): *Industrial Network Security (Second Edition)*, páginas 323–350. Syngress, Boston, second edition edição, 2015, ISBN 978-0-12-420114-9. https://www.sciencedirect.com/science/article/pii/B9780124201149000113. 8