ISBN: 978-989-8533-96-8 © 2019 IADIS

PROPOSTA DE MODELO DE REFERÊNCIA DE INTELIGÊNCIA DE AMEAÇAS

Bruce William Percílio Azevedo, William F. Giozza, Fábio Lúcio Lopes de Mendonça, Demétrio Antônio da Silva Filho, Rafael Timóteo de Sousa Júnior e Robson de Oliveira Albuquerque

Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE) - Departamento de Engenharia Elétrica - Universidade de Brasília - Brasília, Brasil - Zipcode 70910-900

RESUMO

Este artigo propõe um modelo de referência para inteligência de ameaças, juntamente com a descrição de uma ferramenta de prova de conceito como resultado das possibilidades do modelo desenvolvido. O modelo proposto agrega todas as funcionalidades relacionadas ao contexto, integrando-as e distribuindo-as em uma estrutura de camadas, apresentando seus objetivos, características e como elas estão interligados. O modelo em questão foi utilizado como base para o desenvolvimento de uma ferramenta com o objetivo de executar a funcionalidade de compartilhamento de dados de maneira segura e gerenciável.

PALAVRAS-CHAVE

Threat Intelligence, Modelo de Referência, Compartilhamento de Informação

1. INTRODUÇÃO

Todos os dias, aumenta o número de pessoas, empresas e nações, que digitalizam suas informações. Esse deslocamento em direção à esfera tecnológica continua subindo em economias emergentes. Porém, em economias mais desenvolvidas, esse padrão já se encontra em taxas elevadas (J. Poushter et al., 2016). Embora essas mudanças gerem ganhos, elas implicam em custos, e um deles é a necessidade de gerenciar e proteger esses dados. Avaliando o atual cenário de segurança cibernética, em que o número de incidentes vem aumentando (S. Samtani, K. Chinn, C. Larson, and H. Chen, 2016), essa tarefa é bastante desafiadora.

Para auxiliar na missão de proteger a infraestrutura vigente, é recomendável analisar a maior quantidade conhecimento disponível e possível de ser coletada por uma entidade ou indivíduo. A Internet, como uma fonte de dados de amplo acesso, é constantemente utilizada como canal para realização de ataques e, em determinados casos, também atua na contenção desses. Contudo, todos os dias uma enorme quantidade de dados é criada e disponibilizada na Internet, sendo humanamente impossível processá-los e analisá-los sem o aporte de ferramentas especializadas.

Nesse sentido, ferramentas de Inteligência de Ameaças - comumente conhecidas por *threat intelligence*, possuem a finalidade de utilizar fontes de dados como base para a criação de *insights*. Essas ferramentas se propõem a atuar nesse contexto de forma estratégica, visando proporcionar consciência situacional e uma base para o planejamento de ações preventivas.

Threat intelligence é um assunto discutido com certa restrição no contexto acadêmico, sendo tratado majoritariamente na esfera da indústria de software e de tecnologias para a área de segurança cibernética e inteligência cibernética. Dentro do meio acadêmico percebe-se que os termos, normalmente, são discutidos em contextos isolados, como métodos de extração e normalização de dados (R. Meier, C. Scherrer, D. Gugelmann, V. Lenders, and L. Vanbever, 2018), estratégias voltadas para a análise de dados armazenados e a necessidade de compartilhar dados de forma granular e gerenciável (A. Schwartz, S. C. Shah, M. H. MacKenzie, S. Thomas, T. S. Potashnik, and B. Law, 2016).

As ferramentas de *threat intelligence* existentes até o momento da realização desta pesquisa, incluindo as gratuitas, possuem algumas de suas funcionalidades discutidas academicamente, onde são propostas outras abordagens ou até melhorias nas técnicas e métodos utilizados. Porém, aquelas que objetivam englobar a

funcionalidade de compartilhar dados de forma granular, gerenciável e independente de plataforma, não são de fácil acesso e entendimento, e nem encontradas em soluções gratuitas.

A principal contribuição deste trabalho é propor e implementar um modelo de referência de *threat intelligence*, suportado por funcionalidades encontradas em outras ferramentas já existentes, com o intuito de difusão de conhecimento agregado sobre ameaças. Nesse sentido, foi desenvolvido uma ferramenta como prova de conceito que aborda todas as camadas previstas no modelo, tendo seu foco principal no compartilhamento de dados.

A estrutura deste trabalho está dividida nas seguintes seções. O embasamento teórico e os trabalhos correlatos ao modelo aqui proposto estão na Seção 2. Já na Seção 3 é apresentada a proposta de modelo de referência, bem como as camadas da ferramenta de *threat intelligence* desenvolvida como prova de conceito. A Seção 4 apresenta alguns resultados do uso da ferramenta desenvolvida na forma de telas e agregadores de indicadores. A Seção 5 conclui esse trabalho e discute alguns temas futuros a serem considerados.

2. REFERENCIAMENTO TEÓRICO E TRABALHOS CORRELATOS

Segundo Rob McMillan (Gartner, 2016), *threat intelligence* é definido como o conhecimento baseado em evidências, que incluem o contexto, mecanismos, indicadores, implicações e aconselhamento sobre ameaças existentes ou emergentes que podem trazer danos a ativos. Essa definição também é suportada por esse artigo.

A maior parte das informações disponíveis sobre *threat intelligence* é de cunho voltado para a indústria de software e de tecnologia. No entanto, organizações como a *OASIS* (https://www.oasis-open.org) incentivam seu uso de forma livre, através do desenvolvimento de bibliotecas de código aberto e difundindo seus fundamentos. Outro exemplo é a empresa de segurança cibernética *Anomali* (https://www.anomali.com), que tem contribuído para o crescimento da área de *threat intelligence* por meio de ferramentas abertas à comunidade. A ferramenta *STAXX* (https://www.anomali.com/pt/community/staxx) é um exemplo de um software livre, e a fonte de dados *Limo* (https://www.anomali.com/community/limo), é um exemplo de *feed* gratuito e exclusivo para *threat intelligence*.

No que diz respeito às referências acadêmicas existentes sobre *threat intelligence*, a maior parte tem a intenção de pormenorizar tópicos específicos sobre o tema. Por exemplo, o artigo de Sarah Brown e Joep Gommers (S. Brown, J. Gommers, and O. Serrano, 2015) descreve os desafios de coletar dados em meio à diversidade de fontes, à necessidade intrínseca de normalizá-los visando sua padronização, com o intuito de facilitar o armazenamento, a pesquisa e sua manipulação. Por outro lado, o trabalho de Aziz Mohaisen, Omar Al-Ibrahin (A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla, 2017) discute a necessidade de compartilhar informações sobre ameaças, apresentando a necessidade de se criar um modelo de infraestrutura voltado ao compartilhamento, arcar com riscos, escolher uma estrutura de dados aberta e independente de fabricante, além de realizar o controle de qualidade dos dados que são compartilhados. Outro artigo, dos pesquisadores Cynthia Wagner e Gerard Wagner (C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, 2016), relata como foi criada uma ferramenta de *threat intelligence*, desde a estrutura metodológica e os objetivos, até como ela é utilizada dentro de um contexto específico.

Para evidenciar a importância da utilização de ferramentas de *threat intelligence*, a Tabela 1 apresenta o clico de vida de um ataque ocorrido e que teve consequências sérias para diversas empresas (E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, and P. Shakarian, 2016).

Baseado nas informações da *Tabela 1*, observa-se que em fevereiro de 2015, a Microsoft identificou uma falha de segurança no sistema operacional Windows. A falha permitia a execução remota de código malicioso e, até o momento da divulgação, não havia softwares que explorassem essa vulnerabilidade. Em abril de 2015, um *exploit* que se aproveitava dessa vulnerabilidade foi localizado sendo vendido em um mercado na *darknet*. Em julho de 2015 a empresa de segurança FireEye identificou um trojan que foi denominado de *Dyre Banking*. Esse trojan era capaz de roubar números de cartões de crédito, explorando essa vulnerabilidade. A exposição global média do *Trojan Dyre Banking* foi de 57,3%, ou seja, quase 6 em 10 organizações no mundo foram afetadas.

Tabela 1. Ciclo de vida de ataque

Timeline	Event
Fev. 2015	Microsoft identificou uma vulnerabilidade (MS15- 010/CVE 2015-0057) que permite a execução de código remotamente no Windows. Até o momento não existia nenhum *exploit* conhecido para essa vulnerabilidade.
Abr. 2015	Um exploit (MS15-010/CVE 2015-0057) que fazia uso dessa vulnerabilidade, foi encontrado a venda no darknet market por 48 BTC (cerca de \$10,000-15,000).
Jul. 2015	A FireEye identificou que o *Trojan Dyre Banking*, desenhado para roubar dados de cartões de crédito, fazia uso dessa vulnerabilidade.

Analisando a estrutura do ataque, um padrão é translúcido. Entende-se que os cyber-criminosos estão se aproveitando de vulnerabilidades conhecidas objetivando prejudicar infraestruturas vitais para o seguimento das funções desempenhadas na esfera tecnológica, cada vez em menos tempo. No caso do exemplo descrito acima, em menos de 3 meses era possível explorar remotamente e com sucesso a falha.

Devido à grande quantidade de vulnerabilidades expostas e a necessidade de refiná-las a ponto de se tornar um ativo utilizável na contenção de ataques, realizar esse processo de forma manual é uma tarefa complicada e complexa, sendo necessário o emprego de ferramentas apropriadas. Nesse enfoque, a utilização de ferramentas de *threat intelligence* teria como objetivo auxiliar na descoberta de falhas referentes ao contexto investigado, gerando consciência situacional e proporcionando bases para a tomada de decisões. Caso a plataforma utilizada disponibilize funcionalidades de compartilhamento, seria possível repartir o cenário concebido e suas experiências geradas, com parceiros e/ou aliados em curto espaço de tempo.

2.1 Fontes de *Threat Intelligence*

O nome dado aos locais em que se encontram e de onde são extraídos conteúdos necessários para alimentar as ferramentas de *threat intelligence* é amplamente conhecido por "*Feed*". Não existe um padrão para a escolha desses locais, qualquer fonte pode conter dados que, dentro de algum contexto e dentro de alguma abordagem, podem gerar valor. Algumas fontes usuais no contexto de *threat intelligence* podem parecer incomuns na visão de outras ferramentas que também extraem informação de fontes de dados, como por exemplo blogs, fóruns e sites vinculados à *darknet*.

Os *feeds* são divididos em duas categorias: privados e abertos. Os *feeds* privados possuem autoria e objetivos profícuos. Empresas como a McAfee (https://www.mcafee.com/enterprise/pt-br/threat-center/global-threat-intelligence-technology.html) e a Symantec (https://www.symantec.com/services/cyber-security-services/) vendem esse tipo de solução. *Feeds* abertos são dados disponíveis cujo acesso possui autoria, porém não é gerado objetivando lucro. Como exemplo de *feeds* abertos, existem os relatórios de pesquisadores de segurança, blogs de fornecedores de soluções de segurança, listas de bloqueio e reputação de endereços e URLs disponíveis publicamente. Além disso, algumas empresas que oferecem *feeds* de forma gratuita, como *Anomali* (https://www.anomali.com/), *Hailataxii* (http://hailataxii.com/) e *Alienvault* (https://www.alienvault.com/).

Considera-se também que os dados gerados por infraestruturas computacionais são um tipo de fonte de dados que também pode ser utilizada no contexto de *threat intelligence*. Ou seja, internamente, as organizações podem utilizar os dados gerados pelo próprio ambiente nesse contexto, enriquecendo seus próprios dados.

Os *feeds* contém dados disponíveis em diversos tipos, formatos e estruturas. A falta de padronização na disposição desses dados é um problema, pois para cada formato diferente é necessário um algoritmo específico para coleta e normalização em formato padronizado. Visando sanar essa adversidade, a organização *Mitre* (https://www.mitre.org/) foi a autora de uma iniciativa que, de forma aberta e colaborativa, concebeu uma estrutura baseada em ontologias, visando o registro e compartilhamento de eventos relacionados à segurança da informação, para seu uso de forma indiscriminada.

Essa estrutura é utilizada no padrão *Structured Threat Information eXpression* (STIX) (S. Barnum, 2012), também criado por iniciativa da Mitre, como uma linguagem para a especificação, captura, caracterização e comunicação padronizada de eventos. A implementação dessa estrutura de acordo com o padrão STIX é resumido na *Tabela 2*. O STIX fornece mecanismos comuns para lidar com informações estruturadas de *threat intelligence*, objetivando melhorar a consistência, a eficiência, a interoperabilidade e o conhecimento geral da situação. Até o momento da elaboração deste trabalho, existem duas versões do STIX disponíveis, a 1 e a 2. A versão 1 é estruturada em XML e a versão 2 em JSON.

O compartilhamento de informações sobre ameaças pode ser utilizado de forma eficiente, estratégica e eficaz contra ameaças emergentes (A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla, 2017). Já foi dito que "O compartilhamento de dados voltados a inteligência de ameaças é a única maneira de combater o crescente gap de habilidades" (Javvad Malik. 2016). Na prática o compartilhamento de informações é usado para comunicar experiência operacional, visando com que os participantes possam aprimorar suas defesas contra ataques contínuos, criando abordagens proativas nesse contexto.

Tabela 2. Descrição de objetos pertencentes ao STIX

Nome	Descrição
Attack Pattern	Táticas, técnicas e procedimentos (TTP), que indicam como atores de ameaças procuram alvos comprometidos.
Campaign	Um grupo de comportamentos que são usados como base para descrever atividades maliciosas e ataques, que ocorrem em determinado período de tempo.
Identity	Descrição de indivíduos, organizações ou grupos.
Indicator	Contém padrão que pode ser utilizado para identificar alguma ameaça.
Intrusion Set	Um grupo de comportamentos e recursos, usados por atores de ameaças.
Malware	Código malicioso e softwares, usados para comprometer ativos das vítimas.
Observed Data	Contém informações formadas por sistemas de redes (ex: endereço IP).
Report	Abrange detalhes de *threat intelligence*, como atores de ameaças, *malware*, técnicas de ataque e detalhes contextuais.
Threat Actor	Indivíduos, grupos, ou organizações, que se acredita operar com intenções maliciosas.
Tool	Software que pode ser usado por atores de ameaças objetivando realizar ataques.
Vulnerability	A descrição de falhas que podem ser diretamente usadas para causar danos.

Nesse sentido, uma vez que um evento for registrado, é interessante existir a possibilidade de compartilhá-lo. Aspirando essa funcionalidade, a Mitre criou uma outra iniciativa almejando o desenvolvimento de um padrão para suportá-la, o *Trusted Automated eXchange of Indicator Information* (TAXII) (J. Connolly, M. Davidson, and C. Schmidt, 2014). O padrão *TAXII* é um conjunto de especificações técnicas e documentações voltadas para suportar a troca de dados, de forma segura e independente de plataforma. Juntos, os padrões *STIX* e *TAXII* oferecem modelos que visam a disposição de dados e sua transferência de forma segura. Como ambos são livres e abertos, não há necessidade de seguir procedimentos de estruturação ou implantação, permitindo às instituições interessadas determinarem como suas ferramentas e serviços, os implementam e gerenciam o fluxo de dados de seu interesse.

2.2 Revisão sobre Ferramentas de *Threat Intelligence*

Conforme já exposto anteriormente, existe uma quantidade considerável de ferramentas de *threat intelligence* disponíveis. Uma das principais questões é que estas ferramentas não são gratuitas e, a maior parte delas, tem um custo financeiro bastante elevado. Basicamente, as ferramentas de *threat intelligence* se classificam em dois tipos, as pagas e as gratuitas.

Como exemplo de ferramentas pagas, cita-se a Luminar da empresa Verint (https://cis.verint.com/product/cybersecurity/lumiar/). A ferramenta em questão permite a realização de pesquisas de interesse utilizando pontos chave de seu conteúdo (como IPs, marcas, ativos, entre outros), dentro de uma visão de negócio ofertada como serviço. Outra ferramenta paga é a Threat Intelligence Exchange da empresa McAfee (https://www.mcafee.com/enterprise/pt-br/products/threat-intelligence-exchange.html). Essa ferramenta permite o uso de dados gerados pela infraestrutura computacional no contexto de threat intelligence, automatizando a busca por possíveis ameaças.

Em relação às ferramentas gratuitas, como exemplo, cita-se a solução denominada STAXX da empresa de segurança cibernética Anomali (https://www.anomali.com/community/staxx). A ferramenta STAXX tem a capacidade de coletar dados, armazená-los e fornece mecanismos que possibilitam ao usuário manipular e examinar os dados. Outro exemplo de ferramenta gratuita é a Malware Information Sharing Platform (MISP) (https://www.misp-project.org/documentation), uma ferramenta que permite a coleta, o armazenamento, a exploração de dados armazenados e seu compartilhamento. No entanto, o compartilhamento proposto pelo MISP precisa de melhorias, por exemplo, não é possível filtrar dados para requisições específicas e por usuário.

3. PROPOSTA DE MODELO DE REFERÊNCIA E FERRAMENTA DE THREAT INTELLIGENCE

De acordo com o estudo realizado, existe espaço para avanços e/ou melhorias em termos de *threat intelligence*, seja no âmbito acadêmico, seja na indústria de segurança cibernética. Observando esta consideração, este trabalho identifica e explora dois pontos. O primeiro é a ausência de um modelo de referência, que se propõe a promover um mapa de funcionalidades inerentes ao contexto de *threat intelligence*, visando apresentar um escopo em que todas essas funcionalidades se encaixem. O segundo é o número restrito de ferramentas abertas que possuem a funcionalidade de compartilhar dados, independente de plataforma e de forma gerenciável, visando introduzir uma ferramenta voltada a essa funcionalidade.

3.1 Modelo de Referência

Segundo os documentos disponíveis na literatura, observa-se várias funcionalidades sem uma estrutura que as entrelacem. Um modelo de referência serve, entre outras considerações, para as seguintes finalidades: entender o escopo de *threat intelligence*; ser usado como referência para entender funcionalidades encontradas em ferramentas nesse contexto; servir como base para o planejamento, visando a criação de ferramentas similares; e entender o clico de vida dos dados dentro do contexto de *threat intelligence*.

Visando suprir essa lacuna, foi elaborado como proposta um modelo de referência de *threat intelligence* cuja sua estrutura é baseada em seis camadas, conforme ilustrado na Figura 1.

Figura 1. Modelo de referência e suas camadas

A tabela 3 apresenta cada uma das camadas do modelo de referência com uma descrição de cada uma das suas respectivas funções.

Tabela 3. Descrição das camadas do modelo de referência

#	Camada	Descrição
1	Gerenciamento	A camada de gerenciamento é responsável por gerenciar a interação dos usuários com cada funcionalidade que a aplicação oferece e a interação entre elas. Essa camada também é responsável pelo controle de fluxo de dados e seu acesso. A implementação da camada de gerência por parte da aplicação deve fundamentar a gerência de permissões. Essa funcionalidade deve ser vinculada a todas ações que podem ser desempenhadas pelos usuários, como a criação de solicitações para coletar dados, a escolha da localização de armazenamento de dados, a manipulação de dados armazenados, o compartilhamento de dados, entre outras.
2	Armazenamento	Essa camada deve ser suportada por uma estrutura de armazenamento capaz de sustentar a quantidade de entrada e saída de dados almejada para o funcionamento das aplicações. As principais estruturas de armazenamento consideradas nesse caso são de bancos de dados relacional, como SQLLite (https://www.sqlite.org), Mysql (https://www.mysql.com), de bancos de dados não relacional, como por exemplo: Cassandra (http://cassandra.apache.org), MongoDB (https://www.mongodb.com). Ou estruturas customizadas, como a utilizada no Splunk (https://www.splunk.com). A estrutura implementada deve ser capaz de armazenar dados enviados pelas camadas de coleta e geração, e disponibilizar dados no formato exigido pelas camadas de pesquisa e compartilhamento.
3	Coleta	O objetivo dessa camada é fornecer a capacidade de coletar dados externos à infraestrutura vigente e internalizá-los. Essa camada deve oferecer funcionalidades que utilizem

#	Camada	Descrição
		mecanismos que coletam dados em diversos padrões e os estruture em um único formato, também compatível com o padrão requerido pela camada de armazenamento.
4	Geração	Essa camada é responsável fornecer funcionalidades voltadas a coleta de dados gerados pelos ativos internos e sua normalização em um único formato, compatível com o padrão requerido pela camada de armazenamento. Essa camada deve proporcionar a criação de *feeds* a partir de infraestruturas computacionais.
5	Pesquisa	Essa camada é responsável por agregar mecanismos e métodos visando a manipulação e exploração de dados armazenados. A estrutura que suporta essa camada deve oferecer funcionalidades voltadas à consulta de dados a partir da camada de armazenamento e deve fornecer visibilidade adequada segundo a necessidade de visualização de dados.
6	Compartilhamento	Essa camada tem como objetivo agrupar funcionalidades que visam o compartilhamento de dados com agentes fora da estrutura da aplicação. A criação de regras de negócio voltadas à permissividade, é essencial para o gerenciamento de forma granular. Visando a segurança, a aplicação deve possuir uma estrutura de compartilhamento separada, com acesso controlado e limitado somente a camada de armazenamento.

3.2 Implementação do Modelo de Referência

Como prova de conceito referente a funcionalidade prática do modelo apresentado na Seção 3.1, uma ferramenta de *threat intelligence* com o desígnio de compartilhamento de dados foi desenvolvida usando-o como fundamento. Ressalta-se que a ferramenta continua em desenvolvimento e está sendo aprimorada para ser, em futuro próximo, lançada como uma aplicação de software livre. A Figura 2 ilustra a estrutura da aplicação desenvolvida nesse trabalho.

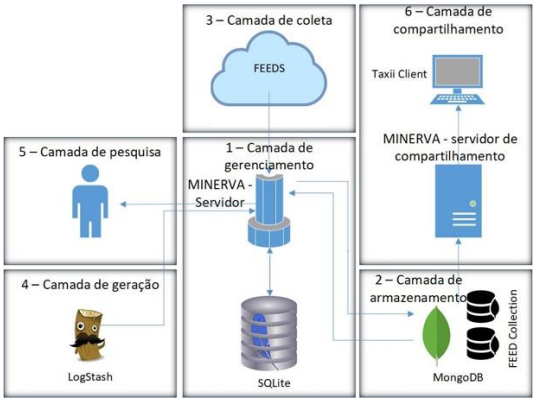

Figura 2. Estrutura da aplicação de threat intelligence

Os padrões elegidos que fundamentam essa aplicação foram o *STIX* 2 para o armazenamento de dados proveniente de *feeds*, o *TAXII* para o compartilhamento de dados e a estrutura de agrupamento de características de objetos em forma tabular, visando seu gerenciamento.

Após o término das definições iniciais sobre os padrões, foi dado preferência para a seleção de componentes da camada de armazenamento. Com o intuito de comportar funcionalidades inerentes de pesquisa rápida, foi escolhido o banco de dados NoSQL *mongoDB* (https://www.mongodb.com). Em linhas gerais, o *mongoDB* é um banco de dados não relacional concebido para trabalhar com dados no formato *JSON*, corroborando o suporte de dados estruturados no padrão *STIX 2*.

Para a camada de gerenciamento, foi escolhido o banco de dados relacional *SqlLite* (https://www.sqlite.org) para comportar as funcionalidades necessárias. Todos as características referentes a *feeds*, usuários e permissões, são armazenadas de forma tabular dentro dessa base.

Visando a camada de coleta de dados provenientes de *feeds*, foram implementadas até o momento 4 estratégias coletas de dados: a) robôs, para *feeds* não estruturados; b) *TAXII* para dados no formato *STIX/TAXII*; c) entrada de dados por arquivos; d) a implementação de uma estrutura de *parser* suportado pela plataforma *LogStash* (https://www.elastic.co/pt/products/logstash) para dados gerados internamente. De maneira geral, a implementação dessa estrutura suporta funcionalidades inerentes às camadas de coleta e de geração.

A interface com o usuário é implementada na camada de pesquisa. Para suportar suas funcionalidades foi escolhido escolhidos *d3js* (https://d3js.org) de maneira a deixar a interface mais amigável. Para desempenhar as funcionalidades pertinentes a camada de compartilhamento, foi implantado um servidor WEB separado dos demais componentes, com cuidados de segurança de maneira a restringir acessos. A estrutura do servidor WEB foi implementada para trabalhar no padrão *TAXII*.

4. APRESENTAÇÃO DOS RESULTADOS INICIAIS

Os resultados iniciais gerados pela ferramenta possuem valor intrínseco de acordo com proposta de modelo de referência. A aplicação traz mecanismos de segurança, como o controle de usuários. A Figura 3 ilustra uma tela de cadastro de usuários dentro aplicação. A aplicação permite o cadastro de *feeds* objetivando a extração de seu conteúdo e o armazenamento localmente. Para isso, são necessários dados como URL, credencias de acesso e local onde será armazenado. A Figura 4 ilustra uma tela de inserção de *feed*.

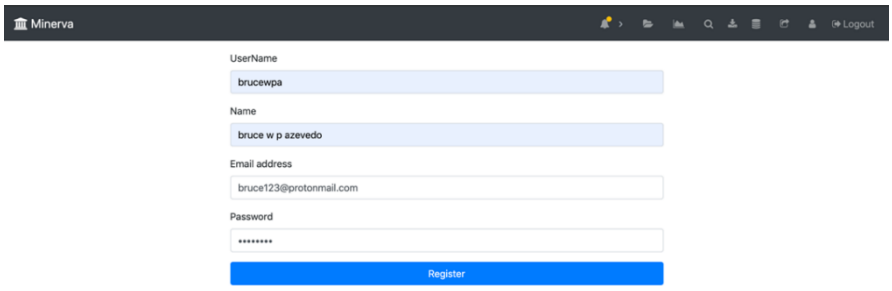

Figura 3. Tela de login

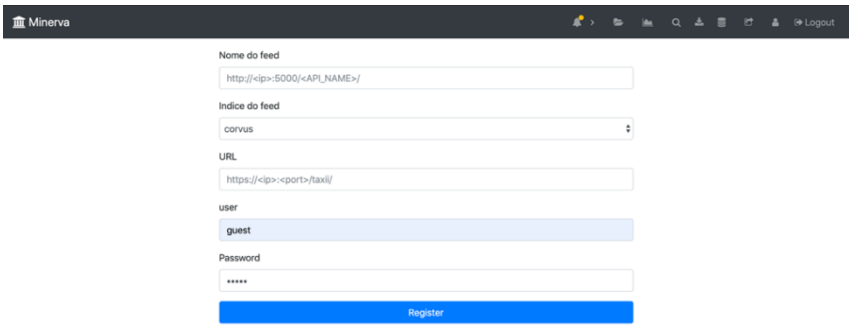

Figura 4. Tela de cadastro de feeds

A solução desenvolvida realiza a segmentação de armazenamento dos dados. Neste caso, cada base de dados armazena um *feed* diferente, e para fins de separação, cada *feed* gera o nome da base de dados a ser cadastrada. A Figura 5 ilustra uma tela de gerência de bases.

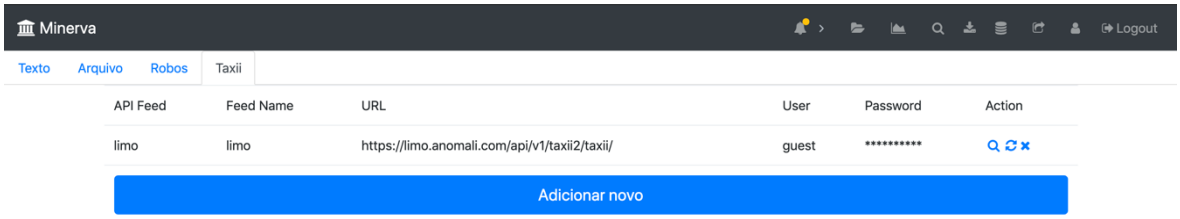

Figura 5. Tela de gerenciamento de feeds

Visando gerar visibilidade adequada das informações armazenadas, foram criadas propostas em forma de gráfico. A Figura 6 apresenta uma dessas propostas. Para controlar o compartilhamento dessas informações, foi criada uma proposta de gerenciador de vínculos entre usuários e *feeds*, onde é especificado qual usuário pode coletar os dados de quais *feeds*. A Figura 7 apresenta essa estrutura.

Figura 6. Gráfico de dados armazenados por feed

Figura 7. Criação de vínculo entre feeds e usuários

A funcionalidade de compartilhamento de dados disponibilizada pela aplicação é vedada a usuários que possuem permissão de coleta vinculada ao *feed* requerido. A Figura 8 apresenta a solicitação de credenciais referente a uma requisição de dados.

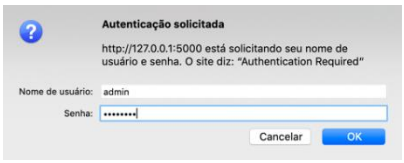

Figura 8. Tela de login exigido pela aplicação

A Figura 9 traz uma pilha de dados STIX (formato *json)* proveniente de uma requisição feita a aplicação.

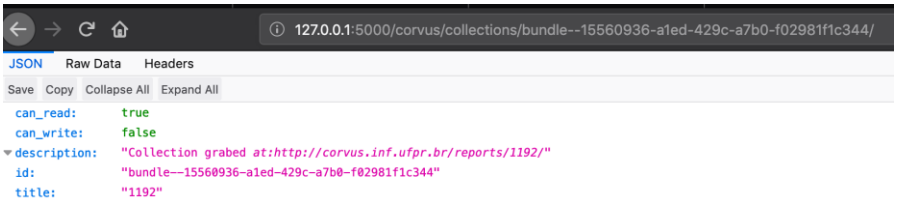

Figura 9. Resposta de requisição realizada ao servidor

5. CONCLUSÃO E TRABALHOS FUTUROS

As principais motivações para esse trabalho foram a identificação da falta de um modelo de referência de *threat intelligence* e de uma ferramenta que realize compartilhamento de dados de forma granular e independente de plataforma.

Foi proposto um modelo de referência que divide as funcionalidades inerentes ao contexto de *threat intelligence* em 6 camadas. Cada camada foi descrita e suas funcionalidades dispostas. Entende-se que, após o término da implementação da solução por completo, a sua utilização pode vir a ser uma ferramenta que permita o usuário entender o escopo de *threat intelligence* com mais facilidade. Além disso, o protótipo implementado na prova de conceito permite considerar novas implementações de ferramentas de *threat intelligence* tendo como base o modelo de referência. Por fim, também se observa que o protótipo serve como base para entender o ciclo de vida de dados no contexto de *threat intelligence*.

Ressalta-se que o modelo de referência proposto serviu como fundamento para o desenvolvimento de uma aplicação demonstrativa de *threat intelligence* que logra atuar em todas as camadas apresentadas. Porém, o principal objetivo desejado para sua implementação é promover a capacidade de compartilhar dados com permissões concedidas de forma granular, gerenciável e independente de plataforma, facilitando o intercâmbio de dados de interesse para questões de análise de segurança cibernética.

Os próximos passos visam continuar o desenvolvimento da ferramenta, permitir a realização de novas pesquisas referente ao consumo e utilização de dados gerados por infraestruturas computacionais, voltando-os para o contexto de *threat intelligence*. Como visão futura do desenvolvimento, entende-se a possibilidade de entregar consciência situacional para suporte para tomada de decisões de forma automatizada.

AGRADECIMENTO

Os autores agradecem o apoio das Agências brasileiras de pesquisa, desenvolvimento e inovação CNPq (Projeto INCT SegCiber 465741/2014-2), CAPES (Projetos FORTE 23038.007604/2014-69 e PROBRAL 88887.144009/2017-00) e FAPDF (Projetos UIoT 0193.001366/2016 e SSDDC 0193. 001365/2016), bem como o suporte do Laboratório LATITUDE/UnB (Projeto SDN 23106. 099441/2016-43), e as cooperações com o Ministério da Economia (TEDs DIPLA 005/2016 e ENAP 083/2016) e o Gabinete de Segurança Institucional da Presidência da República (TED 002/2017).

REFERÊNCIAS

A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla, 2017 “Rethinking information sharing for threat intelligence”. Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies. San Jose, United States. p. 6.

A. Schwartz, S. C. Shah, M. H. MacKenzie, S. Thomas, T. S. Potashnik, and B. Law, 2016. “Automatic threat sharing: How companies can best ensure liability protection when sharing cyber threat information with other companies or organizations” U. Mich. JL Re-form, vol. 50, p. 887.

C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, 2016. “Misp: The design and implementation of a collaborative threat intelligence sharing platform”. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. Vienna, Austria. pp. 49–56.

E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, and P. Shakarian, 2016. “Darknet and deepnet mining for proactive cybersecurity threat intelligence”. IEEE Conference on Intelligence and Security Informatics (ISI). Tucson, United States. pp. 7–12.

Gartner, 2016. “Definition: Threat intelligence”. https://www.gartner.com/doc/2487216/defnition-threat-intelligence.

J. Connolly, M. Davidson, and C. Schmidt, 2014. “The trusted automated exchange of indicator information (taxii)” The MITRE Corporation, pp. 1–20.

J. Poushter et al., 2016. “Smartphone ownership and inter-net usage continues to climb in emerging economies”. Pew Research Center, vol. 22, pp. 1–44.

Javvad Malik. 2016. Threat Intelligence Sharing: The Only Way to Combat Our Growing Skills Gap. Information Security Magazine.

R. Meier, C. Scherrer, D. Gugelmann, V. Lenders, and L. Vanbever, 2018. “Feedrank: A tamper-resistant method for the ranking of cyber threat intelligence feeds”. 10th International Conference on Cyber Conflict (CyCon), pp. 321–344.

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

S. Brown, J. Gommers, and O. Serrano, 2015. “From cybersecurity information sharing to threat management”. Proceedings of the 2nd ACM workshop on information sharing and collaborative security, Denver, United States. pp. 43–49.

S. Samtani, K. Chinn, C. Larson, and H. Chen, 2016. “Az-secure hacker assets portal: Cyber threat intelligence and malware analysis”. IEEE Conference on Intelligence and Security Informatics (ISI). Tucson, United States. pp. 19–24.