

Relatório Prático

Mestrado em Cibersegurança e Informática Forense

***Análise da Ferramenta MISP – Plataforma Open
Source para Conhecimento de Ameaças & Normas
abertas para a Partilha de Informação de Ameaças***

Filipe Henriques, 2180066

Leiria, março de 2019

This page was inthetionally left blank

Resumo

O tratamento de incidentes de segurança informática é uma área essencial na Cibersegurança das organizações, esta proporciona as organizações estabelecer planos que ajudam a assegurar a continuidade do seu negócio, e criar planos contra eventos relacionados com desastres naturais ou informáticos. Para ajudar na execução destas ações, existem várias ferramentas e plataformas que automatizam o processo de gestão e tratamento de eventos numa forma eficaz e rápida.

O MISP é uma dessas ferramentas, este é um software grátis que tem como objetivo a facilitação da partilha de informação de ameaças credíveis entre organizações certificadas. Esta apresenta duas formas de utilização: através de uma plataforma web instalada num servidor local da organização; e através incorporação do REST API do MISP numa ferramenta de segurança já existente numa organização. O MISP apresenta funcionalidades essenciais para exercer interações entre utilizadores da própria organização, e também entre outras organizações. Para além disto, existem as funcionalidades para a gestão de eventos e de criação de características como atributos e *templates* que complementam os eventos. Uma funcionalidade destinta que o MISP apresenta é a funcionalidade para filtrar dados, nomeadamente os dados que entram e saem para a instância da organização.

Após um estudo comparativo entre algumas plataformas e ferramentas relacionadas à partilha de informação de ameaças, conclui-se que o MISP é uma das opções mais atrativas no mercado, isto deve-se principalmente pelo facto da ferramenta ser basicamente grátis, e por proporcionar um enorme número de formas diferentes para lidar com dados de eventos da própria organização, e de outras, mas também para detalhar os seus próprios eventos.

This page was intetionally left blank

Lista de Figuras

Figura 1 - Modelo para gestão de incidentes da NIST	3
Figura 2 - Logotipo do MISP.....	6
Figura 3 - Funcionamento do MISP	7
Figura 4 – Barra de navegação da plataforma MISP	9
Figura 5 - Criação de um evento.....	9
Figura 6 - Criação de uma Tag	10
Figura 7 - Utilização de <i>templates</i> no MISP	10
Figura 8 - Listagem de <i>galaxies</i>	11
Figura 9 - Vista detalhada de uma <i>galaxy</i>	12
Figura 10 - Lista de expressões regulares	12
Figura 11 – Lista de Noticelists	13
Figura 12 - Gestão de feeds	14
Figura 13 - Menu de opções para administração	15
Figura 14 - Formulário de pesquisa de um log específico	15
Figura 15 - IBM X-Force Exchange Dashboard.....	18
Figura 16 - Funcionamento do RTIR.....	19

This page was intetionally left blank

Lista de Tabelas

Tabela 1 - Comparação de ferramentas	20
--	----

This page was intetionally left blank

Lista de acrónimos

API – *Application Programming Interface*

ATT&CK – *Adversarial Tactics, Techniques, and Common Knowledge*

CIRCL – *Computer Incident Response Center Luxembourg*

GDPR – *General Data Protection Regulation*

IBM – *International Business Machines*

IDS – *Intrusion Detection System*

ISO – *International Organization for Standardization*

JSON – *JavaScript Object Notation*

MISP – *Malware Information Sharing Platform*

NATO – *North Atlantic Treaty Organization*

NCIRC – *NATO Computer Incident Response Capability*

NIDS – *Network Intrusion Detection System*

NIST – *National Institute of Standards and Technology*

PGP – *Pretty Good Privacy*

REST – *Representational State Transfer*

RTIR – *Request Tracker for Incident Response*

URL – *Uniform Resource Locator*

This page was intetionally left blank

Índice

Resumo.....	ii
Lista de Figuras	iv
Lista de Tabelas	vi
Lista de acrónimos	viii
Índice.....	x
Introdução	1
1. Enquadramento	2
1.1. Gestão e Tratamentos de Incidentes de Segurança Informática	2
1.1.1. Ferramentas na Gestão de Incidentes de Segurança Informática	4
2. MISP	6
2.1. O que é o MISP?	6
2.2. Análise das Funcionalidades	8
2.2.1 Eventos	9
2.2.2. Galaxies	11
2.2.3. Filtros.....	12
2.2.4. Ações globais	13
2.2.5. Ações de Sincronização	13
2.2.6. Administração	14
2.2.7. Auditoria.....	15
2.3. Discussão	16
3. Estudo Comparativo	18
4. Conclusão.....	21
Referências	22

Introdução

No âmbito da unidade curricular de Tratamento de Incidentes de Segurança Informática, do curso de Mestrado Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, foi elaborado o presente relatório na análise da ferramenta MISP.

A Cibersegurança é uma área cada vez mais presente nas organizações no qual integram o mundo digital no seu negócio, para isto existem várias formas de aplicar a Cibersegurança. A gestão e tratamento de incidentes de segurança de informação é uma dessas formas, esta ajuda a criar planos e medidas para assegurar a continuidade do negócio, e também o estabelecimento de planos para eventos de desastre no qual organizações estão suscetíveis. Existem vários tipos de ferramentas que se especializam em diferentes aspetos no tratamento de incidentes, como por exemplo: ferramentas para investigação, tratamento e resposta a incidentes; plataformas de partilha de informação sobre ameaças; ferramentas de análise de *logs* e entre outras. Deste modo o presente relatório pretende efetuar a análise de uma destas ferramentas, o MISP - Plataforma *Open Source* para Conhecimento de Ameaças & Normas abertas para a Partilha de Informação de Ameaças, no qual trabalha no campo de partilha de conhecimento e de informação de ameaças.

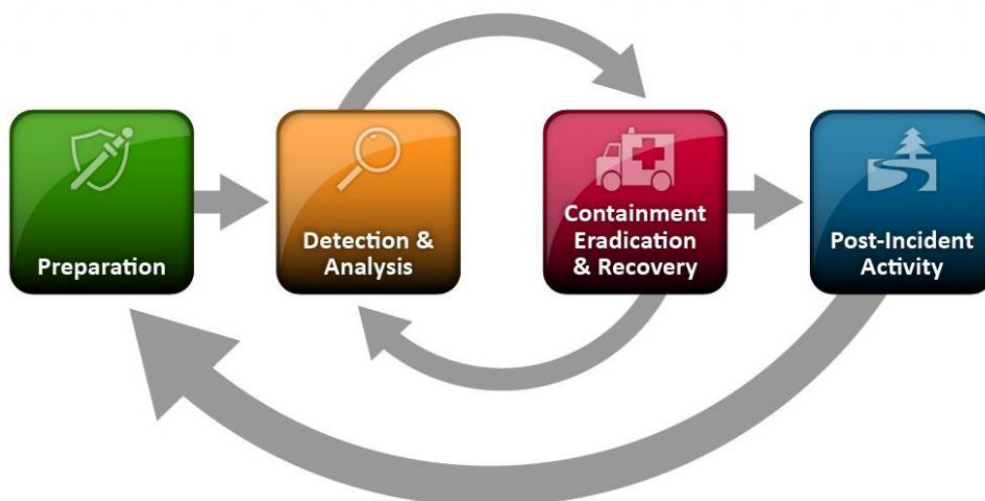
O presente relatório está dividido em quatro capítulos, sendo que o primeiro consiste no enquadramento, abordando os temas relacionados com a segurança informática e a forma como são geridos e tratados os incidentes. Será também abordado o tema sobre as ferramentas utilizadas nesta área, como é o caso da ferramenta em análise no presente relatório. No segundo capítulo é efetuado a análise da ferramenta MISP, passando por uma breve introdução à ferramenta, depois a descrição e análise de cada funcionalidade oferecida na plataforma web do MISP, e por fim, esta termina com uma discussão quanto à análise nesta ferramenta. No terceiro capítulo é realizado um estudo comparativo de algumas ferramentas para a partilha de informação de incidentes de segurança informática. Depois de uma breve descrição de cada ferramenta, é feito a sua classificação prosseguindo com uma pequena comparação com as outras ferramentas consoante as suas características as suas características apresentadas. Por fim, o relatório termina no quarto capítulo onde é realizado um levantamento dos objetivos atingidos, a conclusão sobre o trabalho feito, e recomendações futuras.

1. Enquadramento

Uma vez que a temática do presente trabalho se prende com a análise de uma ferramenta com a finalidade de ajudar a combater ameaças e incidentes de segurança informática, neste capítulo, pareceu relevante elaborar os tópicos: a Gestão e Tratamento de Incidentes de Segurança Informática; e as Ferramentas na Gestão de Incidentes de Segurança Informática.

1.1. Gestão e Tratamentos de Incidentes de Segurança Informática

O tratamento de riscos nas organizações é uma área no qual é quase sempre impossível encontrar soluções para todos os riscos encontrados, por este motivo as organizações devem estar sempre prontas para recuperar de desastres ou de incidentes que possa afetar a continuidade do negócio. A gestão e tratamento de incidentes de segurança da informação é a uma forma para lidar com estes problemas, mais concretamente, com a gestão de incidentes esta vai ajudar no planeamento e recuperação da organização contra desastres e no estabelecimento de formas para saber como garantir a continuidade do negócio. Existem vários documentos na qual ajudam a guiar as ações a tomar nesta área de segurança informática, como é o caso do guia de gestão de incidentes da NIST e as normas da família 27000 da ISO, nomeadamente a 27005 para a gestão de risco, 27031 para a continuidade do negócio, e 27035 para a gestão de incidentes. Estes documentos são uma mais valia para ajudar a perceber a forma para definir planos e medidas no combate dos problemas relacionados com incidentes informáticos. Todas estes guias estabelecem um modelo, que de uma forma fundamentalmente são equivalentes, para a gestão e tratamento dos incidentes informáticos. [1]



[2]

Figura 1 - Modelo para gestão de incidentes da NIST

No caso da NIST, o modelo de gestão de incidentes (ver Figura 1) compõe-se em quatro passos: preparação; detecção e análise; contenção, erradicação e recuperação; e atividade pós acidente. O passo da preparação envolve a tomada de medidas e respostas para possíveis incidentes, e na sua prevenção. Isto envolve usar ferramentas e recursos disponíveis para ajudar na comunicação, detecção e resposta aos incidentes, e por vezes a avaliação de risco por parte da equipa de resposta de incidentes. O objetivo destas ferramentas está portanto na preparação contra incidentes de modo a conseguir prevenir uma sobrecarga de incidentes na qual a equipa de resposta a incidentes terá de lidar. [2]

O segundo passo consiste na detecção dos vetores de ataques mais comuns a uma organização. Isto deve-se pela razão que a criação de respostas contra todo o tipo de incidentes ser inviável, e portanto, a melhor resposta será a preparação contra os incidentes provocados pelos vetores de ataque de maior probabilidade em acontecer. Este é um processo que envolve a recolha de fontes sobre precursores e indicadores no qual iram ajudar também na identificação de sinais/sintomas de possíveis incidentes. Por fim é efetuado a análise de incidentes. Como nem todos os precursores e indicadores de incidentes são garantidos ser completamente corretos, a equipa de resposta de incidentes tem de analisar, validar e documentar cada incidente identificado. [2]

No terceiro passo, após o incidente é realizado a sua contenção de modo a evitar causar maiores danos ao negócio da organização. Cada estratégia de contenção depende do tipo de incidente sendo que diferentes tipos de incidentes apresentam critérios de importância diferentes para cada negócio. Assim que o incidente é contido ocorre a recolha e análise das

evidências do incidente. Isto tem como objetivo principal a resolução do incidente para que seja reposto o funcionamento normal do negócio. [2]

Por fim no último passo, depois da resolução de um incidente são exercidas várias atividades, nomeadamente a análise sobre o que aconteceu. Esta é uma das partes mais importantes na resposta a incidentes sendo que esta análise tem como objetivo a aprendizagem do que aconteceu e a partir disso, o aperfeiçoamento contra esse tipo de incidentes. Esta é feita através da análise de *logs* vindos das atividades relativas ao incidente, ou de outros dados recolhidos durante o incidente. Outra atividade, é a retenção das evidências no qual poderá ajudar nos atos judiciais contra o atacante responsável pelo incidente. Com estas atividades concluídas o modelo volta ao passo inicial com vista a melhorar a preparação da organização de acordo com o que foi aprendido pelo incidente. [2]

1.1.1. Ferramentas na Gestão de Incidentes de Segurança Informática

Atualmente o tratamento de incidentes está cada vez mais difícil devido à crescente quantidade de dados recolhidos, e relativo à falta de automatização dos processos que tratam estes dados. Como a escalabilidade desempenha um papel fundamental na manipulação eficaz de incidentes de segurança, o uso de ferramentas que tornem os processos de tratamento de incidentes automáticos, provam ser um grande benefício para as organizações. [3] Existem várias ferramentas que ajudam na gestão e tratamento dos incidentes de segurança, estes de forma resumida estes podem-se dividir em dois grupos: as ferramentas de tratamento de incidentes; e as ferramentas de coordenação e partilha de informação sobre incidentes de segurança informática. [2]

As ferramentas do tratamento de incidentes, envolvem essencialmente vários tipos de softwares que se especializam nos vários passos dos modelos de resposta a incidentes de segurança informática. Estas ferramentas variam desde aplicações para a gestão dos dados resultantes dos incidentes, como é o caso do IntelMQ (que também apresenta uma funcionalidade para coordenação de envio de informação a entidades interessadas) [4] ou o Highlighter [5] para ajudar a gestão e análise de dados dos *logs*. Neste grupo existem também *frameworks* para análises forenses como o PowerForensics [6] e The Volatility [7], ou mesmo aplicações para avaliação de vulnerabilidades, como o Pakiti [8], que apesar desta

não ser uma atividade exercida pela equipa de resposta a incidentes, por vezes a equipa tem de lidar consoante o incidente encontrado.

Depois com o segundo grupo de ferramentas, existem as aplicações e plataformas para auxiliar na partilha de dados e informações sobre os eventos de segurança. [2] Apesar das ferramentas no segundo grupo serem apenas para a partilha da informação, as aplicações como o MISP [9] e o X-Force Exchange [10] da IBM, são das ferramentas mais importantes nas organizações, no qual ajudam tremendamente na preparação contra possíveis incidentes de segurança informático.

Devido à natureza contemporânea das ameaças e ataques que as organizações enfrentam, é cada vez mais importante a partilha de informação entre outras organizações. A coordenação com as outras organizações torna-se num aspeto crucial nas atividades de resposta a incidentes. Isto prova ser essencial na partilha de informação com as diferentes organizações, onde a partilha de informação sobre ameaças, ataques e vulnerabilidades das outras entidades favorece o aumento do conhecimento já acumulado em cada organização. Desta forma, a partilha de informação prova ser um benefício mútuo sendo que um ataque que ocorra numa organização, muito possivelmente irá também acontecer noutra organização. Portanto, o que a partilha de informação vai possibilitar às organizações é o reforço na sua habilidade da resposta eficaz contra os vários tipos de incidentes de segurança informática. [2]

2. MISP

2.1. O que é o MISP?

MISP ou *Malware Information Sharing Platform* (ver Figura 2 - Logotipo do MISP) é um *software* grátis desenvolvido por um grupo de desenvolvedores, este é composto por indivíduos da CIRCL, do departamento de Defesa Belga e da NATO/NCIRC. Este software é uma plataforma para partilha, armazenamento e correlação de “Indicadores de Comprometimento” de ataques com um alvo específico. Apesar do MISP ser uma ferramenta grátis, para obter acesso a esta um utilizador deverá pertencer a uma organização certificada, ou uma CERT credenciada, ou pertencer uma entidade de fornecimento de segurança confiável. Será também necessário possuir uma chave PGP por organização, só então será possível efetuar o registo ao contactando a CIRCL e utilizar por completo o MISP. [11]



[11]

Figura 2 - Logotipo do MISP

Tal como o nome indica, o MISP foca-se na partilha de informação sobre *malware* e dos seus indicadores. Estes podem ser acedidos pela organização onde irá tirar partido da sua informação para melhorar a preparação contra ataques informáticos. O MISP tem vários objetivos, nomeadamente: [11]

- A facilitação do armazenamento de informação técnica e não técnica sobre o *malware* e ataques conhecidos;
- Criação de relações automáticas entre *malware* e os seus atributos;
- Armazenar dados numa forma estruturada, pelo que possibilita a automatização da recolha de dados da base de dados para uso em IDS ou ferramentas forenses;

- Geração de regras para NIDS (*Network Intrusion Detection System*) que podem ser importadas em sistemas de IDS;
- Partilha de características de *malwares* ou ameaças com outras entidades confiáveis;
- Promover a partilha de informação entre organizações para evitar trabalhos duplicados sobre a deteção de novos *malwares*;
- Criar uma plataforma de confiança onde informação credível é obtida a partir de entidades confiáveis;
- E garantir confidencialidade na pesquisa de informação através do armazenamento local de toda a informação das outras instâncias.

O MISP tem a vantagem de obter conhecimento sobre *malwares* ou ameaças conhecidas a partir de fontes confiáveis visto que apenas entidades certificadas ou reconhecidas podem utilizar esta ferramenta. Com isto é possível garantir que as organizações que utilizam o MISP preparem as ações de prevenção e deteção necessárias para combater ameaças iminentes. [11]



Figura 3 - Funcionamento do MISP

Como se pode ver na Figura 3, o funcionamento da ferramenta MISP tira partido de diferentes entradas para interagir com o software, sendo estes a *interface web* e o REST API. Desta forma, um utilizador não é forçado a instalar uma instância do MISP podendo simplesmente usar a opção da API do MISP para a incorporar no seu SIEM, ou IDS da organização. Ao contrário dos utilizadores da API, os utilizadores da *interface web* utilizam a sua própria base de dados local para desempenhar as funcionalidades da plataforma, só realizado o acesso aos recursos externos pela API para exportar ou importar informação sobre novas ameaças. No que toca à partilha de eventos, o MISP oferece quatro opções distintas para a partilha de informação: partilhar apenas dentro da própria organização; partilhar apenas na sua comunidade; partilhar com todas as comunidades ligadas; e partilhar com todas as comunidades. [11]

2.2. Análise das Funcionalidades

Como já foi referenciado anteriormente, o MISP oferece duas formas para interagir com as suas funcionalidades: através da utilização de uma plataforma web de uma instância criada do MISP, instalada localmente; e através da incorporação da REST API do MISP num software de segurança já existente. Por forma a testar as funcionalidades do MISP, a análise desta ferramenta foi realizada usando uma pré-gerada instância do MISP, fornecida para efeitos de testes e de demonstrações da plataforma.

A plataforma web MISP oferece vários tipos de funcionalidades que são desde logo visíveis na página inicial da plataforma como se pode visualizar na Figura 4, as funcionalidades disponíveis são várias: ações para a gestão de eventos de segurança; ações para gerir as *Galaxies*; ações de filtro para os dados que entram e saem da instância; ações globais, tais como a visualização de informações sobre o MISP ou da conta do utilizador; ações de sincronização apenas visíveis pelos administradores; ações de administração; e ações de auditoria visíveis apenas para os utilizadores com permissões de auditoria.

2.2.1 Eventos

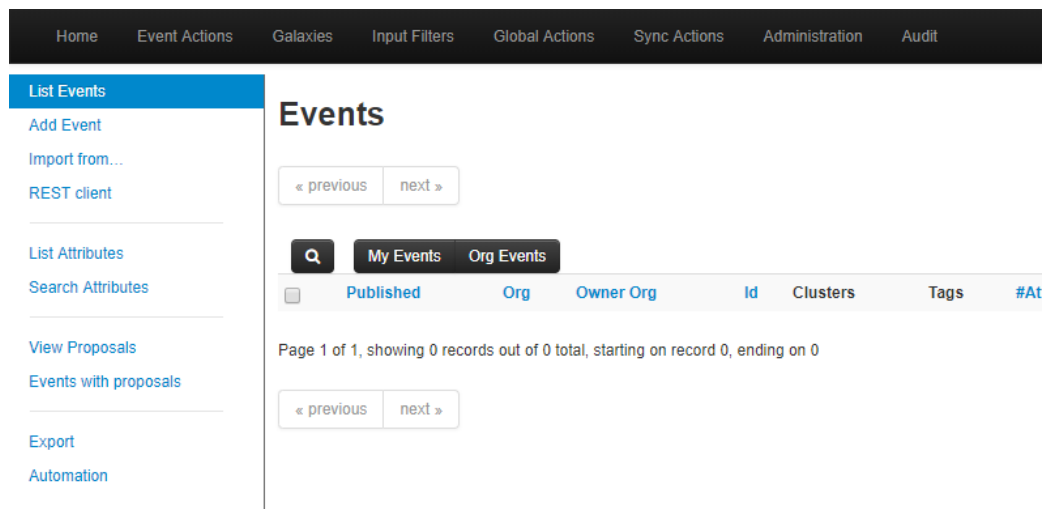


Figura 4 – Barra de navegação da plataforma MISP

Todos os dados de *malware* que entram no MISP vem na forma de um objeto do tipo evento, este é caracterizado principalmente através de atributos. Com os eventos, um utilizador pode exercer vários tipos de ações:

- Listar e adicionar eventos, visível na Figura 5. Ao criar um evento este é inicialmente gerado utilizando apenas informações como a data, o nível de ameaça ou para quem será distribuído o evento. Só depois de criado o evento é que será possível adicionar outras características do evento como atributos, *galaxies*, ou ficheiros;

The screenshot shows the 'Add Event' form. On the left is the same sidebar as in Figure 4, with 'Add Event' highlighted. The form has several fields: 'Date' (2019-03-11), 'Distribution' (This community only), 'Threat Level' (Undefined), and 'Analysis' (Initial). Below these is a text area for 'Event Info' with the placeholder 'Quick Event Description or Tracking Info'. There is also a field for 'Extends event' with the placeholder 'Event UUID or ID. Leave blank if not applicable.' and a blue 'Add' button at the bottom.

Figura 5 - Criação de um evento

- listar e procurar atributos de um evento, estes atributos representam vários aspetos que um *malware* ou evento pode apresentar;
- visualizar propostas, e visualizar eventos com propostas pendentes. As propostas são uma funcionalidade distinta no MISP que permitem outras organizações que não criaram o evento original, propor uma adição ou alteração de atributos no evento original;
- listar e criar *tags*. Como se pode verificar na Figura 6, *tags* são elementos bastantes simples que são compostos por apenas um nome e uma cor, porém, estes podem ser restritos ou não à própria organização ou a um utilizador. As *tags* têm a função de dinamizar e personalizar a listagem dos eventos ao adicionar informação extra, criada pela própria organização;

Figura 6 - Criação de uma Tag

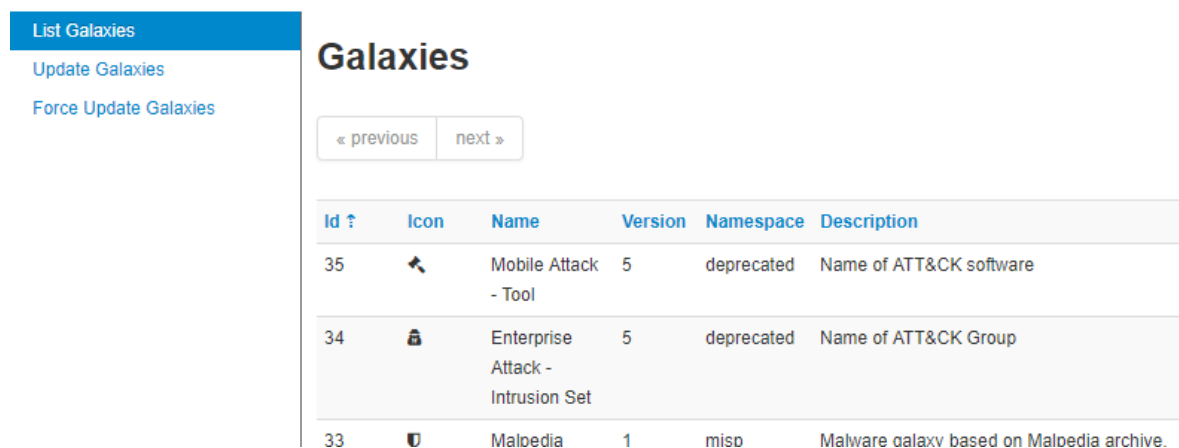
- listar e criar *templates*. *Templates* no MISP são objetos compostos por informação, ficheiros ou atributos que ajudam a preencher um evento. Por exemplo na Figura 7, depois de criado um evento, MISP oferece a opção de “popular” o evento a partir de um *template*;

Figura 7 - Utilização de *templates* no MISP

- exportar dados em vários formatos. A funcionalidade de exportar tem o objetivo de gerar automaticamente assinaturas para sistemas de detecção de intrusos, isto aplica-se a eventos e a atributos;
- e por fim a opção de automatização. Esta funcionalidade tem como objetivo o auxílio ao acesso do repositório da MISP através da utilização das funcionalidades REST. Esta funcionalidade é essencialmente igual à funcionalidade de exportar, no entanto, a diferença é que na opção de automatizar este processo através do API do MISP, está apenas disponível para aqueles que possuam uma chave de autenticação.

2.2.2. Galaxies

No MISP *galaxies* são a forma de demonstrar objetos grandes, também denominados como clusters. *Galaxies* podem ser constituídos para um ou mais elementos e podem ser usados como características de eventos ou de atributos. Ao contrário de eventos ou de *templates*, *galaxies* são vocabulários disponibilizados pela MISP que só podem ser atualizados ou trocados por vocabulários de diferentes normas para informação de ameaças.



Id ↑	Icon	Name	Version	Namespace	Description
35		Mobile Attack - Tool	5	deprecated	Name of ATT&CK software
34		Enterprise Attack - Intrusion Set	5	deprecated	Name of ATT&CK Group
33		Malpedia	1	miso	Malware galaxy based on Malpedia archive.

Figura 8 - Listagem de *galaxies*

Galaxies podem ser visualizadas na sua própria secção onde o utilizador poderá então atualizar as *galaxies* no qual o MISP disponibiliza. Como se pode ver na Figura 8, as *galaxies* têm várias características como por exemplo o *namespace* que indica o grupo no qual pertence uma *galaxy*, a descrição que serve de indicador de onde vem esta *galaxy*. Depois, na Figura 9 é possível visualizar na tabela abaixo da informação da *galaxy* os vários tipos de ocorrências registadas pertencentes a esta.

Mobile Attack - Tool galaxy

Galaxy ID	35
Name	Mobile Attack - Tool
Namespace	deprecated
Uuid	1d0b4bce-1708-11e8-9e6e-1b130c9b0a91
Description	Name of ATT&CK software
Version	5

« previous next »

Value ↓	Synonyms	Activity	#Events	Description
Xbot - MOB-S0014	Xbot		0	Xbot is a family of Android malware analyzed by Palo Alto Networks (Citation: PaloAlto-Xbot) that "tries to steal victims' banking credentials and credit card information", "can also remotely lock infected Android devices, encrypt the user's files in external storage (e.g., SD card), and then ask for a U.S. \$100 PayPal cash card as ransom" and "will steal all SMS message and contact information, intercept certain SMS messages, and parse SMS messages for mTANs (Mobile Transaction Authentication Number) from banks." Aliases: Xbot

Figura 9 - Vista detalhada de uma *galaxy*



2.2.3. Filtros

A funcionalidade para filtrar dados no MISP possibilita alterar quais e como os dados podem entrar e sair numa instância do MISP. Como alternativa à validação da entrada de dados por género, o MISP oferece também uma forma mais elaborada de validação de dados aos administradores. Administradores podem definir uma lista de expressões regulares (ver Figura 10) que permite alterar certos valores e também bloquear certos valores durante a exportação dos dados. Caso um administrador necessite de importar expressões regulares, o MISP oferece também essa funcionalidade para suplementar a funcionalidade de filtragem.

Signature Whitelist

Regex entries (in the standard php regex `/[regex]/[modifier]` format) entered below will restrict matching attributes from being included in the IDS flag sensitive exports (such as NIDS exports).

« previous next »

Id	Name ↓	Actions
1	/8.8.8.8/	 

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

« previous next »

Figura 10 - Lista de expressões regulares

Para além de bloquear certos valores de serem inseridos, expressões regulares podem também ajudar na filtragem de informação pessoal dos *imports* automáticos como os *usernames* dos *paths* de ficheiros.

O MISP oferece também juntamente com os filtros duas listas: a “warninglists”, uma lista de indicadores bem conhecidos e associados a potenciais falsos positivos ou erros; e a “noticelists”, uma lista que informa utilizadores do MISP sobre as implicações legais de privacidade, políticas e técnicas ao usar atributos, categorias ou objetos específicos. Exemplo disto é o GDPR como se pode ver na Figura 11.

Noticelists

« previous

next »

Id	Name	Expanded Name	ref	geographical_area	version	enabled	Actions
1	gdpr	General Data Protection Regulation	http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679	EU	1	<input type="checkbox"/>	

Figura 11 – Lista de Noticelists

2.2.4. Ações globais

A plataforma web do MISP permite realizar operações gerais para a gestão da conta do utilizador, tais como a visualização e alteração do perfil de utilizador. É também dentro das ações globais que um utilizador poderá aceder a informação sobre o MISP como o manual de utilizador, as notícias, termos de utilizador e a lista e histograma das contribuições feitas por organizações ativas na presente instância.

2.2.5. Ações de Sincronização

A funcionalidade de sincronização no MISP, que é apenas acessível pelos administradores, permite gerir a lista de instâncias ligadas e iniciar a sincronização de dados destas instâncias com a sua. Existe também uma lista de *feeds* que o MISP disponibiliza na plataforma, esta lista consiste em indicadores que vêm de URLs remotos ou locais. Como se pode ver na Figura 12, é possível adicionar *feeds* adicionais à lista como também importar e exportar *feeds* em formato JSON.

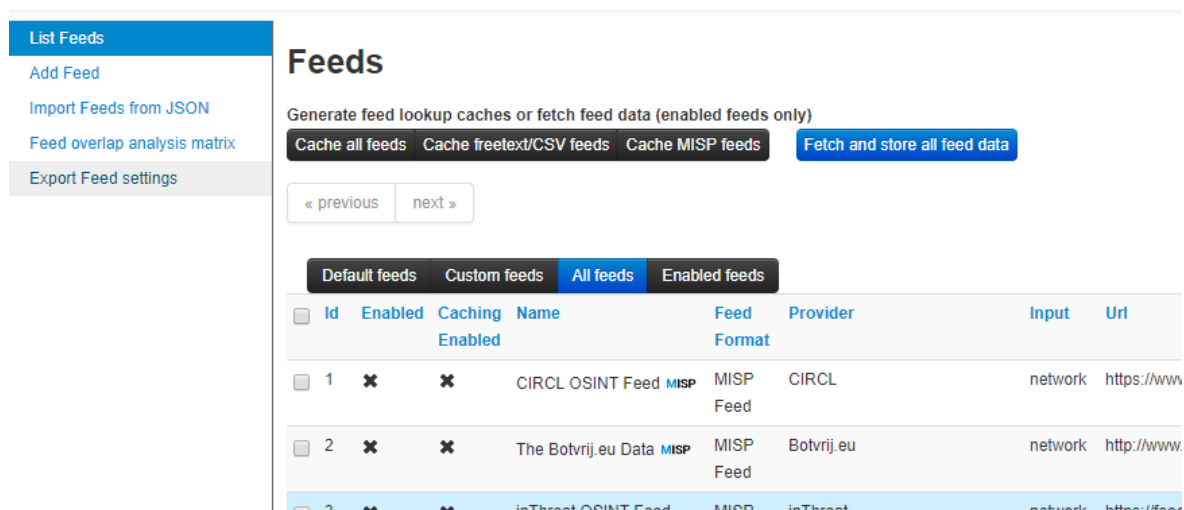


Figura 12 - Gestão de feeds

2.2.6. Administração

Para a administração da plataforma, MISP oferece funcionalidades de administrador como adicionar, editar e remover contas de utilizadores e *roles* de utilizador. Os *roles* definem os direitos de acesso a certas funcionalidades tais como a publicação de eventos, a utilização da interface de REST ou da sincronização de utilizadores com o mesmo *role*. Também é oferecido as funcionalidades aos administradores para efetuarem *reset* a passwords dos utilizadores e de entrarem em contacto com estes via emails encriptados.

É oferecido a opção “*Scheduled Tasks*”, que são essencialmente scripts executados numa certa data e hora, e várias ferramentas de diagnose e de manutenção da instância do MISP. Também, dentro destas opções de administração, existe a possibilidade de gerir uma *blacklist* de eventos e uma para organizações no qual não se queira receber dados (ver Figura 13).

Add User

List Users

Contact Users

Add Organisation

List Organisations

Add Role

List Roles

Server Settings & Maintenance

Jobs

Scheduled Tasks

Blacklists Event

Manage Event Blacklists

Blacklists Organisation

Manage Org Blacklists

Organisation Blacklists

« previous

next »

Id	Org Name	Org Uuid
1	Setec Astronomy	58d38339-7b24-4386-b4b4-4c0f9
2	Acme Finance	58d38326-eda8-443a-9fa8-4e129

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, e

« previous

next »

Figura 13 - Menu de opções para administração

2.2.7. Auditoria

A funcionalidade de auditoria é uma das ferramentas dos administradores que não se enquadra na gestão da plataforma mas sim, na administração da organização em si.

Search Logs

Email

Organisation

Model

Model ID

Action

Title

Change

Search

Figura 14 - Formulário de pesquisa de um log específico

Tal como outras ferramentas para auditoria, o MISP possibilita a visualização de *logs* de forma geral e de forma específica tanto da própria organização ou de outra que esteja presente na lista de dados da instância. Na Figura 14 é possível ver o nível de especificidade existente na pesquisa de *logs* no MISP, nesta pesquisa é possível procurar *logs* por cada um dos campos no qual os *logs* estão organizados, como por exemplo a organização e o tipo de *log*.

2.3. Discussão

MISP é um projeto que procura automatizar e facilitar a partilha de informação sobre eventos da segurança informática, o que a sua plataforma web, fornece exatamente esse objetivo. Após a análise das várias funcionalidades disponíveis na plataforma web, facilmente se chega à conclusão que esta plataforma, apesar de se apresentar com um aspeto simples, fornece todas as funcionalidades necessárias para a gestão de incidentes de segurança de forma gratuita. E ainda adiciona funcionalidades extras como as notícias, fóruns para discussões dentro da organização, várias listas de indicadores de ameaças, e as *galaxies* que suplementam as fontes de dados principais utilizadas pela organização.

Como ferramenta de partilha de informação de incidentes, naturalmente a funcionalidade de criação e gestão de eventos é um dos focos principais do MISP. O nível de detalhe disponibilizado na plataforma para criar os eventos é extremamente alta, sendo que é possível atribuir vários tipos de características, atributos e informações ao evento no qual ajudam na compreensão de coisas como o estado, o nível, e de outros pequenos pormenores de um evento. Para além disto, é também disponibilizado várias opções na forma como acrescentar a informação e estatísticas ao evento. Exemplo disto são os *templates*, as *galaxies*, os ficheiros relacionados com o evento e as *tags*. Este fornece também diferentes formas de publicação de um evento, para depois partilhar entre outras organizações, e opções para importar eventos na instância. Mas, com as *proposals* do MISP, este será certamente a funcionalidade que mais torna a ferramenta interativa para ser utilizada entre entidades. Com as *proposals* é possível uma organização externa, que não tenha os direitos de alteração de um evento, propor uma alteração ou adição de dados a um evento.

As *galaxies* são uma particularidade do MISP que vem suplementar os atributos usados nos eventos. Como as *galaxies* são essencialmente atributos mas na realidade são objetos grandes, estas apresentam uma grande utilidade no que toca na obtenção de informação sobre *malwares* ou ameaças vindo de fontes respeitadas. Estas fontes são por exemplo base de

dados como o ATT&CK, que partilham dados sobre ameaças de forma organizada e estruturada.

A funcionalidade para filtrar os dados que entram e saem da instância é uma grande ajuda, isto para evitar a entrada de dados que a organização pondere ser desnecessário na sua gestão de incidentes. Esta é também útil na prevenção da fuga de dados cuja a exposição externa possa prejudicar a privacidade e confidencialidade da informação da organização durante a importação de dados automáticas, aqui a lista de expressões regulares, *Signature Whitelist*, possibilita trocar ou eliminar certos valores encontrados nos dados.

Como no presente relatório foi feito um foco na análise da plataforma web do MISP, a análise do REST API foi impossível de realizar porque era necessário um utilizador da API realizar o registo na CIRCL e possuir uma chave de autenticação. Apesar disto é possível discutir os benefícios da utilização da API. Tal como na plataforma web, é possível tirar partido das funcionalidades principais do MISP. Isto significa que para utilizar o MISP, uma organização não é obrigada a efetuar a instalação da plataforma web da MISP, podendo simplesmente incorporar as funcionalidades de partilha de incidentes da MISP no seu sistema de gestão de incidentes de segurança informática utilizando a API da MISP. Este diferente modo de utilização da MISP é uma vantagem do ponto de vista do utilizador que não usufrua de poucos recursos para gerir outra plataforma juntamente com as que já existem na sua organização. É também uma vantagem, o facto de muitas dos softwares de gestão de incidentes possuírem um modo opcional para aceder às funcionalidades da ferramenta.

Apesar do aspeto simples do MISP, as suas funcionalidades e modos de utilização, tornam esta ferramenta numa mais valia para qualquer tipo de organização. Certamente, a qualidade mais benéfica que esta ferramenta oferece é o quantidade de detalhe disponível para os eventos/incidentes. As caraterísticas como os atributos, *galaxies*, *templates*, ficheiros relacionados e informação em formato texto tornam o MISP numa ferramenta extremamente flexível, e que qualquer organização pode tirar partido na sua segurança informática. As funcionalidades extras que a plataforma web disponibiliza, como as discussões, notícias e as ações de sincronização oferecem uma boa interatividade entre utilizadores da mesma organização.

3. Estudo Comparativo

Como já foi discutido, MISP é uma ferramenta simples mas que oferece funcionalidades suficientes para classificá-la como uma ferramenta eficaz e útil, mas como é que esta se compara com outras ferramentas do mesmo género.

X-Force Exchange é uma plataforma de partilha de informação de ameaças da IBM, e este pode ser usado para investigação de ameaças de segurança, acumulação de dados e colaboração com parceiros de negócio. O X-Force Exchange (ver Figura 15) é uma ferramenta simples, fácil de compreender e extremamente acessível para utilização sendo que esta é uma plataforma baseada na *cloud* e não necessita de instalação como a do MISP. Esta ferramenta é bastante parecida com o MISP no que toca na gestão de eventos/incidentes, ambas permitem criar este tipo de objetos com grande opção para detalhe. [10]

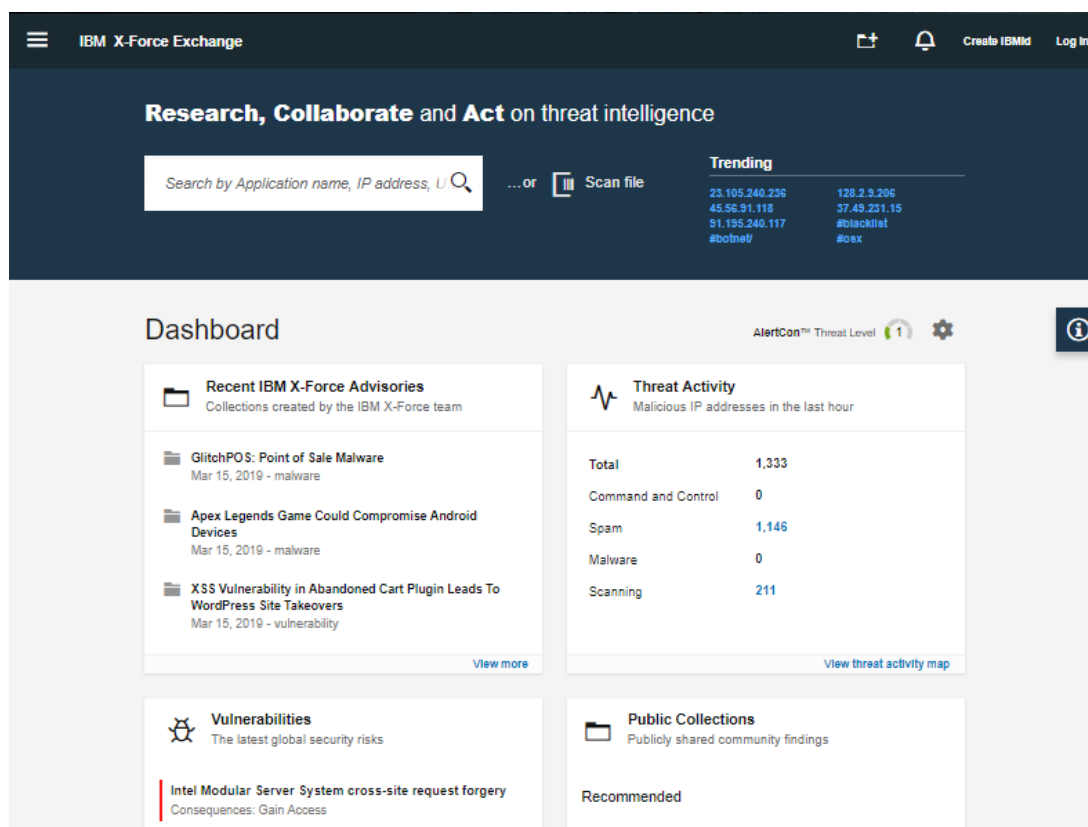


Figura 15 - IBM X-Force Exchange Dashboard

RTIR, *Request Tracker for Incident Response*, tem como base as funcionalidades do *Request Tracker*, por este motivo o RTIR é uma ferramenta que tem como foco mais o tratamento e resposta a incidentes do que na partilha da informação de incidentes. RTIR apresenta funcionalidades para correlacionar dados dos relatórios de incidentes e para

encontrar padrões no qual poderão guiar à causa dos incidentes. Este apresenta também a funcionalidade de partilha de informação com outras entidades, nomeadamente a gestão de comunicação com várias entidades interessadas ou em colaboração na determinação de contramedidas. Como se pode visualizar na Figura 16, o funcionamento do RTIR segue os princípios do modelo de tratamento de incidentes mas com partilha de dados dos incidentes apenas às entidades interessadas. [12]

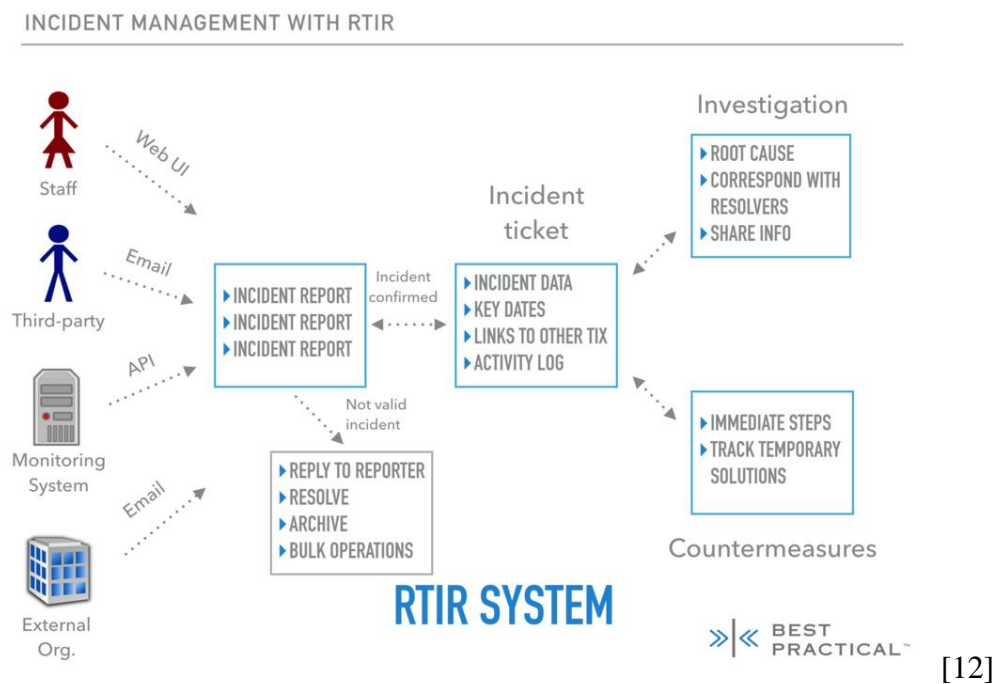


Figura 16 - Funcionamento do RTIR

Ao comparar estas ferramentas segundo as suas características e formas de funcionamento na Tabela 1, é possível concluir que o MISP, apesar de necessitar de mais conhecimento para instalar uma instancia, esta é a que oferece mais funcionalidades tanto através da sua plataforma web ou incorporando o seu REST API numa aplicação já existente. A X-Force Exchange não fica muito atrás do MISP sendo que apesar de expor não tantas funcionalidades no modo gratuito que o MISP, esta é definitivamente uma boa alternativa para uma organização que não tenha recursos ou conhecimentos necessárias para efetuar a instalação de uma ferramenta como o MISP, ou que tenha a disponibilidade económica para escolher entre várias edições do X-Force Exchange oferecida pela IBM. O RTIR por outro lado, não é muito proveitoso como uma plataforma de partilha de dados de ameaças, esta centra-se mais na área da investigação e resposta a incidentes do que em vez da partilha e gestão de eventos de segurança informática. Ela tem apenas como funcionalidade de partilha

de informação a coordenação e comunicação com entidades interessadas o que não se compara com as funcionalidades oferecidas pelas outras.

Tabela 1 - Comparação de ferramentas

	Local de Execução	Partilha de Informação	Funcionalidades Principais	Modo de utilização	Instalação
MISP	Local	Entidades específicas; Qualquer entidade na comunidade	Gestão e partilha de eventos; Atributos; Templates; Filtros; etc.	Grátis mas requer registo e chave de autenticação	Requer instalação num servidor ou incorporação da API
RTIR	Local	Entidades específicas	Tratamento, investigação e resposta a incidentes; e comunicação de incidentes	Grátis	Requer instalação
X-Force Exchange	<i>Cloud</i>	Entidades específicas	Gestão e partilha de eventos;	Modo Grátis e Modo Pago	Não requer instalação

4. Conclusão

O presente relatório tinha como objetivos principais: o estudo e análise da ferramenta MISP; e a comparação de outras ferramentas com o MISP. Estes objetivos foram alcançados sendo que foi possível utilizar a plataforma web do MISP através de uma instância criada para ambiente de teste. Aqui foram analisadas as várias funcionalidades oferecidas, nomeadamente a criação de eventos, *templates*, atributos e filtros, a utilização de atributos, *galaxies* e outras informações para adicionar a eventos criados. Com o estudo do MISP, foi possível proporcionar um melhor entendimento das ferramentas de partilha de informação de ameaças como também, perceber as vantagens do MISP em relação a outras ferramentas com o X-Force Exchange.

O conceito da partilha de informação de ameaças não é algo de novo no mundo da segurança, mas as ferramentas desta área são uma absoluta necessidade para qualquer organização que pretenda ganhar qualquer tipo de vantagem na preparação contra incidentes de segurança informática. A utilização de plataformas como o MISP, que facilita a partilha de relatórios de incidentes entre várias organizações, ajuda a reforçar o primeiro passo no modelo de tratamento de incidentes. Este é o passo de preparação, que irá permitir às organizações que ainda não tenha sido afetadas por uma ameaça, precaver contra essa ameaça. Desta forma, considero que o MISP seja uma das opções mais atrativas, sendo esta uma ferramenta extremamente forte para a criação de boas base de dados, compostas por indicadores de risco de incidentes tanto com informação técnica e não técnica. Também, pelo facto do MISP oferecer várias formas de utilizar de modo gratuito.

Para concluir, uma recomendação para trabalho futuro seria melhorar a análise realizada do MISP através do estudo do API incorporado nas ferramentas de segurança utilizadas pelas organizações. Sendo que não foi possível adquirir o acesso a uma ferramenta com estas características, obter uma destas seria uma oportunidade para melhor analisar as funcionalidades disponibilizadas pelo MISP no seu API.

Referências

- [1] INFOSEC Institute, “CISSP Domain 1: Security And Risk Management-What You Need To Know For The Exam,” [Online]. Available: <https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/#gref>. [Acedido em 1 3 2019].
- [2] NIST, “Computer Security Incident Handling Guide,” [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>. [Acedido em 3 3 2019].
- [3] ENISA, “Incident Handling Automation,” [Online]. Available: <https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation>. [Acedido em 6 3 2019].
- [4] CertTools, “IntelMQ,” [Online]. Available: <https://github.com/certtools/intelmq>. [Acedido em 4 3 2019].
- [5] FireEye, “Highlighter,” [Online]. Available: <https://www.fireeye.com/services/freeware/highlighter.html>. [Acedido em 4 3 2019].
- [6] PowerForensics, “PowerForensics,” [Online]. Available: <https://powerforensics.readthedocs.io/en/latest/>. [Acedido em 4 3 2019].
- [7] Volatility Foundation, “The Volatility,” [Online]. Available: <https://www.volatilityfoundation.org/>. [Acedido em 4 3 2019].
- [8] Cesnet, “Pakiti,” [Online]. Available: <https://github.com/CESNET/pakiti-server>. [Acedido em 4 3 2019].
- [9] MISP project, “MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing,” [Online]. Available: <https://www.misp-project.org/index.html>. [Acedido em 4 3 2019].

- [10] IBM, “X-Force Exchange,” IBM, [Online]. Available: <https://exchange.xforce.ibmcloud.com/>. [Acedido em 17 3 2019].
- [11] CIRCL, “Malware Information Sharing Platform (MISP) - A Threat Sharing Platform,” [Online]. Available: <https://www.circl.lu/services/misp-malware-information-sharing-platform/>. [Acedido em 9 3 2019].
- [12] BestPractical, “Request Tracker for Incident Response,” BestPractical, [Online]. Available: <https://bestpractical.com/rtir>. [Acedido em 17 3 2019].