MISP

Entendendo o propósito da plataforma e adaptando seu uso para as necessidades de sua organização.

Whoami

Carlos Borges

Sr. Cyber Analyst na Câmara Interbancária de Pagamentos - CIP

Twitter: @huntingneo

Github/Medium: @hackunagi

Linkedin: @carlosavborges

Contribuidor do projeto MISP, Mitre ATT&CK e outros projetos open source.

Criei um workshop sobre MISP com abordagem prática.

Meus Objetivos

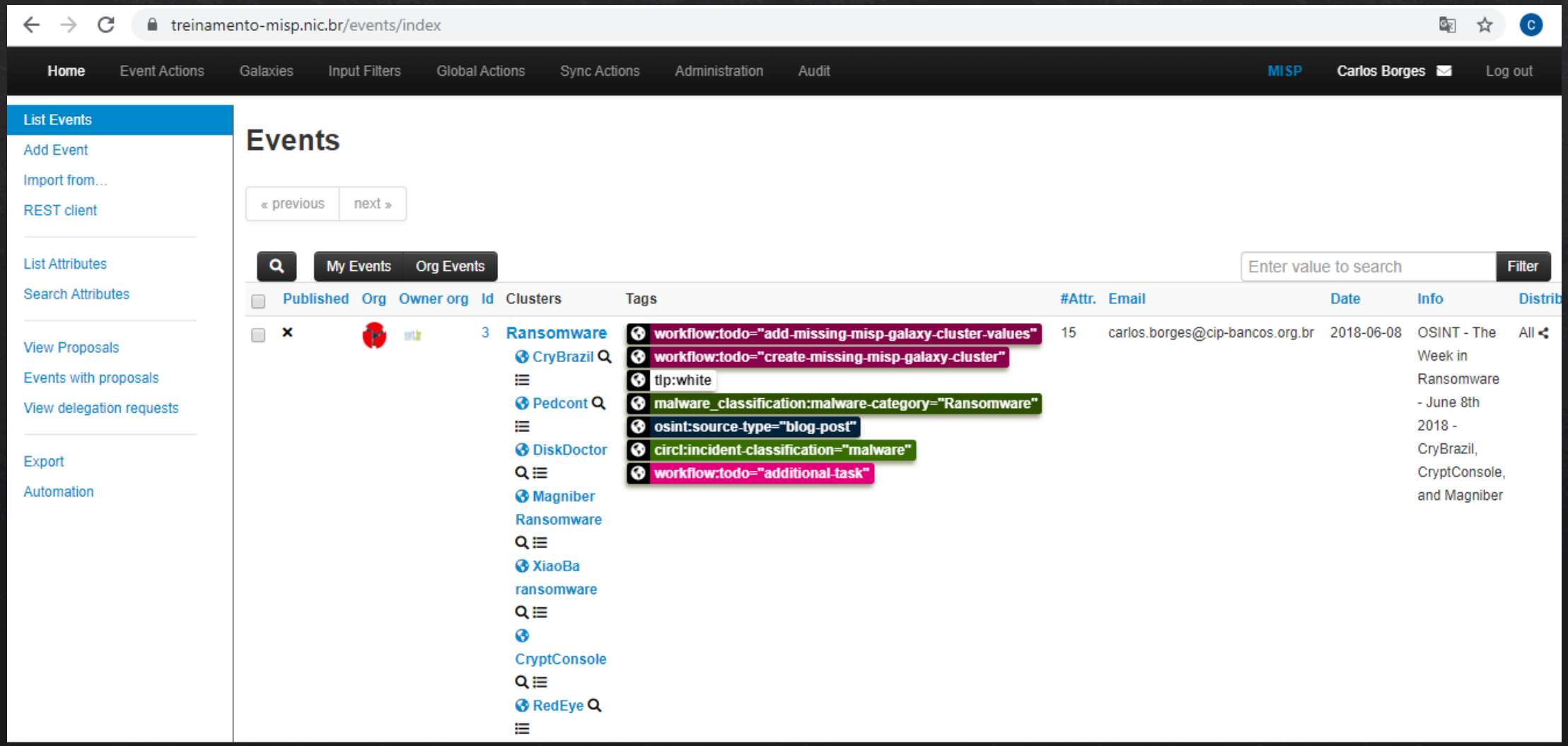
- Mostrar como a plataforma pode ajudar a melhorar a estratégia de defesa cibernética da sua organização.

- Ponto de vista prático sobre o uso da plataforma, seja com ideias ou funcionalidades.

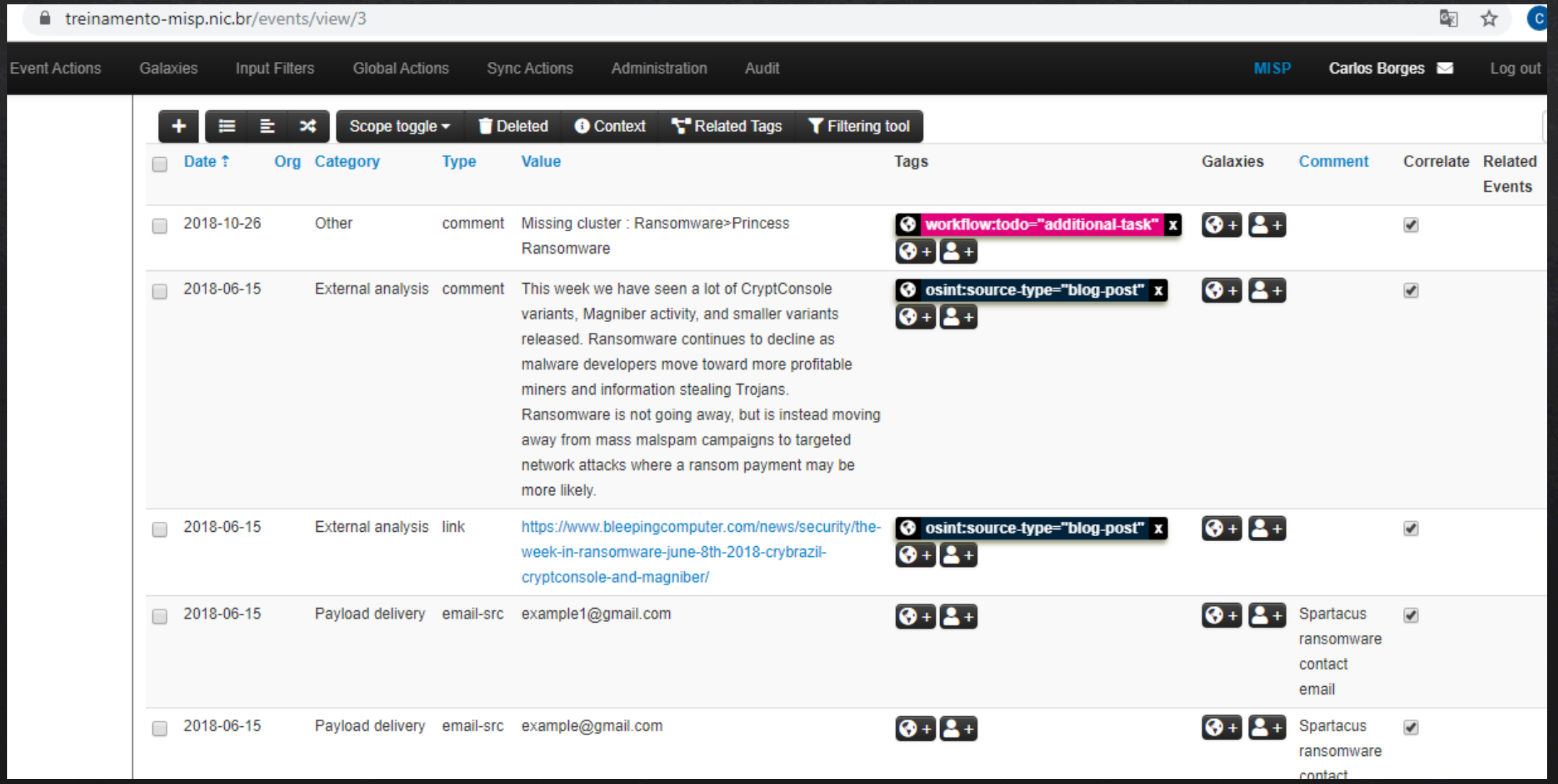
O que é o MISP?

- Malware Information Sharing Platform (MISP).
- Open source.
- Várias formas de se contribuir com o projeto.
- Compartilhamento, armazenamento e correlacionamento de indicadores sobre ameaças.

O que é o MISP?


treinamento-misp.nic.br/events/index
Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Carlos Borges
Log out
List Events
Add Event
Import from...
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation
Events
« previous
next »
My Events
Org Events
Enter value to search
Filter
Published
Org
Owner org
Id
Clusters
Tags
#Attr.
Email
Date
Info
Distrib
3
Ransomware
CryBrazil
Pedcont
DiskDoctor
Magniber Ransomware
XiaoBa ransomware
CryptConsole
RedEye
workflow:todo="add-missing-misp-galaxy-cluster-values"
workflow:todo="create-missing-misp-galaxy-cluster"
tlp:white
malware_classification:malware-category="Ransomware"
osint:source-type="blog-post"
circl:incident-classification="malware"
workflow:todo="additional-task"
15
carlos.borges@cip-bancos.org.br
2018-06-08
OSINT - The Week in Ransomware - June 8th 2018 - CryBrazil, CryptConsole, and Magniber
All

O que é o MISP?


treinamento-misp.nic.br/events/view/3
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Carlos Borges
Log out
Scope toggle
Deleted
Context
Related Tags
Filtering tool
Date
Org
Category
Type
Value
Tags
Galaxies
Comment
Correlate
Related Events
2018-10-26
Other
comment
Missing cluster : Ransomware>Princess Ransomware
workflow:todo="additional-task"
2018-06-15
External analysis
comment
This week we have seen a lot of CryptConsole variants, Magniber activity, and smaller variants released. Ransomware continues to decline as malware developers move toward more profitable miners and information stealing Trojans. Ransomware is not going away, but is instead moving away from mass malspam campaigns to targeted network attacks where a ransom payment may be more likely.
osint:source-type="blog-post"
2018-06-15
External analysis
link
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
osint:source-type="blog-post"
2018-06-15
Payload delivery
email-src
example1@gmail.com
Spartacus ransomware contact email
2018-06-15
Payload delivery
email-src
example@gmail.com
Spartacus ransomware contact

Principais valores do projeto

The key is Automation

Isn't it sad to have a lot of data and not use it because it's too much work? Thanks to MISP you can store your IOCs in a structured manner, and thus enjoy the correlation, automated exports for IDS, or SIEM, in STIX or OpenIOC and synchronize to other MISPs. You can now leverage the value of your data without effort and in an automated manner.
Check out MISP features.

Simply Threats

The primary goal of MISP is to be used. This is why simplicity is the driving force behind the project. Storing and especially using information about threats and malware should not be difficult. MISP is there to help you get the maximum out of your data without unmanageable complexity.

By giving you will receive

Sharing is key to fast and effective detection of attacks. Quite often similar organisations are targeted by the same Threat Actor, in the same or different Campaign. MISP will make it easier for you to share with, but also to receive from trusted partners and trust-groups. Sharing also enabled collaborative analysis and prevents you from doing the work someone else already did before.
Join one of the existing MISP communities.

Reflexão
Como foi seu primeiro contato o MISP?

- Viu alguma apresentação sobre a plataforma?
- Como foi a implantação?
- Como estava alinhado à estratégia de Defesa?

Minha visão

- Mudou muito com o tempo.
- Entender como o MISP pode ser utilizado na organização também é um caso de entender como nossa área muda e evolui com o tempo.
- Defesa em profundidade, prevenção, hardening, detecção e resposta, evolução das tecnologias de segurança, melhores práticas, frameworks, modelos, red team, blue team, CTI, etc.

Principais elementos para toda organização

- Threat model
- Collection framework
- Intelligence requirements (CTI).

[7] GCTI SANS Certification.

Cyber Threat Intelligence?

- É algo complicado de ser definido, até mesmo por profissionais de referência na área.

Intelligence Defined and its Impact on Cyber Threat Intelligence

August 25, 2016

Michael Cloppert wrote a great piece to argue for a new definition of cyber threat intelligence. The blog is extremely well written (I personally love the academic style and citations) and puts forth a good discussion on operations. Sergio Caltagirone published a rebuttal equally valuable where he agreed with Mike that there is accuracy missing from current cyber threat intelligence definitions but noted that Mike focused too much on operations. The purpose of this blog is not to rebut their findings but to add to the conversation. In many aspects I agree with both Mike and Sergio; I would highlight that the forms of intelligence discussed though are very policy focused (sometimes even military focused) and influence how we define cyber threat intelligence. I do not envision that between these three blogs we've settled a long standing debate on intelligence but the intent is to add to the discussion and encourage thoughts by others.

[1] Discussão sobre definição de CTI

Cyber Threat Intelligence?

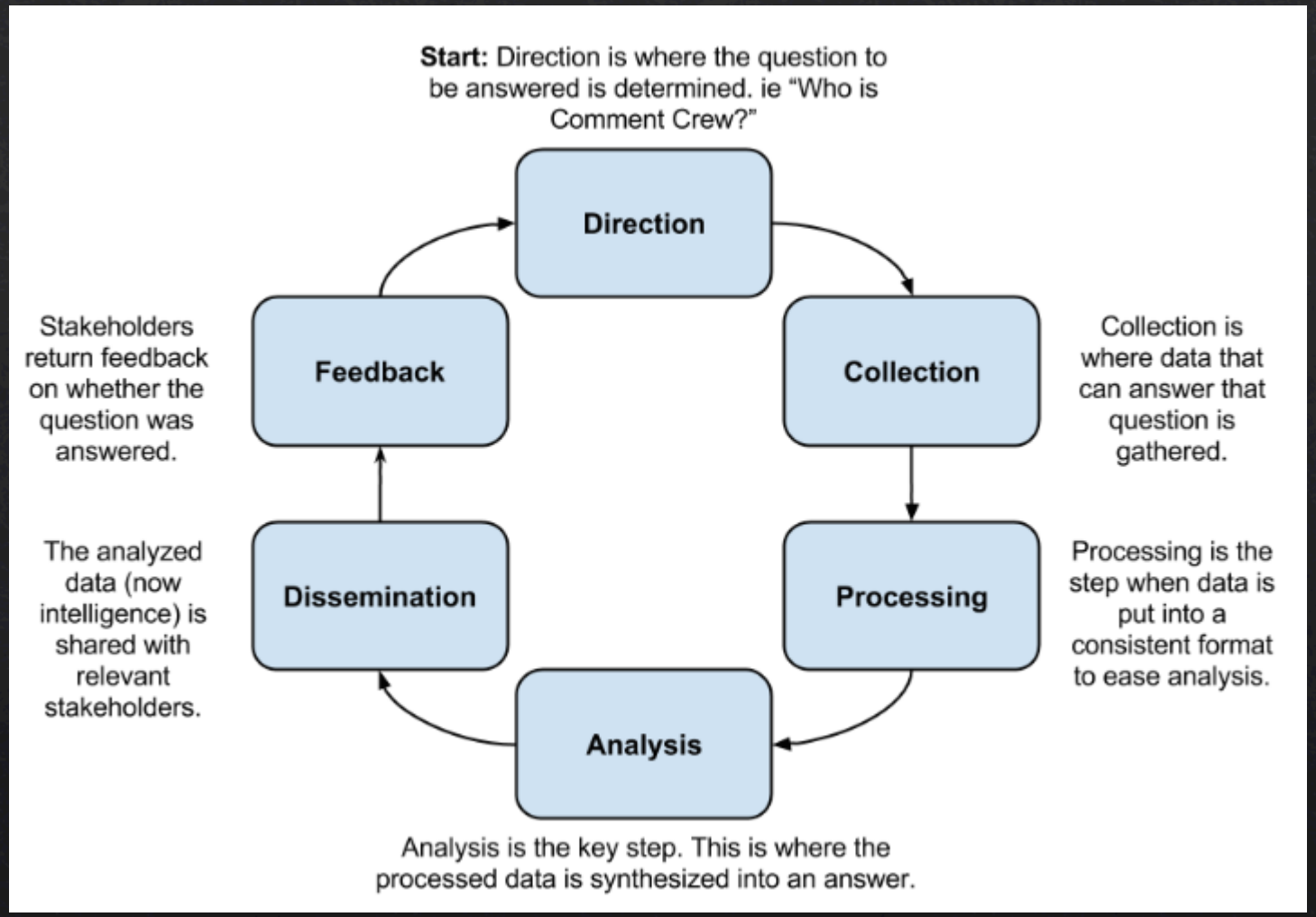
- Por questões de simplicidade, o próprio Robert M. Lee, define como:

"The process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm."

Cyber Threat Intelligence?

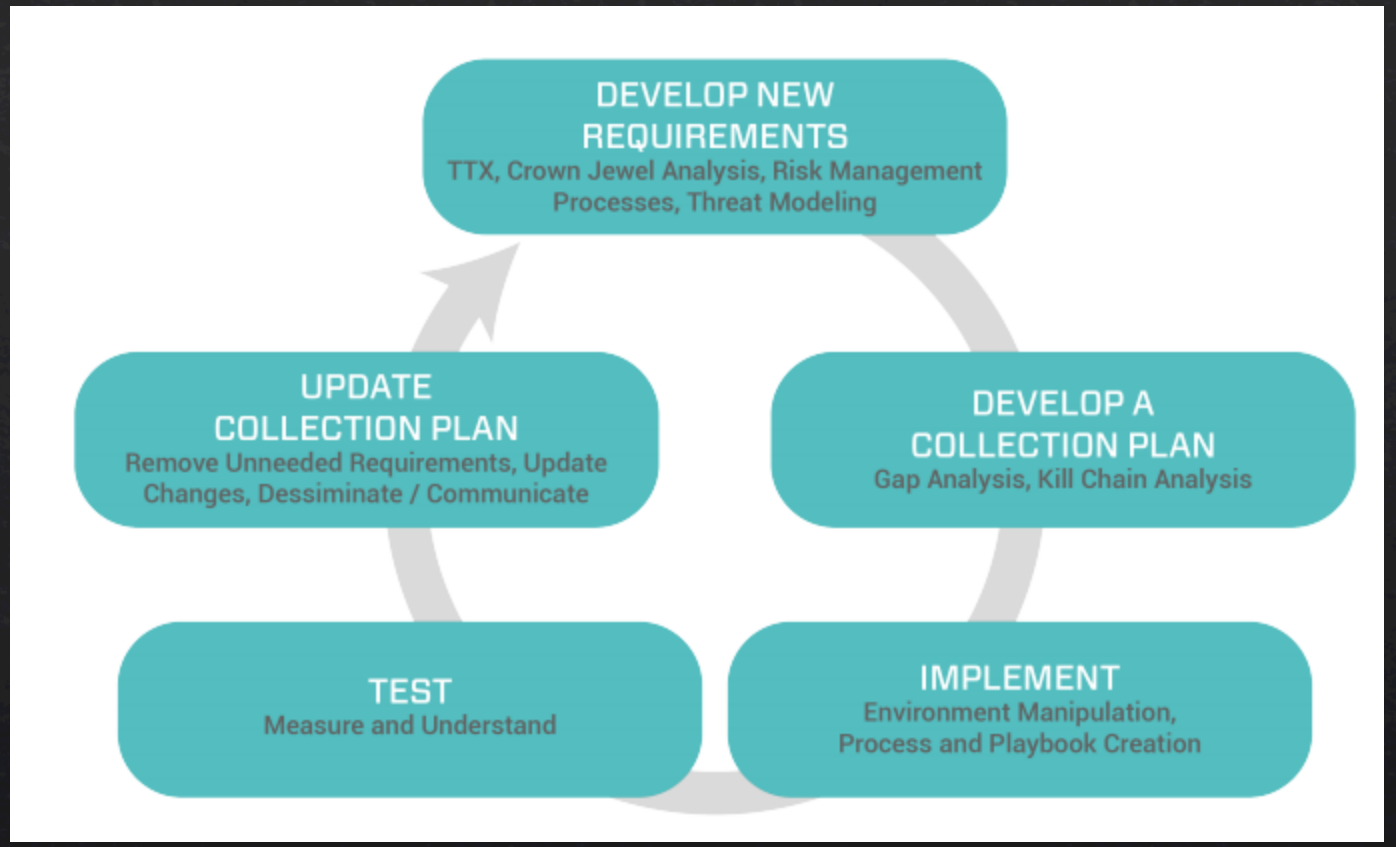
- Essa definição vem com aspectos importantes.
- Temos uma definição do que é ameaça.
- Sempre temos um adversário.
- O entendimento que a análise de dados é importante.
- E o mais importante, temos os REQUISITOS (Driven by).

Ciclo de CTI – 1° caso de uso



[3] Processo de CTI Sugerido

Collection Framework



[8] Logs Collection Framework. Dragos. https://github.com/hackunagi/Logsspot

Collection Framework

github.com/MISP/MISP/blob/2.4/app/Model/Attribute.php

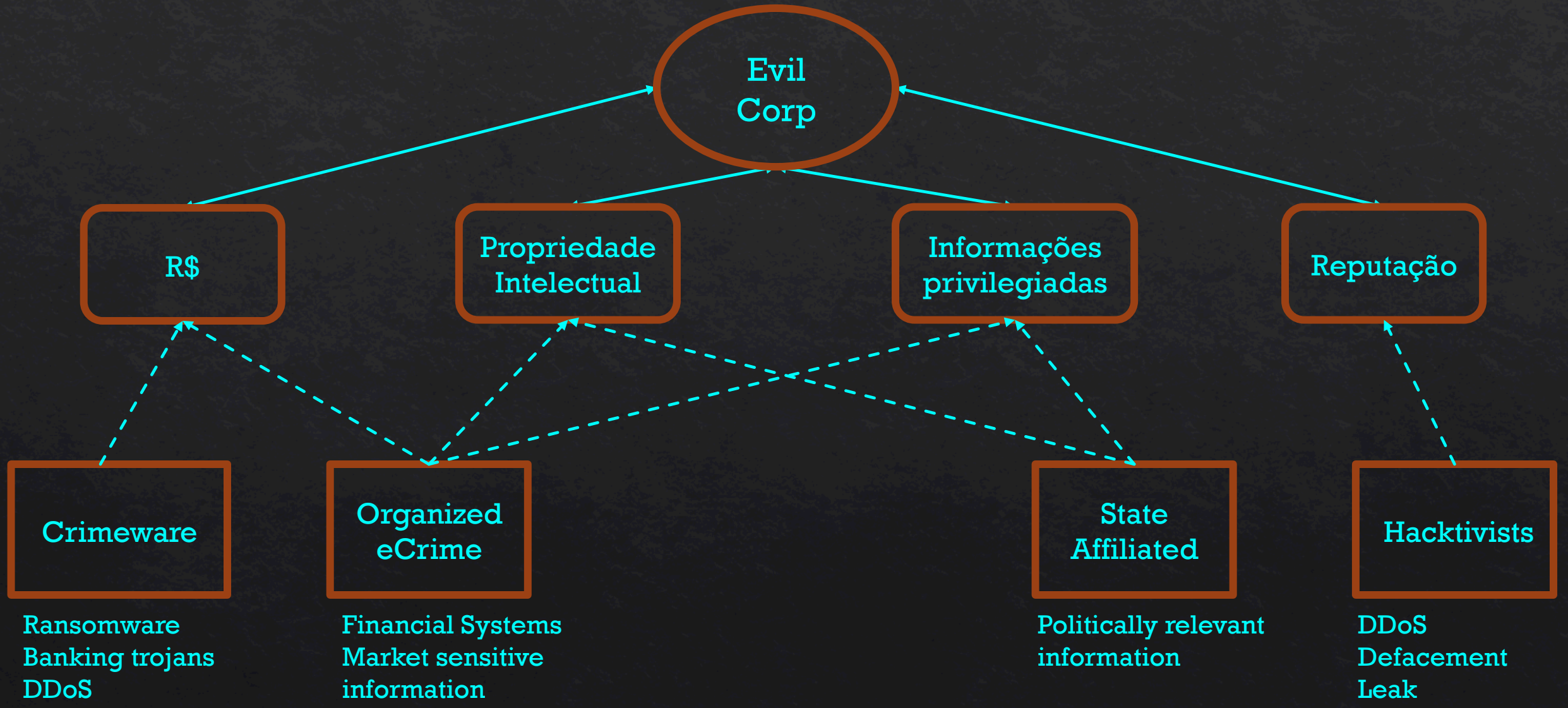
```
//
$this->typeDefinitions = array(
    'md5' => array('desc' => __('A checksum in md5 format'), 'formdesc' => __("You are encouraged to use filename|md5 instead. A c
    'sha1' => array('desc' => __('A checksum in sha1 format'), 'formdesc' => __("You are encouraged to use filename|sha1 instead.
    'sha256' => array('desc' => __('A checksum in sha256 format'), 'formdesc' => __("You are encouraged to use filename|sha256 ins
    'filename' => array('desc' => __('Filename'), 'default_category' => 'Payload delivery', 'to_ids' => 1),
    'pdb' => array('desc' => __('Microsoft Program database (PDB) path information'), 'default_category' => 'Artifacts dropped', '
    'filename|md5' => array('desc' => __('A filename and an md5 hash separated by a |'), 'formdesc' => __("A filename and an md5 h
    'filename|sha1' => array('desc' => __('A filename and an sha1 hash separated by a |'), 'formdesc' => __("A filename and an sha
    'filename|sha256' => array('desc' => __('A filename and an sha256 hash separated by a |'), 'formdesc' => __("A filename and an
    'ip-src' => array('desc' => __("A source IP address of the attacker"), 'default_category' => 'Network activity', 'to_ids' => 1
    'ip-dst' => array('desc' => __('A destination IP address of the attacker or C&C server'), 'formdesc' => __("A destination IP a
    'hostname' => array('desc' => __('A full host/dnsname of an attacker'), 'formdesc' => __("A full host/dnsname of an attacker.
    'domain' => array('desc' => __('A domain name used in the malware'), 'formdesc' => __("A domain name used in the malware. Use
    'domain|ip' => array('desc' => __('A domain name and its IP address (as found in DNS lookup) separated by a |'),'formdesc' =>
    'email-src' => array('desc' => __("The email address used to send the malware."), 'default_category' => 'Payload delivery', 't
    'email-dst' => array('desc' => __("A recipient email address"), 'formdesc' => __("A recipient email address that is not relate
    'email-subject' => array('desc' => __("The subject of the email"), 'default_category' => 'Payload delivery', 'to_ids' => 0),
    'email-attachment' => array('desc' => __("File name of the email attachment."), 'default_category' => 'Payload delivery', 'to_
    'email-body' => array('desc' => __('Email body'), 'default_category' => 'Payload delivery', 'to_ids' => 0),
    'float' => array('desc' => __("A floating point value."), 'default_category' => 'Other', 'to_ids' => 0),
    'url' => array('desc' => __('url'), 'default_category' => 'Network activity', 'to_ids' => 1),
    'http-method' => array('desc' => __("HTTP method used by the malware (e.g. POST, GET, ...)."), 'default_category' => 'Network
    'user-agent' => array('desc' => __("The user-agent used by the malware in the HTTP request."), 'default_category' => 'Network
    'ja3-fingerprint-md5' => array('desc' => __("JA3 is a method for creating SSL/TLS client fingerprints that should be easy to p
    'hassh-md5' => array('desc' => __("hassh is a network fingerprinting standard which can be used to identify specific Client SS
    'hasshserver-md5' => array('desc' => __("hasshServer is a network fingerprinting standard which can be used to identify specif
    'regkey' => array('desc' => __("Registry key or value"), 'default_category' => 'Persistence mechanism', 'to_ids' => 1),
    'regkey|value' => array('desc' => __("Registry value + data separated by |"), 'default_category' => 'Persistence mechanism', '
    'AS' => array('desc' => __('Autonomous system'), 'default_category' => 'Network activity', 'to_ids' => 0),
    'snort' => array('desc' => __('An IDS rule in Snort rule-format'), 'formdesc' => __("An IDS rule in Snort rule-format. This ru
    'bro' => array('desc' => __('An NIDS rule in the Bro rule-format'), 'formdesc' => __("An NIDS rule in the Bro rule-format."),
```

Threat Modeling

- Com base em uma análise continua sobre a missão, processos, estrutura e ativos da organização, definir os pontos relevantes para nossa estratégia de defesa.
- A partir destes dados, identificar os tipos de adversários de acordo com vários critérios:

Histórico de ameaças, adversários com interesses em organizações ou ativos similares, de acordo com localização geopolítica, entre outros.

Threat Modeling



[9] Threat Modeling sample.

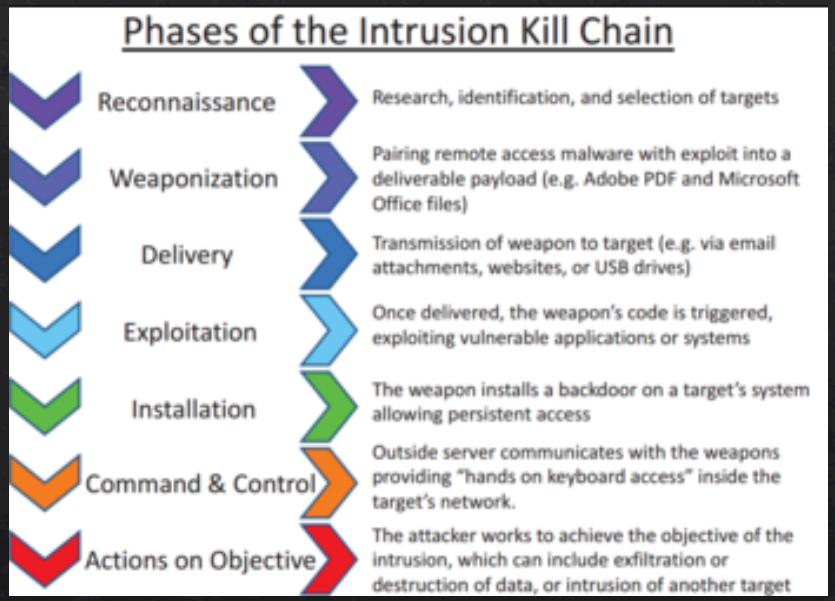
Modelos!

- Concordo com a fala atribuída a George E. P. Box: “All models are wrong; some models are useful”.

- Modelos nos ajudam a resolver melhor um problema.

Cyber Kill Chain

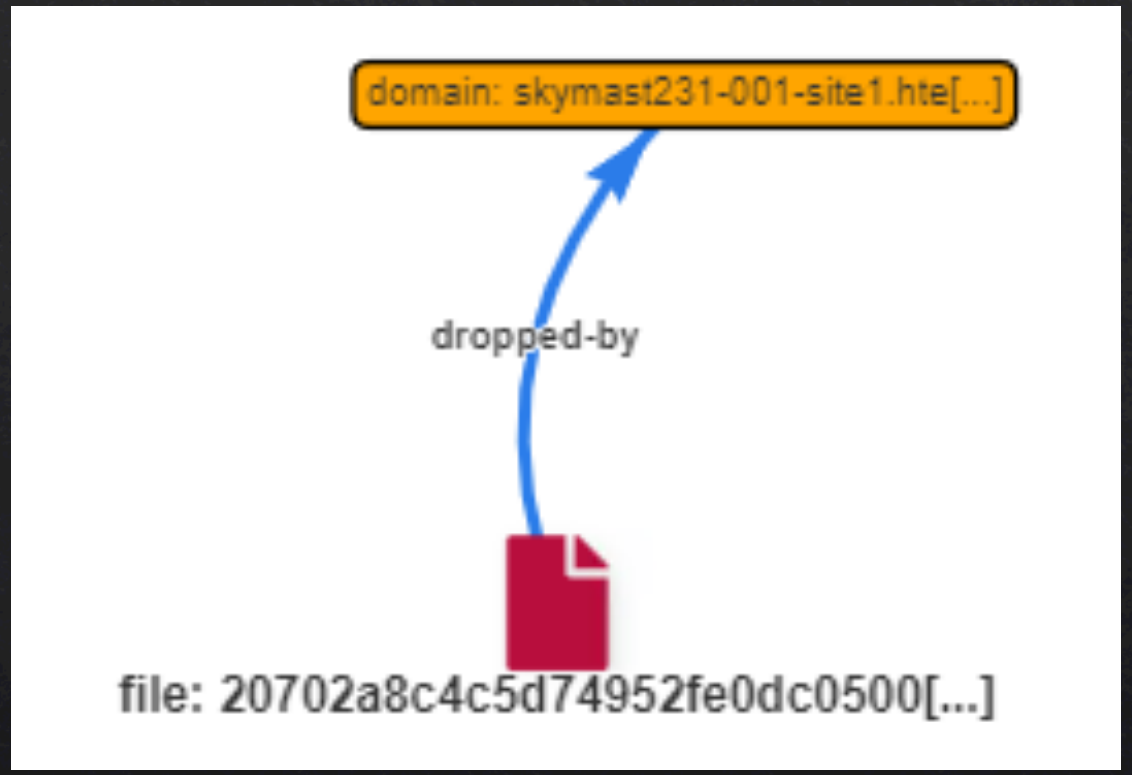
- Modela em fases, as ações feitas por um adversário para concretizar uma intrusão.
- Em questão de CTI, pode ser aplicada de maneiras diferentes.
- Entender a quais fases estamos mais sujeitos a falha.



Cyber Kill Chain – 2° Caso de uso

Category	Type	Value	Tags	Galaxies	Comment	Corr
External analysis	url	https://www.cyberark.com/threat-research-blog/krypton-stealer-kryptonite-for-credentials/				☐
Payload installation	filename|sha256	kryp_XoxoxolUa_6.8_22.59.exe a84f1fe984e6fb04af0e029b67245f2167bcec766959f5033bfbf5ac00f0d396	kill-chain:Installation x		krypton stealer binary	☑
Network activity	hostname	f0304768.xsph.ru	kill-chain:Command and Control x		Command & Control Server	☑

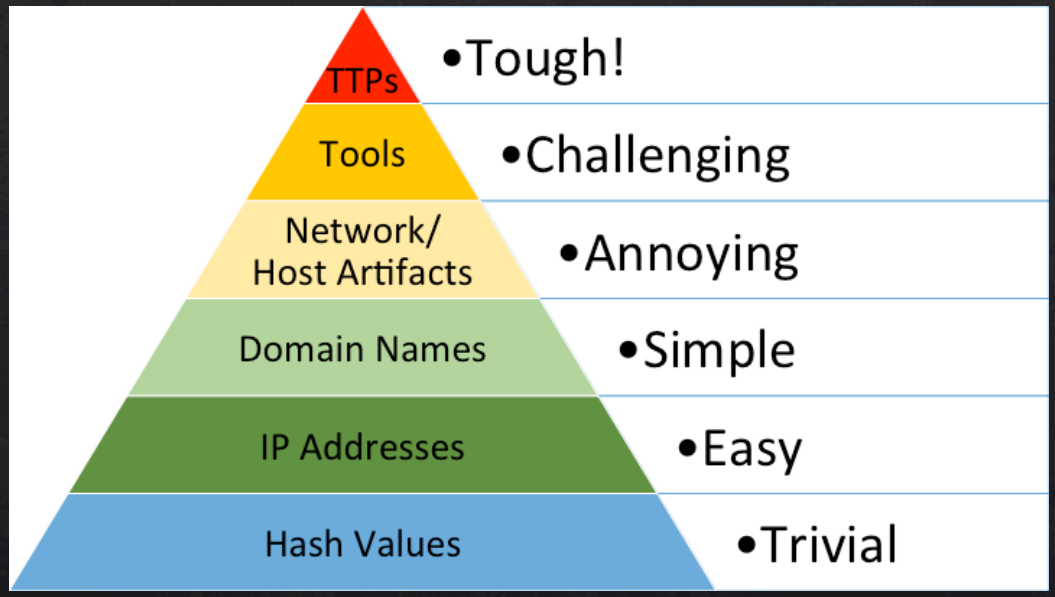
Cyber Kill Chain



UUID 5d6d2aa8-80d4-4324-a3ab-4cbd73e10023

Pyramid of Pain

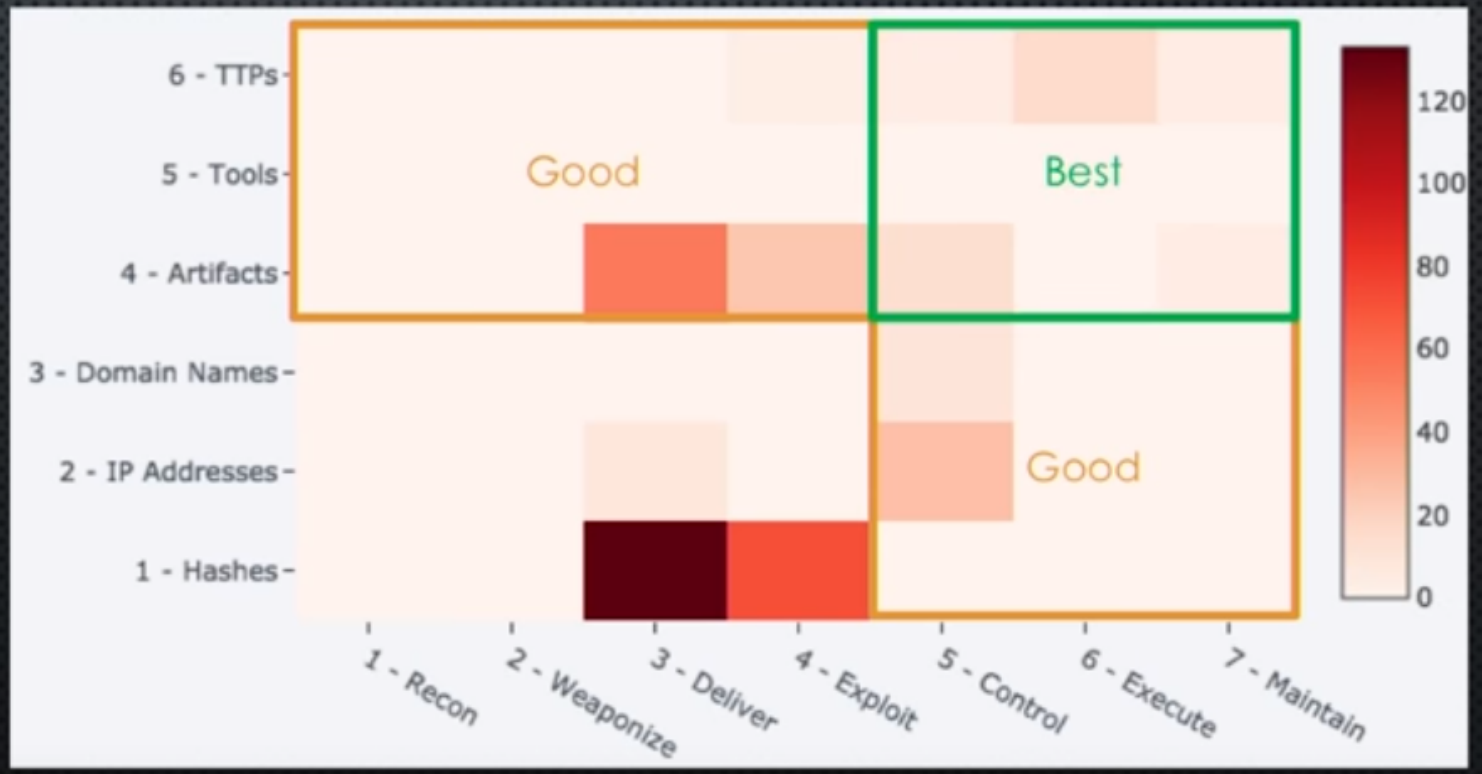
- Indica as dificuldades que um adversário cibernético tem para mudar características de sua infraestrutura e cadeia de ataque.
- Quanto mais para cima da pirâmide, mais complicado é de alterar.
- Podemos aplicar essa visão à CTI.
- Entendemos que a detecção de itens mais acima da pirâmide, são mais valiosos a longo prazo, enquanto mais abaixo à curto prazo.
- Quanto mais pudermos focar nossos esforços para detectar os itens acima da pirâmide, mais preciso será nossa análise sobre um potencial adversário.



Kill Chain + Pyramid of Pain

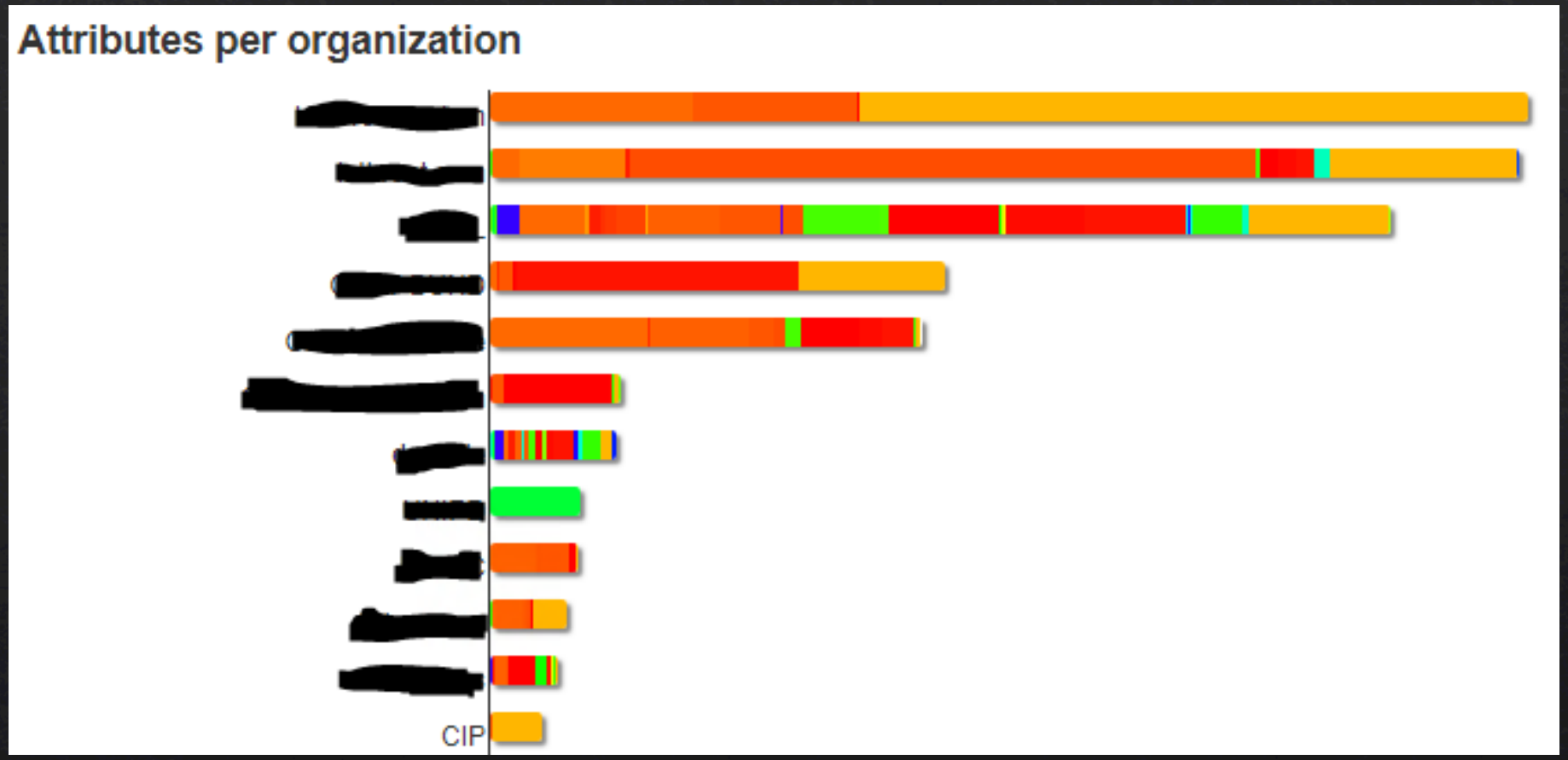
COMBINED VISUALIZATION

Plotting the lifecycle phase vs. Pyramid level can reveal not only current strengths, but also opportunities for improvement.



[5] Medindo a qualidade das informações coletadas

Kill Chain + Pyramid of Pain – 3° Caso de uso



URL's, IP's e domínios.

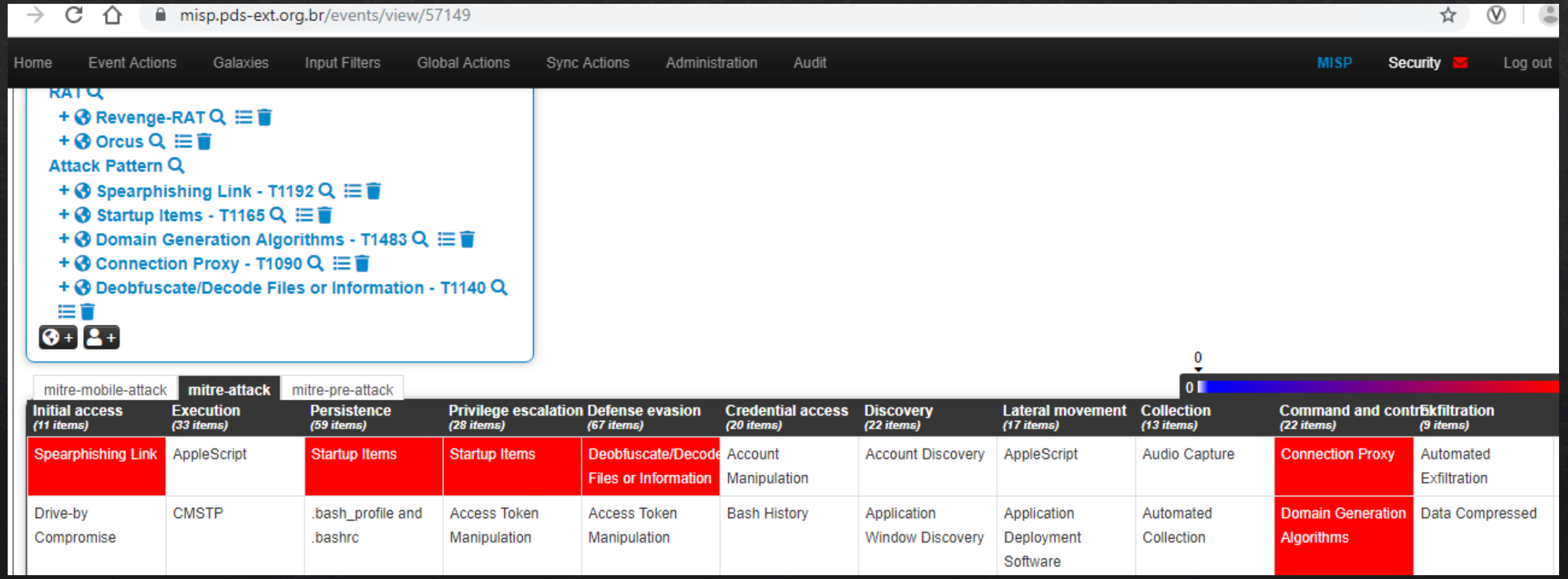
Mitre ATT&CK

- Relaciona técnicas pré (174) e pós (244) invasão utilizadas por adversários.
- Coleta inteligência a nível de Tools e TTP's.
- Colaborar com o projeto dá um bom retorno.
- https://attack.mitre.org/software/S0373/

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation

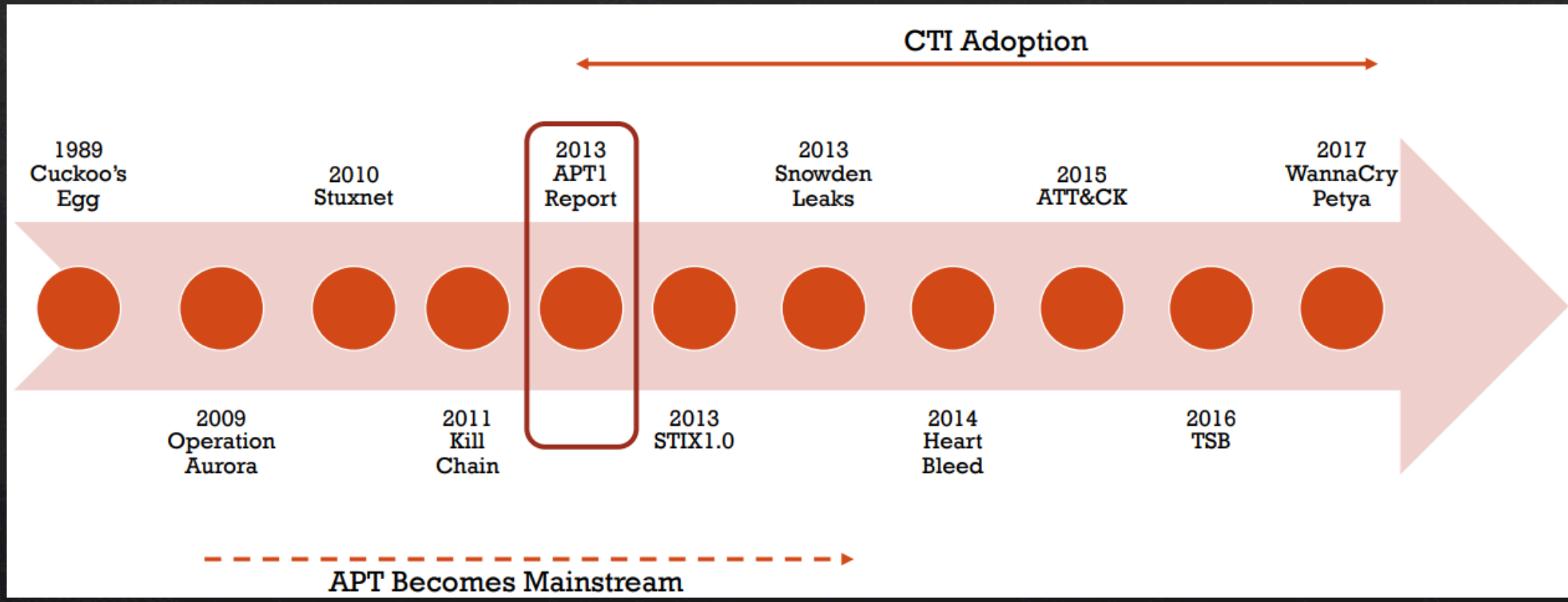
Mitre ATT&CK – 4° Caso de uso



UUID 5d6d2aa8-80d4-4324-a3ab-4cbd73e10023

5° Caso de Uso – Base de conhecimento

Evolução do CTI



[2] Timeline de evolução de CTI

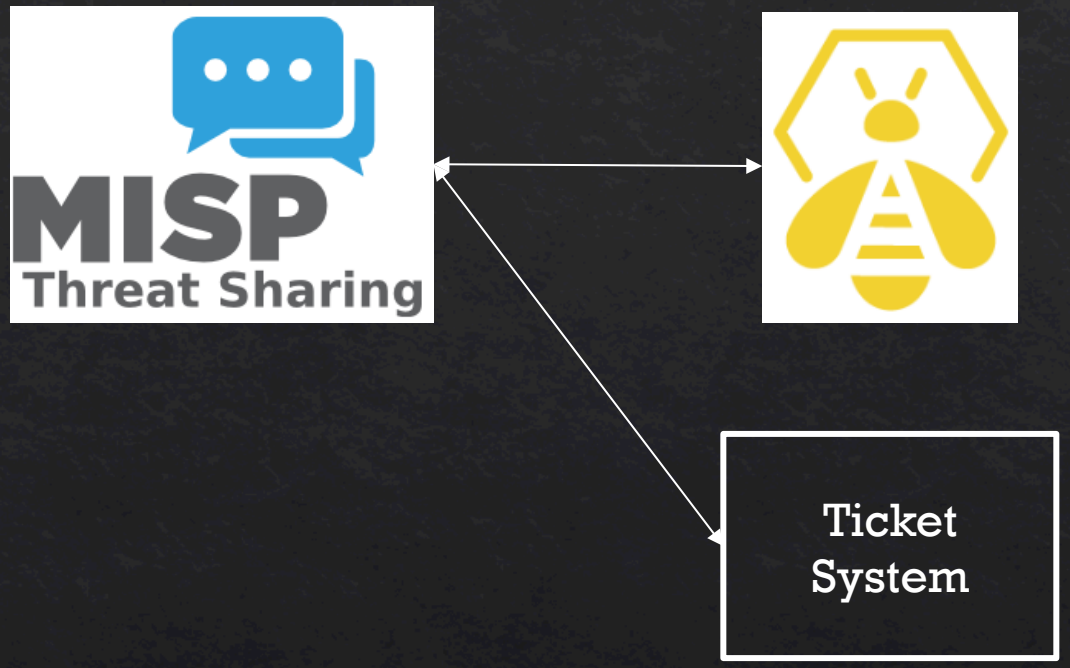
MISP como base de conhecimento

- O MISP nasceu também por volta de 2013.
- Hoje em dia relatórios sobre ameaças e adversários são praticamente diários.
- Ter este conteúdo em um local centralizado é amplamente vantajoso.

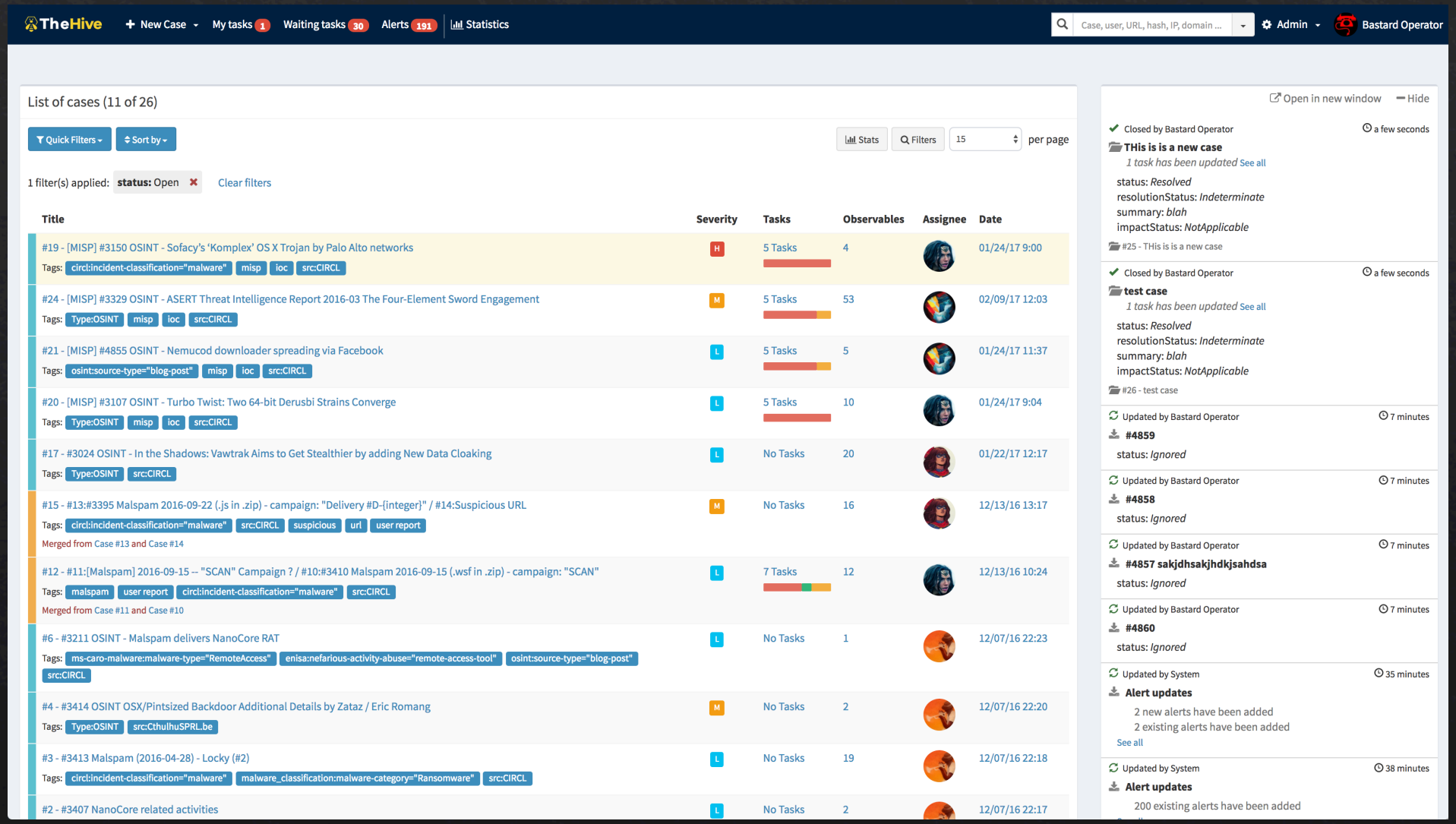
CIRCL	malware_classification:malware-category="Ransomware" osint:source-type="blog-post" tlp:white	2019-05-03	Low	Initial	OSINT - Mystery Git ransomware appears to blank commits, demands Bitcoin to rescue code
CthulhuSPRL.be	tlp:white type:OSINT	2015-11-23	Undefined	Completed	OSINT Yara rules for GlassRAT in Loki IOC Scanner by Florian Roth
CIRCL	type:OSINT tlp:white osint:source-type="blog-post" Android Malware malware_classification:malware-category="Spyware" misp-galaxy:android="Tizi"	2017-11-28	Low	Completed	OSINT - Google Discovers New Tizi Android Spyware
CIRCL	tlp:white type:OSINT	2016-03-25	Low	Completed	OSINT - New self-protecting USB trojan able to avoid detection
CIRCL	type:OSINT tlp:white	2016-03-30	Undefined	Initial	OSINT - GongDa vs. Korean News
CIRCL	type:OSINT tlp:white osint:source-type="blog-post"	2017-08-14	Low	Completed	OSINT - Threat actor goes on a Chrome extension hijacking spree

6° Caso de Uso – Como plataforma de resposta a incidentes

Arquitetura simplificada



The Hive + MISP



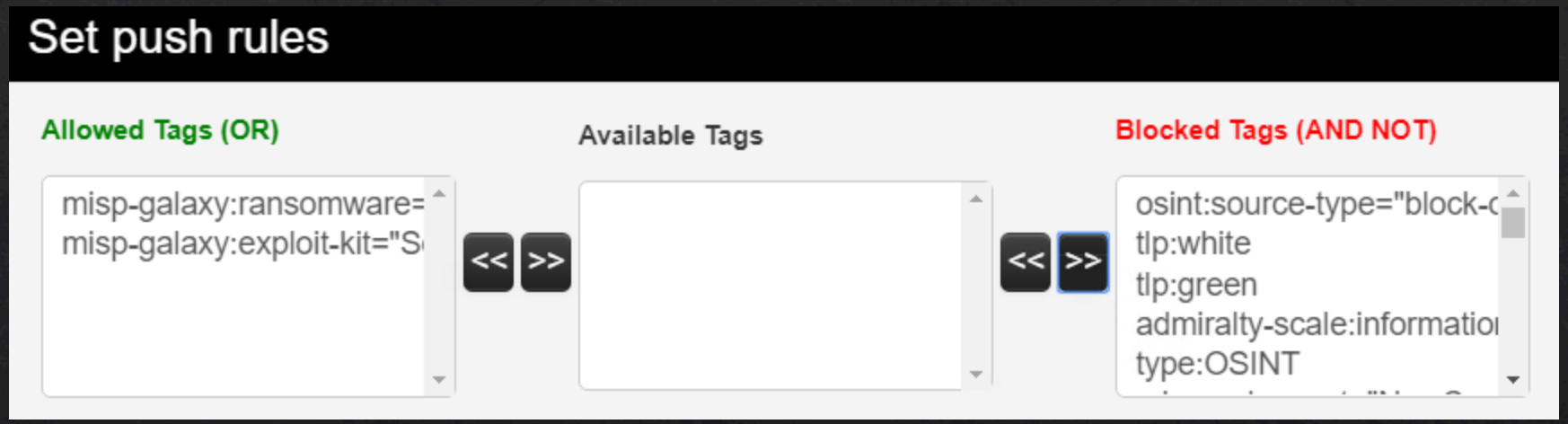
7° Caso de Uso – MISP Externo e Interno

Arquitetura simplificada

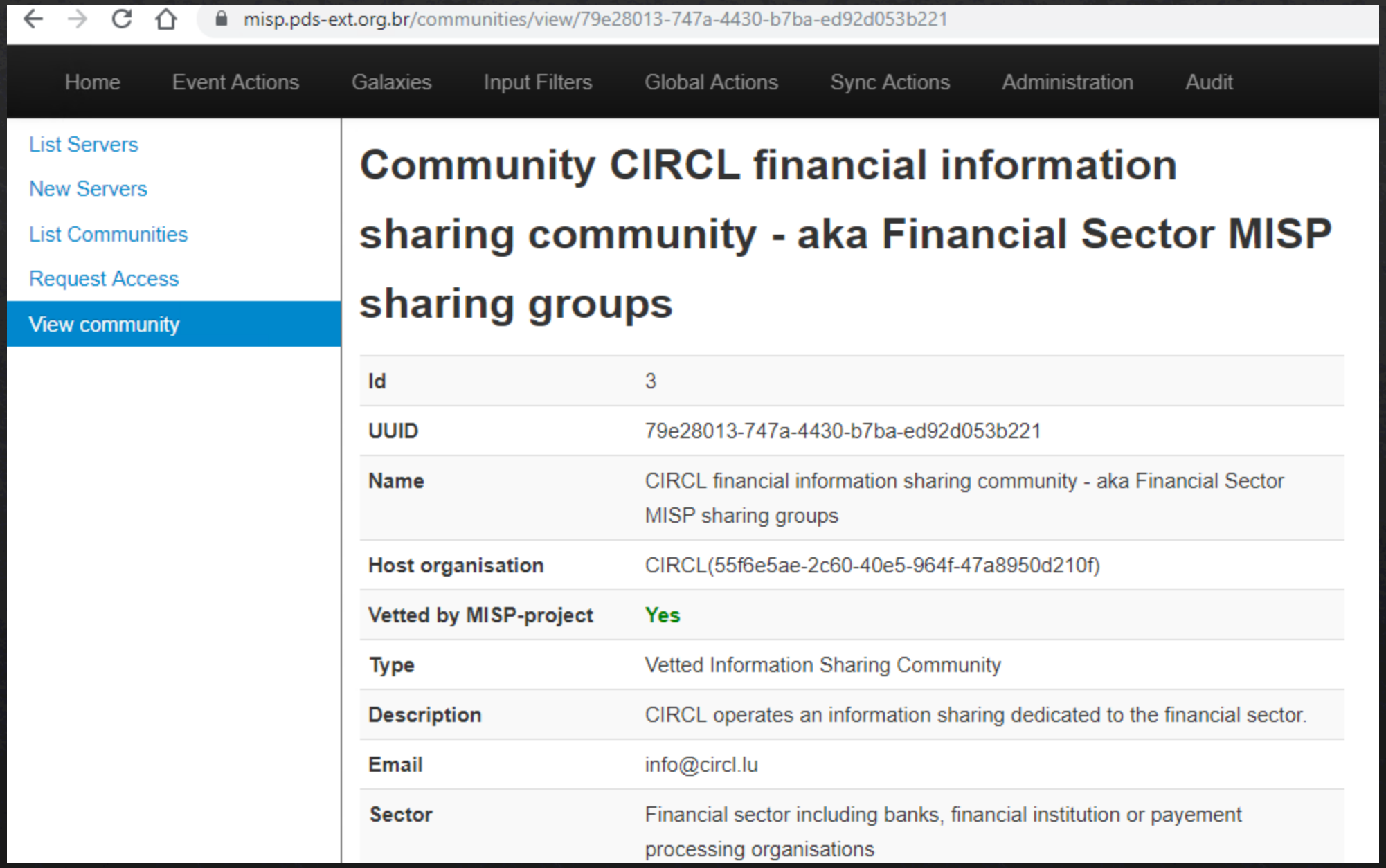
MISP Externo

Filtro via tags

MISP Interno

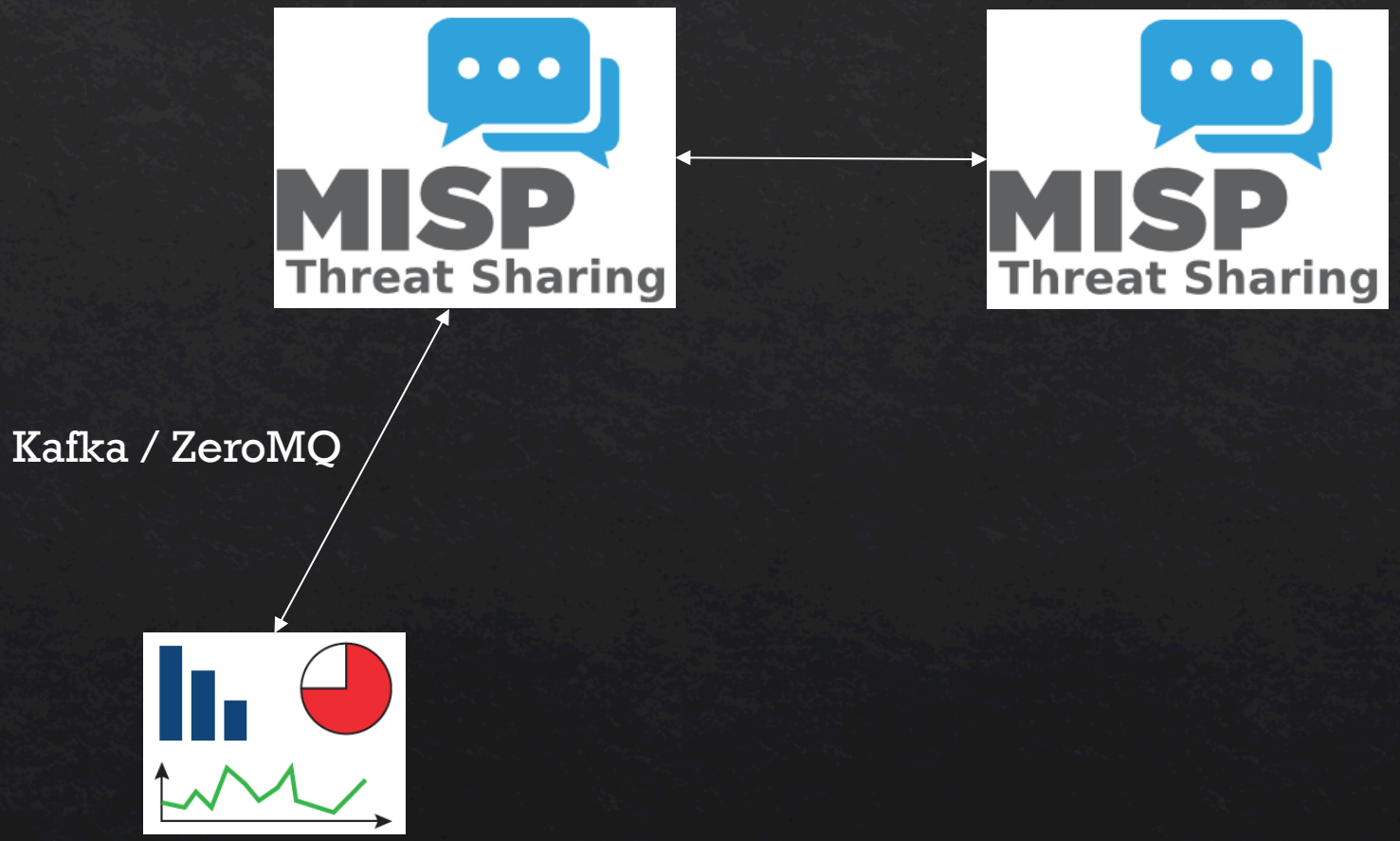

Set push rules
Allowed Tags (OR)
misp-galaxy:ransomware=
misp-galaxy:exploit-kit="S
<<
>>
Available Tags
<<
>>
Blocked Tags (AND NOT)
osint:source-type="block-
tlp:white
tlp:green
admiralty-scale:informatio
type:OSINT

8° Caso de Uso – Tratamento de dados especializados

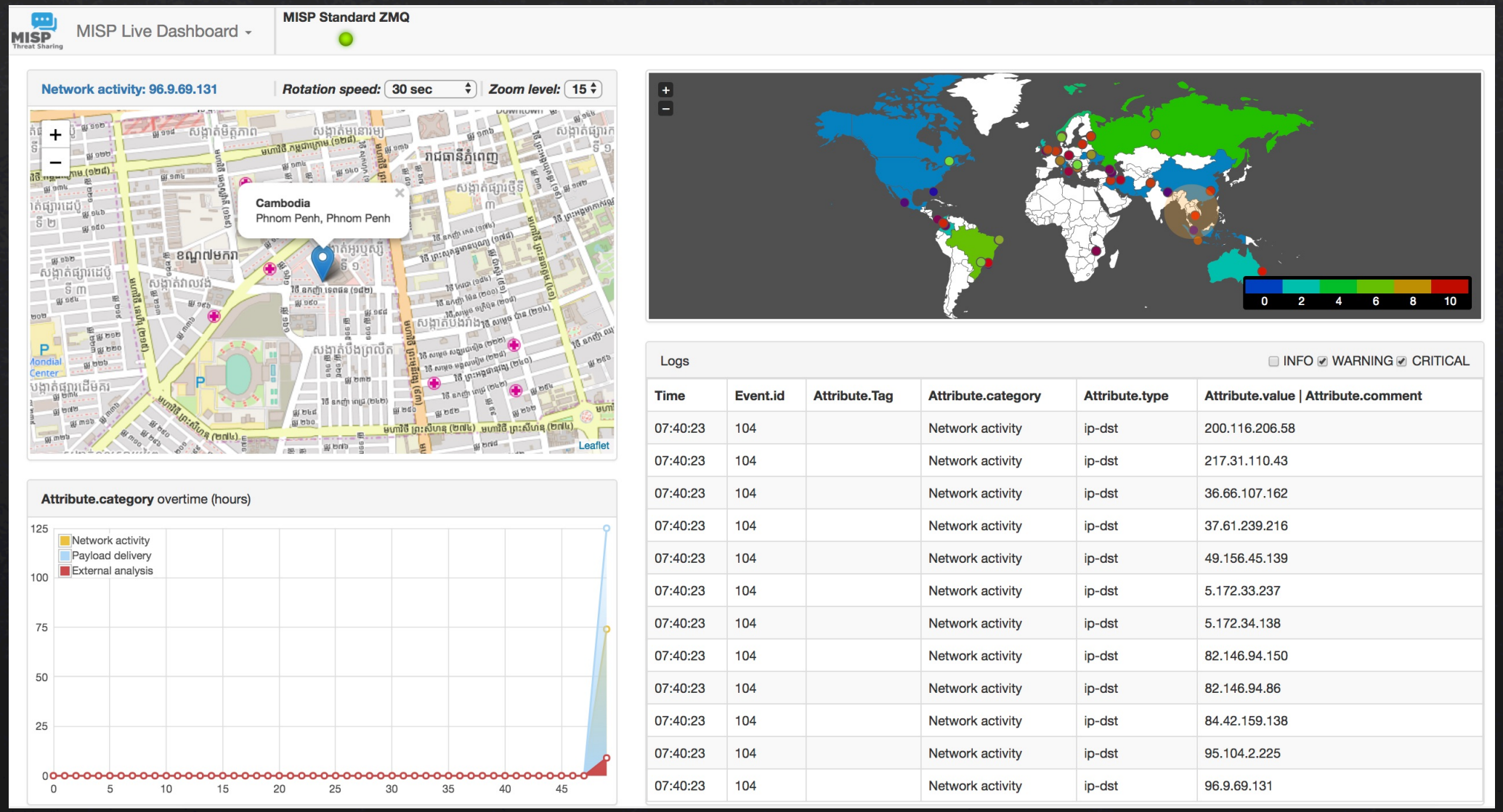

misp.pds-ext.org.br/communities/view/79e28013-747a-4430-b7ba-ed92d053b221
Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
List Servers
New Servers
List Communities
Request Access
View community
Community CIRCL financial information sharing community - aka Financial Sector MISP sharing groups
Id 3
UUID 79e28013-747a-4430-b7ba-ed92d053b221
Name CIRCL financial information sharing community - aka Financial Sector MISP sharing groups
Host organisation CIRCL(55f6e5ae-2c60-40e5-964f-47a8950d210f)
Vetted by MISP-project Yes
Type Vetted Information Sharing Community
Description CIRCL operates an information sharing dedicated to the financial sector.
Email info@circl.lu
Sector Financial sector including banks, financial institution or payement processing organisations

9° Caso de Uso – Como plataforma de monitoração em tempo real

Arquitetura simplificada



MISP Dashboards



10° Caso de Uso – Como plataforma de hunting (automatizada)

Mas qual a estratégia?

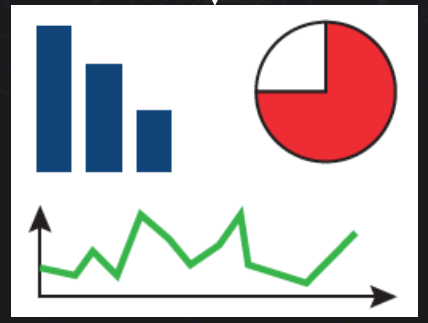
- Ajuda a formular as hipóteses do seu hunting, a partir de critérios definidos.
- Usa CTI, framework de coleta de dados, e modelagem de ameaças.

Arquitetura simplificada

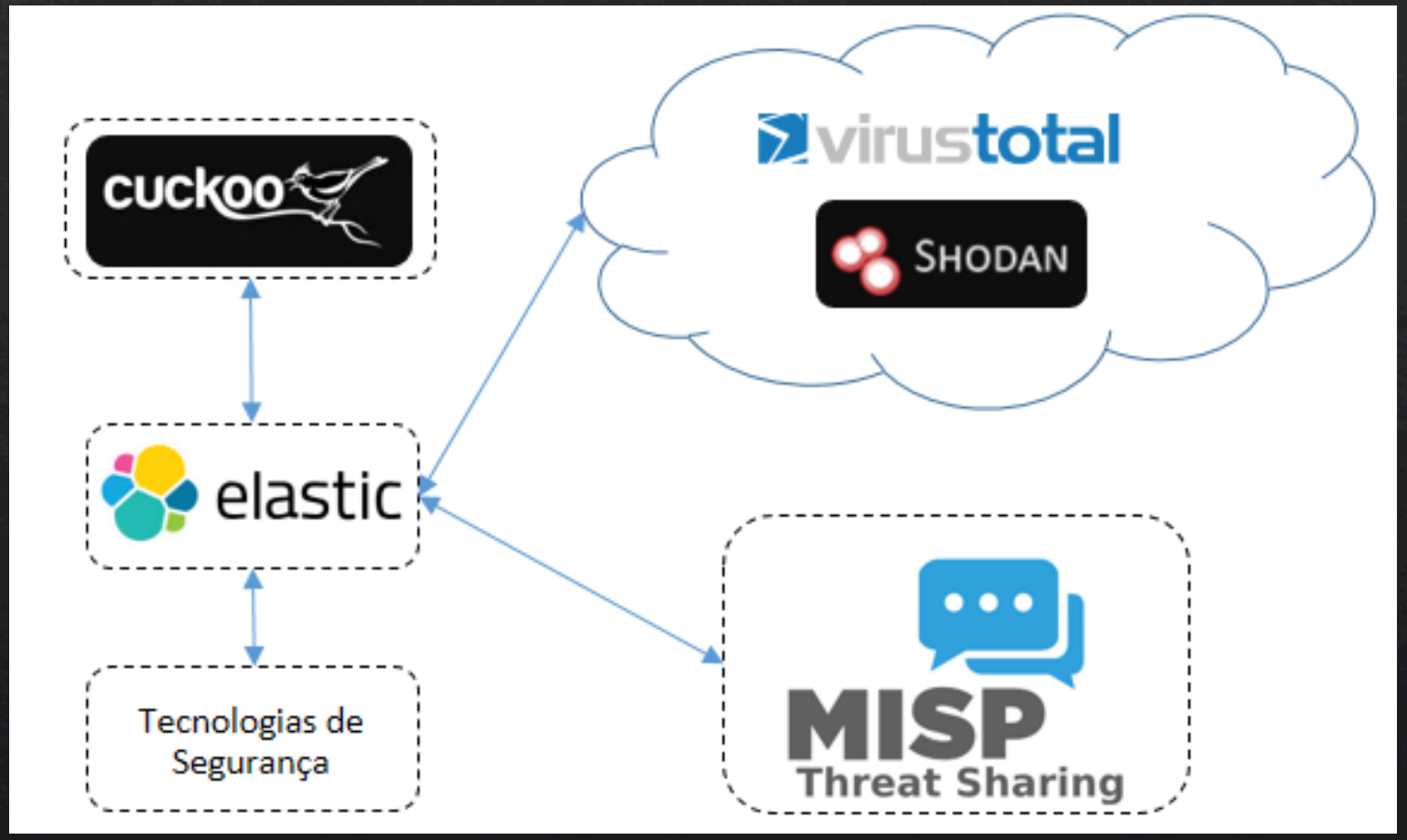
Novo evento

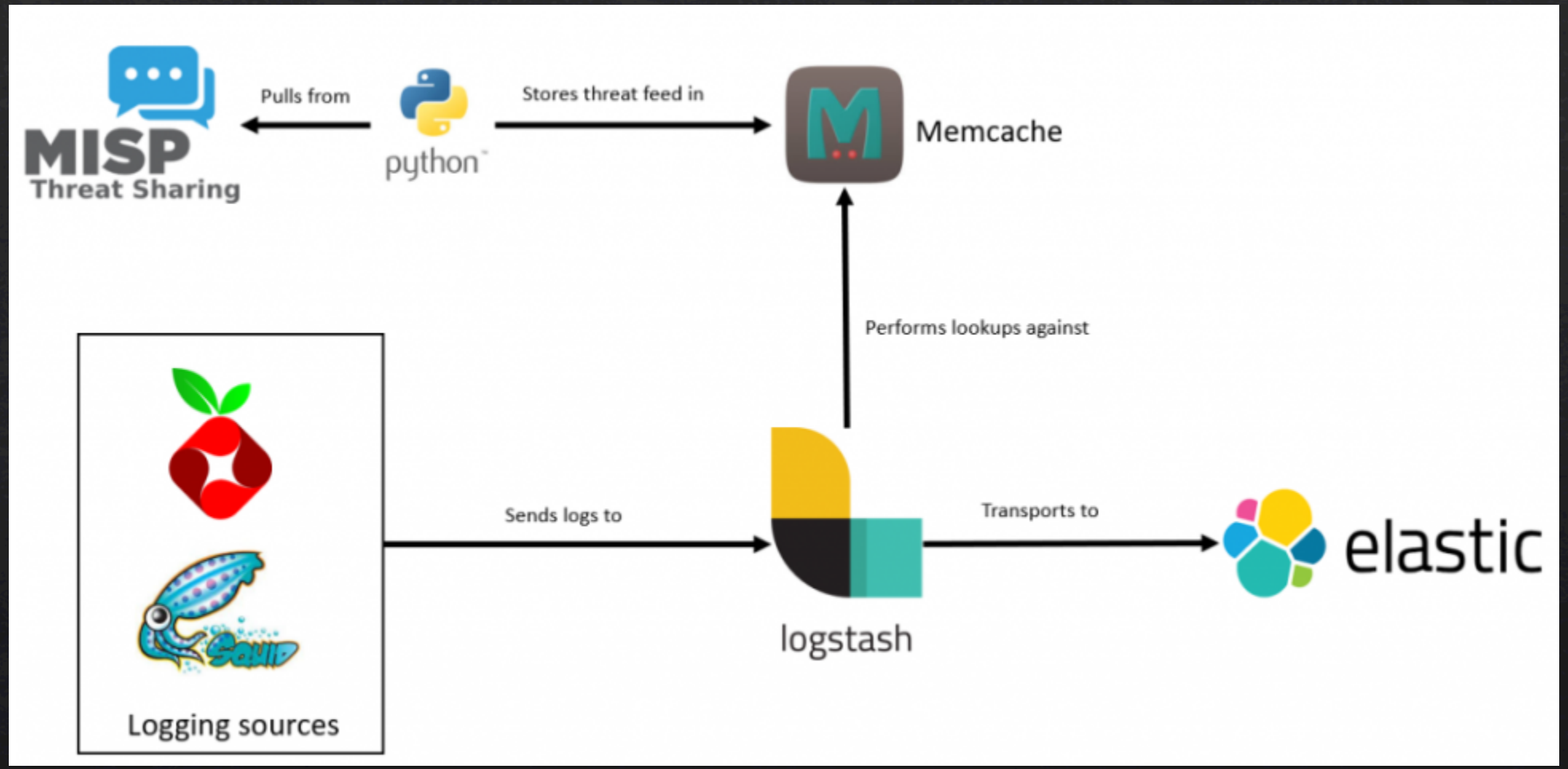
Critérios de
Filtro e busca

SIEM



11° Caso de Uso – Como plataforma de monitoração e correlacionamento


cuckoo
virustotal
SHODAN
elastic
Tecnologias de Segurança
MISP
Threat Sharing



[10] Enriching Elasticsearch with threat data.

Katie Nickels @likethecoins · 18 de mai

+💯 for calling them threat data feeds and not threat intel feeds. ❤️

> **DTCSec** @DCSecuritydk
>
> I got delayed promising to release my MISP-ELK integration posts... But here it is in all its glory... 6 months work into 3 posts..
> securitydistractions.com/2019/05/17/enr.....
>
> Mostrar esta sequência

12° Caso de Uso – Integrações diversas

Integrações – MISP Modules

Expansion modules

- Backscatter.io - a hover and expansion module to expand an IP address with mass-scanning observations.
- BGP Ranking - a hover and expansion module to expand an AS number with the ASN description, its history, and position in BGP Ranking.
- BTC scam check - An expansion hover module to instantly check if a BTC address has been abused.
- BTC transactions - An expansion hover module to get a blockchain balance and the transactions from a BTC address in MISP.
- CIRCL Passive DNS - a hover and expansion module to expand hostname and IP addresses with passive DNS information.
- CIRCL Passive SSL - a hover and expansion module to expand IP addresses with the X.509 certificate seen.
- countrycode - a hover module to tell you what country a URL belongs to.
- CrowdStrike Falcon - an expansion module to expand using CrowdStrike Falcon Intel Indicator API.
- CVE - a hover module to give more information about a vulnerability (CVE).
- CVE advanced - An expansion module to query the CIRCL CVE search API for more information about a vulnerability (CVE).
- Cuckoo submit - A hover module to submit malware sample, url, attachment, domain to Cuckoo Sandbox.
- DBL Spamhaus - a hover module to check Spamhaus DBL for a domain name.
- DNS - a simple module to resolve MISP attributes like hostname and domain to expand IP addresses attributes.
- docx-enrich - an enrichment module to get text out of Word document into MISP (using free-text parser).
- DomainTools - a hover and expansion module to get information from DomainTools whois.

Integrações – MISP Modules

Export modules

- CEF module to export Common Event Format (CEF).
- Cisco FireSight Manager ACL rule module to export as rule for the Cisco FireSight manager ACL.
- GoAML export module to export in GoAML format.
- Lite Export module to export a lite event.
- PDF export module to export an event in PDF.
- Nexthink query format module to export in Nexthink query format.
- osquery module to export in osquery query format.
- ThreatConnect module to export in ThreatConnect CSV format.
- ThreatStream module to export in ThreatStream format.

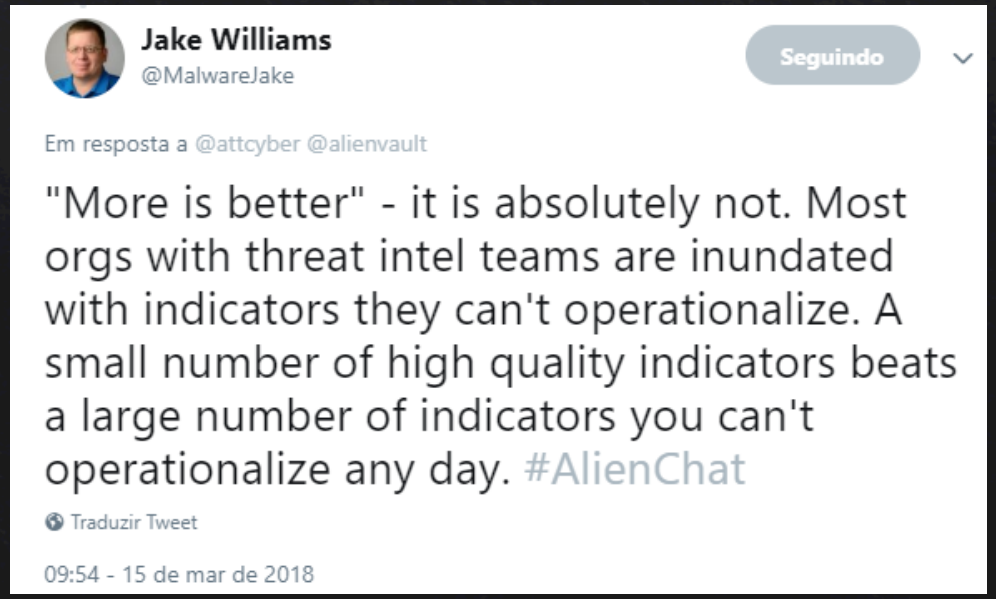
Integrações – MISP Modules

Import modules

- CSV import Customizable CSV import module.
- Cuckoo JSON Cuckoo JSON import.
- Email Import Email import module for MISP to import basic metadata.
- GoAML import Module to import GoAML XML format.
- Joe Sandbox import Parse data from a Joe Sandbox json report.
- OCR Optical Character Recognition (OCR) module for MISP to import attributes from images, scan or faxes.
- OpenIOC OpenIOC import based on PyMISP library.
- ThreatAnalyzer - An import module to process ThreatAnalyzer archive.zip/analysis.json sandbox exports.
- VMRay - An import module to process VMRay export.

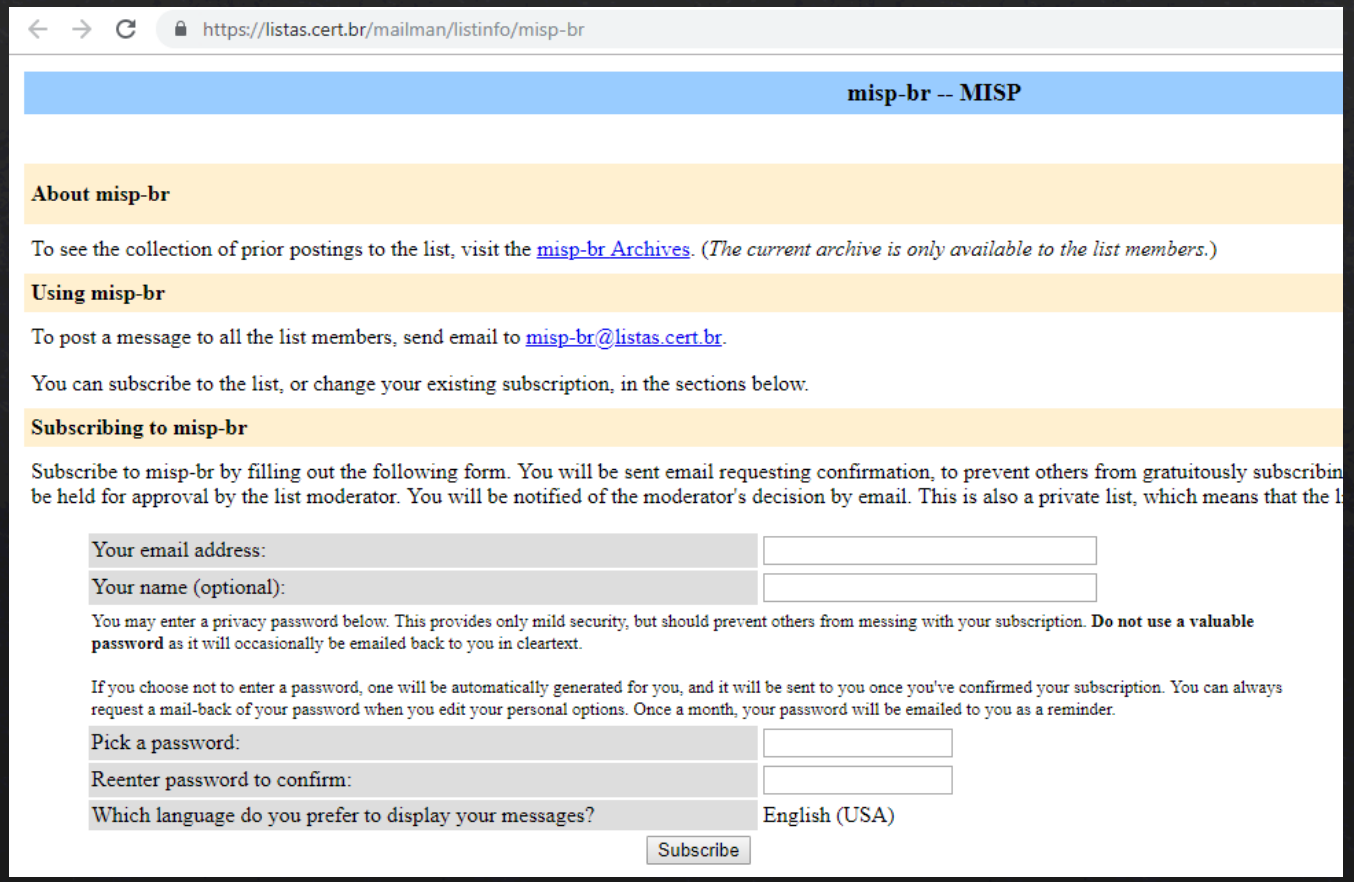
Erros “comuns” cometidos

- O MISP não é CTI.
- Sua plataforma não é melhor porque tem “MAIS INDICADORES”.



Lista do CERT.br sobre MISP

https://listas.cert.br/mailman/listinfo/misp-br



Referências

[1] LEE, Robert M. Intelligence Defined and its Impact on Cyber Threat Intelligence. Disponível em http://www.robertmlee.org/intelligence-defined-and-its-impact-on-cyber-threat-intelligence/

[2] SFAKIANAKIS, Andreas. 5 years of applied CTI discipline. FIRST CTI 2019. Disponível em https://github.com/sfakiana/FIRST-CTI-2019/blob/master/Andreas_Sfakianakis_FIRST_CTI_2019_v2.0.pdf

[3] S Roberts. Intelligence Concepts. Disponível em https://medium.com/@sroberts/intelligence-concepts-the-intelligence-cycle-f25ec067f1d6

[4] LEE, Robert M. Leveraging Cyber Threat Intelligence in an Active Cyber Defense. Disponível em https://www.youtube.com/watch?v=ea50SyPBDBo&t=8s

[5] BIANCO, David. Quality Over Quantity: Determining Your CTI Detection Efficacy

Disponível em: https://www.youtube.com/watch?v=ueGZosLD7iE&t=

[6] SEIRA, Alexandre. PINTO, Alex. Data-Driven Threat Intelligence: Metrics On Indicator Dissemination And Sharing. Disponível em https://www.youtube.com/watch?v=6JMEKnes-w0

[7] LEE, Robert M. Why and How to Take the GCTI The Industry's Cyber Threat Intelligence Certification

Disponível em https://www.youtube.com/watch?v=KNwpY-RkJ2k

[8] DRAGOS. Collection Management Frameworks – Looking beyond Asset Inventories in Preparation for and Response to Cyber Threats. Disponível em https://dragos.com/wp-content/uploads/CMF_For_ICS.pdf.

[9] INCIBE. CyberSecurity Summer Bootcamp. 2017, León.

[10] CLAYTON, David. Enriching Elasticsearch with threat data. Disponível em https://www.securitydistractions.com/2019/05/17/enriching-elasticsearch-with-threat-data-part-1-misp/

Obrigado pela presença =]

- Carlos Borges, CTI Analyst
- Twitter: @huntingneo
- Github/Medium: @hackunagi
- Material disponível em:

https://pt.slideshare.net/hackunagi