Arquitetura de Cyber Threat Intelligence para cenários aplicados à Cibersegurança

Proposta de Tese Doutoral em Ciência e Tecnologia Web

Cyber Threat Intelligence Architecture for Applied Cybersecurity Scenarios

PhD Thesis Proposal in Web Science and Technology

Ivo Rosa[1], Ricardo Batista[2], Ramiro Gonçalves[1,5], José Martins[3,4], Frederico Branco[1,5]

[1] Universidade de Trás-os-Montes e Alto Douro, Vila Real, Portugal
[2] FEUP – Universidade do Porto, Porto, Portugal
[3] Instituto Politécnico de Bragança, Bragança, Portugal
[4] AquaValor – Centro de Valorização e Transferência de Tecnologia da Água, Chaves, Portugal
[5] INESC TEC, Porto, Portugal

ivorosa@gmail.com, ricardo.batista@uab.pt, ramiro@utad.pt, jose.martins@aquavalor.pt, fbranco@utad.pt

Resumo — **Quando se fala em Cibersegurança, em particular nos processos de resposta a incidentes de segurança da informação, é muito comum e relevante falar-se na capacidade de detetar atividades e/ou comportamentos maliciosos ou suspeitos o mais antecipadamente possível, ou seja, neste domínio da Cibersegurança todos desejam reduzir o tempo médio de deteção, (MTTD) ou o tempo médio para responder (MTTR) a um potencial incidente de segurança. A utilização de técnicas de *Cyber Threat Intelligence* - CTI pode contribuir para a redução do tempo médio para detetar ameaças e consequentemente influenciar diretamente o tempo de resposta, no entanto, existem diferentes tipos de *Cyber Threat Intelligence* que servem diferentes propósitos. O objetivo do estudo é o desenvolvimento de uma arquitetura de referência para apoiar e processar informações provenientes dos mais diversos tipos de fontes de dados em termos de *Cyber Threat Intelligence*, por exemplo, combinando dados recolhidos de em *Open Source Intelligence* - OSINT e *honeypots*, tendo em consideração as vantagens e desvantagens de cada um destes tipos de fontes de dados para os correlacionar entre si, de modo a aumentar a confiança e fiabilidade dos indicadores relevantes que podem ser utilizados pelos analistas de segurança nos processos de resposta a incidentes. Este artigo apresenta a proposta de trabalho de doutoramento em Ciência e Tecnologia Web, com previsão para conclusão em julho de 2023. Esta tese de doutoramento insere-se na área da Engenharia Informática, com aplicabilidade no domínio da Cibersegurança e consequentemente no subdomínio do *Threat Intelligence*. O projeto de investigação encontra-se na fase de estudo do estado da arte. Espera-se com a participação neste Simpósio Doutoral obter potenciais comentários que podem potencializar o crescimento e complemento do trabalho de investigação em curso.**

Palavras Chave - Cibersegurança, Cyber Threat Intelligence, Security Feeds.

Abstract — **When talking about Cybersecurity, particularly in security incident response plan and processes it is very common and relevant to talk about the ability to detect malicious or suspicious activities and behavior as soon as possible, in other words, in this domain, in Cybersecurity everyone wants to reduce the Mean time to detect (MTTD) or Mean time to respond (MTTR) a potential security incident. The use of *Cyber Threat Intelligence* - CTI indicators can contribute to the reduction of the mean time to detect threats and consequently directly influence the time to response, however there are different types of *Cyber Threat Intelligence* that serve different purposes. The objective of the study is the development of a reference architecture to support and process data from the most diverse type of data sources in terms of *Cyber Threat Intelligence*, for example using the combination data from Open Source Intelligence - OSINT sources and honeypots, taking into consideration the advantages and dis-advantages of each of these types of data sources to correlate them with each other in order to increase the trust and reliability of the relevant indicators that can be used by security analysts in incident response processes. This paper presents the proposed work for a PhD thesis in Web Science and Technology, scheduled for completion in July 2023. This doctoral thesis falls within the area of Computer Engineering, with applicability in the domain of Cybersecurity and consequently in the subdomain of *Threat Intelligence*. The research project is in the state-of-the-art study phase. It is expected that the participation in this Doctoral Symposium will provide potential comments that can enhance the growth and complement the ongoing research work.**

Keywords - Cybersecurity, Cyber Threat Intelligence, Security Feeds.

2022 17th Iberian Conference on Information Systems and Technologies (CISTI)
22 – 25 June 2022, Madrid, Spain
ISBN: 978-989-33-3436-2

I. Introdução

Nos dias de hoje temos identificado um aumento exponencial dos ciberataques e incidentes de segurança, sendo por isso difícil ou até mesmo impossível, para as organizações e consequentemente para equipas de segurança, garantir que os seus sistemas estão a cem por cento seguros, no entanto, podem e devem estar preparadas para responder e reagir em conformidade com determinados objetivos que sejam para, responder, conter, mitigar ou até mesmo recuperar os sistemas que foram atacados.

Este projeto de investigação não irá, nem é o objetivo, resolver todo o tipo de incidentes ou ameaças de segurança, mas sim contribuir, através da disponibilização de *feeds* de inteligência que ajudem a identificar o mais cedo possível a existência de possíveis ameaças.

O trabalho proposto almeja ser diferenciador relativamente aos estudos atuais, pois irá abranger a recolha de *feeds* de segurança em fontes abertas e em uma rede de honeypots recolhendo dados estruturados (endereços IPs, domínios, URLs, vulnerabilidades, listas de endereços de email comprometidos, dicionários de *username* e *password* utilizados em ataques de força bruta (*brute force*) e não estruturados (como por exemplo a recolha de determinados conteúdos ou simples *keywords* em redes sociais, como o *Github*, ou em determinadas aplicações web de partilha de informação como o *Pastebin* ou simplesmente através da recolha de determinados *payloads* tecnológicos, que depois são alvo de tratamento através de um algoritmo, a desenvolver, para classificar os dados recolhidos, aumentando o nível de fiabilidade e confiança sobre os indicadores a disponibilizar às equipas de monitorização de segurança. Este processo de classificação dos indicadores recolhidos será efetuado através da utilização de técnicas de inteligência artificial.

Esta abordagem será diferenciadora pelo tipo de dados recolhidos e investigados, o que irá reduzir o número de falsos positivos nos indicadores disponibilizados, mas também pela variabilidade dos dados analisados que certamente contribuirão para um aumento dos cenários de casos de uso em que os indicadores de ciberinteligência podem ser aplicados e comparados com os dados de sistemas internos, numa organização para a identificação de possíveis ameaças ou de comportamentos suspeitos.

No final a arquitetura desenvolvida corresponderá a um *Big Data* de indicadores de *Threat Intelligence*, devidamente classificados de acordo com o seu nível dinâmico de risco (este nível de risco irá considerar como atributos chave o tipo de ameaça, o tipo de técnicas de ataque, a atualidade e a persistência) e os resultados disponibilizados por esta solução podem ser utilizados num contexto organizacional para aferir as suas vantagens e/ou desvantagens na identificação da presença de ameaças numa rede informática.

Para suportar o desenvolvimento desta proposta de trabalho de investigação, foi identificada a metodologia *Design Science Research* (DSR) pois é a que melhor se adequa com ideia base de desenvolvimento de uma arquitetura de referência.

II. Contexto Conceptual

A. Definição de Cibersegurança

De uma forma global, este projeto, situa-se na área da Engenharia Informática, no entanto e de um modo mais específico irá focar-se no domínio da Cibersegurança.

A Cibersegurança é um termo que á aplicável a todas atividades que possam ocorrer em um novo e recente espaço de atuação denominado de Ciber Espaço [1]. Diakun [2] propõem a seguinte definição para a Cibersegurança:

"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de fact property rights." [2]

A Cibersegurança faz parte do conceito geral de Segurança de Informação que, consensualmente até na comunidade internacional através do referencial da ISO27001 [3], é definida como sendo assente em três grandes pilares que são as Tecnologias, Pessoas e Processos e identifica um conjunto de controlos chave de forma que seja garantida a segurança da informação.

O domínio da Cibersegurança é muito atual e presente no nosso dia-a-dia e já tem um grande número de subdomínios de conhecimento relacionados, *Threat Intelligence* é um desses subdomínios.

B. Conceitos chave de Cibersegurança

No domínio da Cibersegurança existem 4 grandes definições que se aplicam em diferentes contextos:

- Vulnerabilidade;
- Incidente de Segurança;
- Riscos;
- Controlos de Segurança;

Uma **vulnerabilidade** corresponde a uma fraqueza num sistema de informação, procedimentos de segurança, situação anómala ou de não conformidade com os controlos do sistema de gestão de segurança de informação de uma organização, ou uma implementação que pode ser explorada ou acionada através de fonte externa com intenções maliciosas [3]. Estas fraquezas podem corresponder a uma alteração do nível de risco de segurança de informação e/ou de privacidade. O ato de exploração de uma vulnerabilidade corresponde a um incidente de segurança.

No que respeita à gestão de **incidentes de segurança** e de acordo com os standards internacionais [3] que identificam dois grandes conceitos distintos, mas relacionados: evento de segurança e incidente de segurança.

Entende-se por evento de segurança da informação a ocorrência identificada em um sistema, serviço, rede ou recurso, que indica uma possível falha na aplicação da política de segurança da informação, falha de/em controlos de segurança ou uma situação até então desconhecida que pode ser relevante para a segurança da informação. Por outro lado, um **incidente de segurança** de informação corresponde a uma falha ou quebra de políticas, procedimentos ou regras de segurança da informação, e/ou um evento ou série de eventos/vulnerabilidades de

2022 17th Iberian Conference on Information Systems and Technologies (CISTI)
22 – 25 June 2022, Madrid, Spain
ISBN: 978-989-33-3436-2

segurança da informação, inesperados e indesejados, que comprometem ou podem comprometer as operações de negócio e a segurança da informação de uma organização.

Por definição entende-se por **risco** o nível de impacto gerado nas operações e continuidade de negócio de uma organização, cujo resultado objetivo resulta da combinação entre a probabilidade de ocorrência de um determinado evento/ameaça e o impacto que pode resultar desse mesmo evento [3].

Os **controlos de segurança** definidos no sistema de gestão de segurança de informação de uma organização [3], correspondem a uma proteção ou contramedida prescrita para um sistema de informações que visa proteger a confidencialidade, integridade e disponibilidade das suas informações e dados e responderem a um conjunto de requisitos de segurança definidos, evitando ou reduzindo a probabilidade de ocorrência de incidentes de segurança de informação.

III. Princípios de Cyber Threat Interlligence

A. Conceitos

A Cibersegurança é um domínio bastante atual e presente no nosso dia-a-dia, e já possui uma grande quantidade de subdomínios de conhecimento. Este projeto de investigação irá focar-se no subdomínio do *Threat Intelligence* e como estas abordagens influenciam a Cibersegurança.

O *Threat Intelligence* corresponde ao processo de tratamento de dados sobre possíveis ameaças e os grupos de atores considerados atacantes que as exploram, esses dados contribuem para que as organizações identifiquem, o mais antecipadamente possível, riscos de Cibersegurança que merecem ser acauteladas de forma a evitar cenários de ataque a organizações [4].

A utilização de técnicas da CTI está relacionada com os conceitos-chave acima mencionados, uma vez que podem contribuir para a identificação de vulnerabilidades ou, em situações mais avançadas, a presença de um incidente de segurança ou, de outra perspetiva, podem ajudar a identificar a necessidade de aplicar controlos de segurança adicionais tendo em conta o aparecimento de novos riscos.

As fontes de *cyber threat* são múltiplas, sendo que podem provir da utilização de fontes abertas – OSINT (*Open Source Intelligence*), da análise de social *media*, pesquisa de informação tecnológica, ou até à investigação profunda na *darkweb*.

Até agora, e tendo por base os estudos analisados, é muito comum encontrarmos soluções que já fazem a recolha de dados, com um significado de *Threat Intelligence*, porém de forma isolada, ou seja, queremos com isto dizer que existem estudos que se baseiam na recolha de dados estruturados e específicos [5][6] como são o caso de endereços IPs, domínios, URLs, vulnerabilidades entre outros, outros autores optaram por recolher dados não estruturados [7][8] baseados em pesquisas assentes em *keywords* relevantes para o contexto de uma determinada organização ou com significado de Cibersegurança.

A utilização de técnicas de *Threat Intelligence* [9] corresponde ao conhecimento adquirido através de mecanismos de recolha de informação e indicadores sobre possíveis ameaças externas a uma determinada organização, posteriormente esse novo conhecimento poderá ser utilizado e aplicado para descobrir possíveis ameaças a ocorrerem internamente numa organização [5]. Este novo conhecimento produz uma visão holística sobre os ciberataques, permitindo a identificação de quem são os atacantes e quais são as táticas, técnicas e procedimentos envolvidos [10].

B. Categorias de Cyber Threat Intelligence

Tipicamente "CTI - *Cyber Threat Intelligence*" pode ser dividido por categorias, sendo que na literatura podemos encontrar a divisão entre táticas, técnicas, operacionais e estratégicas [11].

Adotando a divisão em quatro níveis, temos [11] na Tabela 1 a descrição e o significado de cada uma das categorias:

Categorias de *Cyber Threat Intelligence*	Descrição
Táticas	Informação que guia a atuação do dia-a-dia das operações de segurança, sendo exemplo a deteção de máquinas infetadas a comunicar com servidores de comando e controlo de botnets na Internet.
Técnicas	São as informações que suportam a atividade da segurança operacional, que podem ser integradas em automatismos nas plataformas de segurança (usualmente denominadas de IoC – *Indicators of Compromise*). Enquadra-se neste cenário informações que podem corresponder a localizações maliciosas na internet, que serão automaticamente bloqueadas nas firewalls e equipamentos das redes de comunicações, de modo a impedir que os utilizadores lhe acedam desde a rede corporativa das organizações e evitando assim a eventual contaminação dos dispositivos.
Operacionais	Informação detalhada que explica as táticas, técnicas ou mais baixo nível os procedimentos associados a determinado ator ou ameaça.
Estratégicas	Informação de caracter executivo, como atividades de atacantes, risco de Cibersegurança nos setores de atividade, identificação de ameaças a digitais aos VIPs da organização ou ainda *Brand Protection*. São *feeds* de informação para serem interpretadas por humanos e não máquinas.

Tabela 1 – Descrição das categorias de Cyber Threat Intelligence

IV. Definição do Problema

Em estudos anteriores que se focaram em métodos de recolha e classificação de indicadores CTI, como é o caso da recolha em fontes abertas denominadas de OSINT de, por exemplo, endereços IPs, que evidenciaram ser possível usar estes indicadores de comprometimento (IoC) para procurar padrões numa rede interna que se relacionem com novas *blacklist* descobertas.

Nos casos em que é identificada uma correspondência entre os padrões na rede interna e a *blacklist*, significa uma deteção que merece ser avaliada com maior atenção tendo em vista a contenção e erradicação da ameaça. Estas metodologias mostram estudos favoráveis na perspetiva de Cibersegurança porém, apresentam sempre, com maior ou menor taxa de confiança nos resultados, que são considerados falsos positivos, colocando em causa o nível de confiança dos indicadores recolhidos e processados.

Existe um conjunto de outro tipo de trabalhos e investigações com o objetivo de recolherem indicadores de *Threat Intelligence* que passa pela utilização de mecanismos e técnicas para recolha de dados através dos denominados *honeypots*. Ao contrário dos estudos anteriores em que existe um sistema central com um conjunto de regras bem definidas que interroga um conjunto de fontes de dados, nos *honeypots* não controlamos quando se consegue obter novos dados, dependem apenas se os

ISBN: 978-989-33-3436-2

mesmos foram ou não capazes de atrair [12] ciberataques, que devem ser mitigados e contidos, sendo apenas útil para recolher informações chave sobre o atacante e as técnicas utilizadas. Em [12][13] são apresentadas abordagens cujo objetivo passa pela recolha de indicadores de inteligência contra-ameaças e a forma de integrar e partilhar esses dados de forma automatizada nos sistemas e mecanismos de monitorização de segurança de uma organização.

No entanto esta abordagem encontra-se limitada e dependente da capacidade de atrair atacantes e ciberataques, podendo não identificar, atempadamente, ameaças graves.

Perante as limitações de cada uma das abordagens, por um lado os níveis de confiança dos dados recolhidos através de OSINT e por outro a capacidade de atrair atacantes de através de *honeypots*, identificou-se uma proposta diferenciadora de tratamento deste tipo de informação, que passa pela correlação destes mesmos dados entre as diferentes fontes em que foram recolhidos com o objetivo de se aumentar os níveis de fiabilidade dos indicadores.

V. Questões de Investigação

A definição das questões a investigar é um dos passos mais importantes na investigação científica e define o modo como o problema é abordado. Assim, foram identificadas as seguintes questões base que guiarão esta investigação para melhor compreensão desta temática:

1. Quais as características que deve incorporar um sistema de *Big Data* de indicadores de *Threat Intelligence* para a segurança da informação, tendo em conta a problemática e os próprios desafios das tecnologias *Big Data*?
2. Quais os fatores críticos de sucesso e benefícios identificados pela análise do impacto, devido à adoção de uma arquitetura de sistemas de informação de *Big Data* de indicadores de *Threat Intelligence* aplicados no contexto da área da segurança da informação?
3. Graças à utilização de *Cyber Threat Intelligence* será possível as organizações anteciparem e descobrirem tendências de comportamento e padrões que podem pôr em risco a segurança da informação e continuidade do negócio?
4. Avaliar os dados perante a realização de testes aplicados a situações concretas como, por exemplo, a utilização das *feeds* de *Threat Intelligence* em cenários que usam tecnologias emergentes, através da denominada internet das coisas (IoT), em particular nos postos de carregamento de veículos elétricos com o objetivo da identificação de possíveis ameaças ou comportamentos anómalos.

VI. Objetivos Científicos

Este trabalho de investigação possui um objetivo geral, que passa por conseguirmos analisar, com rigor, a realidade e relevância do *Threat Intelligence* aplicado à área da segurança informática e da informação, através da análise aprofundada dos estudos elaborados por outros autores.

O macro objetivo passará pelo desenvolvimento de um artefacto tecnológico baseado na arquitetura chave que seja definida de forma a criar e suportar um *Big Data* de indicadores de *Threat Intelligence*.

Desta forma e para atingir o objetivo principal, foram identificados os seguintes objetivos específicos:

1. Fazer uma revisão sistemática sobre *Cyber Threat Intelligence;*
2. Identificar e classificar a importância e impacto do *Cyber Threat Intelligence* do ponto de vista de Cibersegurança nas organizações;
3. Avaliar a arquitetura definida de uma forma transversal e global, ao nível da fiabilidade e qualidade dos resultados devidamente processados pelas *feeds*;
4. Avaliar os resultados obtidos através da utilização da arquitetura definida, quando aplicada ao caso de estudo sobre os postos de carregamento de veículos elétricos;

VII. Metodologia Proposta

Para execução deste projeto de investigação foram identificadas 4 grandes fases de suporte à investigação. A primeira fase do trabalho irá incluir uma pesquisa aprofundada e respetiva revisão da bibliografia.

Numa segunda fase, provavelmente a mais complexa, e com a revisão da literatura bem presente, o foco passará pelo desenvolvimento do sistema baseado numa arquitetura de referência. Este trabalho irá resultar no desenvolvimento de um artefacto tecnológico - *Big Data* - que irá recolher, armazenar e disponibilizar dados de *Cyber Threat Intelligence* que depois, podem ser utilizados por organizações como fontes de inteligência para a identificação atempada de possíveis ameaças e de comportamentos suspeitos ou maliciosos.

Nos múltiplos tipos de sensores estamos a considerar a recolha periódica e direta de informação em fontes abertas e especificas, mas também a recolha em tempo real de indicadores numa rede distribuída, a desenvolver, de *honeypots*. Antes da disponibilização das *feeds* os dados armazenados devem ser devidamente classificados para aumentar a fiabilidade e nível de confiança da informação, através da utilização de um algoritmo específico que também reutiliza os diferentes tipos de sensores para classificar um determinado indicador, ou seja, se tenho um indicador descoberto através de fontes abertas posso validar a sua reputação e persistência nos dados recolhidos pela rede em tempo real de *honyepots*, sendo que, se existir relação o risco deste indicador será maior porque é uma ameaça que se encontra ativa. A mesma metodologia entre a rede de *honeypots* e as fontes abertas para classificar os indicadores também deve ser considerada.

ISBN: 978-989-33-3436-2

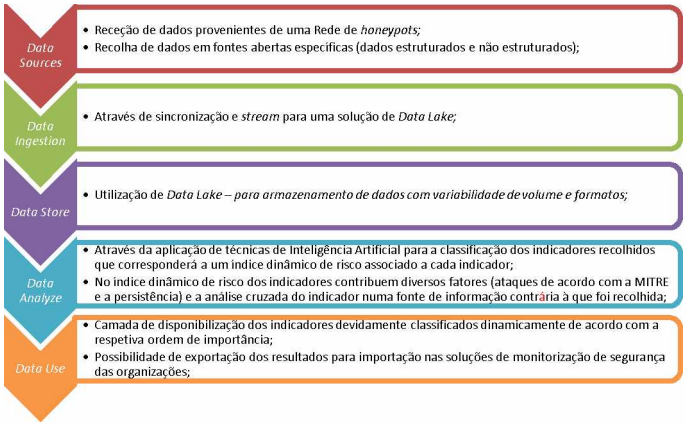

Figura 1- Big Data Pipeline com a descrição das componentes que o artefacto a desenvolver deve possuir

Conceptualmente, as soluções de *Big Data*, não se limitam ao armazenamento ou apenas ao suporte para grandes volumes de dados, no entanto a ideia passa pelo desenvolvimento de um *Big Data* de indicadores de *Cyber Threat Intelligence*, tendo em conta este propósito desenvolvi o *Big Data Pipeline* da Figura 1 e que pretende mapear as características que o artefacto deve possuir com diferentes componentes de um ambiente *Big Data*.

A terceira fase da investigação irá permitir avaliar o sistema, sendo que, a qualidade dos indicadores identificados bem como a aplicabilidade dos *feeds* em cenários que utilizem tecnologias emergentes, deve ser validada no contexto das equipas de monitorização de segurança de uma organização, que será identificada como validador e experimentador da solução.

Para finalizar, na quarta fase pretende-se analisar os resultados obtidos e inferir as vantagens e desvantagens da utilização avançada de indicadores, devidamente classificados e com suporte a múltiplos tipos de caso de uso, de *threat Intelligence*.

VIII. Resultados Esperados

Como vimos a utilização de *feeds* de *Cyber Threat Intelligence* são extremamente úteis para antecipar, identificar e em alguns casos desvendar, determinados eventos de segurança de informação, estas técnicas são enquadráveis com as típicas etapas do processo de resposta a incidentes.

Tendo por base e inspiração nos casos mencionados anteriormente, o nosso interesse de investigação passa por agregar num modelo único dados estruturados - IPs, domínios, URLs, vulnerabilidades, listas de endereços de email comprometidos, dicionários de *username* e *password* utilizados em ataques de *brute force* - e não estruturados - como por exemplo a recolha de determinados conteúdos ou simples *keywords* em redes sociais, como o *Github*, ou aplicações web de partilha de informação como o *Pastebin*, ou o *Ghostbin*, ou simplesmente a recolha de determinados *payloads* tecnológicos - classificáveis de *threat intelligence*, criando assim um verdadeiro *Big Data* de *Cyber Threat Intelligence* que correlacionando com dados, logs ou indicadores internos apresentam um valor real na identificação de ameaças ou de comportamentos e atividades suspeitas que merecem ser monitorizados e seguidos através de uma análise mais detalhada.

Com esta abordagem e conforme representado graficamente na Figura 2, espera-se aumentar os níveis de fiabilidade, confiança e precisão dos indicadores descobertos para a deteção de padrões suspeitos ou atividade anómala e que estes possam ser aplicáveis a um maior conjunto de casos de uso em particular em tecnlogias emergentes como a internet das coisas - IoT, sendo objetivo deste projeto a avaliação da aplicabilidade destes novos *feeds* aos postos de carregamento de veículos eléctricos.

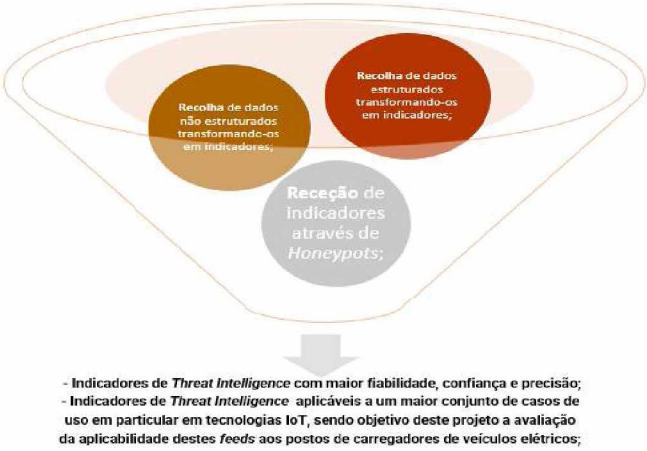

Figura 2 - Princípios previstos para o desenvolvimento do Big Data de indicadores de Cyber Threat Intelligence. Imagem desenvolvida pelos autores.

Para a avaliação da aplicabilidade do artefacto a desenvolver será feito uma análise de caso de estudo, que irá avaliar relevância dos resultados em matéria de *Cyber Threat Intelligence* e as vantagens/desvantagens do ponto de vista de Cibersegurança, quando aplicado no contexto dos postos de carregamento de veículos elétricos.

Agradecimentos

Este trabalho é financiado por fundo nacionais através da FCT – Fundação para a Ciência e a Tecnologia, I.P., no âmbito do projeto LA/P/0063/2020.

Referências Bibliográfica

[1] R. Bravo, Segurança Da Informação e Cibersegurança: Aspetos Práticos e Legislação, 2021.

[2] N. Diakun-Thibault, Defining Cybersecurity. Technology Inno-vation Management Review., 2014.

[3] "ISO/IEC 27001 - INFORMATION SECURITY MANAGEMEN," [Online].

[4] R. McMillan, "Definition: threat intelligence," Gartner, 16 Maio 2013. [Online]. Disponivel: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence. [Acedido em: 21 Novembro 2021].

[5] J. Alves, A. Respício, I. Rosa and P. Rodrigues, "Threat Intelligence – Improving SIEM cybercriminality awareness using information from IP blacklists," in eCrime2017.EU – APWG.EU Symposium on Electronic Crime Research, Porto, Portugal, 2017.

[6] J. Alves, "Threat intelligence: using osint and security metrics to enhance siem capabilities. Tese de mestrado, Segurança Informática, Universidade

ISBN: 978-989-33-3436-2

de Lisboa, Faculdade de Ciências," 2017. [Online]. Available: http://hdl.handle.net/10451/31162. [Accessed 25 Novembro 2021].

[7] N. Dionísio, "Improving cyberthreat discovery in open source intelligence using deep learning techniques. Tese de mestrado, Segurança Informática, Universidade de Lisboa, Faculdade de Ciências," 2018. [Online]. Available: http://hdl.handle.net/10451/36434. [Accessed 22 November 2021].

[8] E. Branco, "Cyberthreat discovery in open source intelligence using deep learning techniques. Tese de mestrado, Informática, Universidade de Lisboa, Faculdade de Ciências," 2017. [Online]. Available: http://hdl.handle.net/10451/30699. [Accessed 15 December 2021].

[9] M. Bromiley, Threat Intelligence: What It Is, and How to Use It Effectively, SANS Institute Reading Room site, 2016.

[10] F. Courtney, "An Ontology for Threat Intelligence," in Conference: European Conference on Cyber Warfare and Security, Munich, Germany, 2016.

[11] T. Olufohunsi, Understanding Cyber Threat Intelligence, 2020.

[12] S. Kumar, B. Janet and R. Eswari, "Multi Platform Honeypot for Generation of Cyber Threat Intelligence," 2019 IEEE 9th International Conference on Advanced Computing (IACC), 2019, pp. 25-29, doi: 10.1109/IACC48062.2019.8971584.

[13] H. Almohannadi, I. Awan, J. Al Hamar, A. Cullen, J. P. Disso and L. Armitage, "Cyber Threat Intelligence from Honeypot Data Using Elasticsearch," 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), 2018, pp. 900-906, doi: 10.1109/AINA.2018.00132.

ISBN: 978-989-33-3436-2