SEMINÁRIO

Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)

15 AGO 18

MISP
Threat Sharing

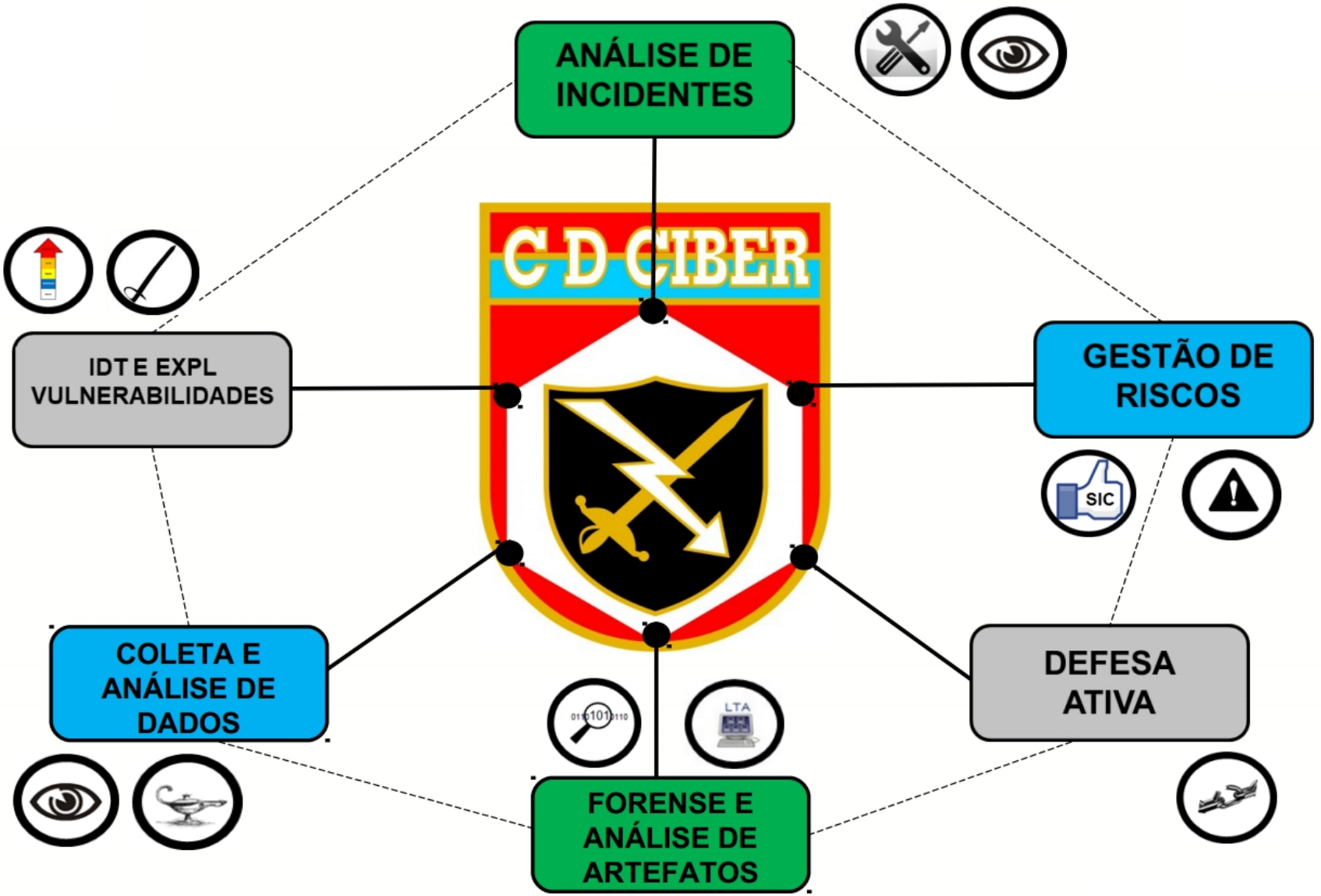
Sumário

- ✓ Missão da Divisão de Proteção – CDCiber
- ✓ Colaboração Cibernética
- ✓ O que é MISP?
- ✓ Principais funcionalidades e benefícios
- ✓ Ecossistema MISP e ATT&CK MITRE
- ✓ Comunidades
- ✓ Plano de trabalho para implantação
- ✓ Reuniões de especialistas
- ✓ Conclusão

Missão da Divisão de Proteção

Ser capaz de conduzir ações para **neutralizar ataques e exploração cibernética** contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter **permanente**.

Células Funcionais



Alertas, Notificações e Recomendações

Alerta CVE-2018-7600

Drupalgeddon2

Destinatários: CTIR FFAA

Notificações e Recomendações de Segurança – Campanhas de Ransomware 2017

WannaCry, Petya e Bad Rabbit

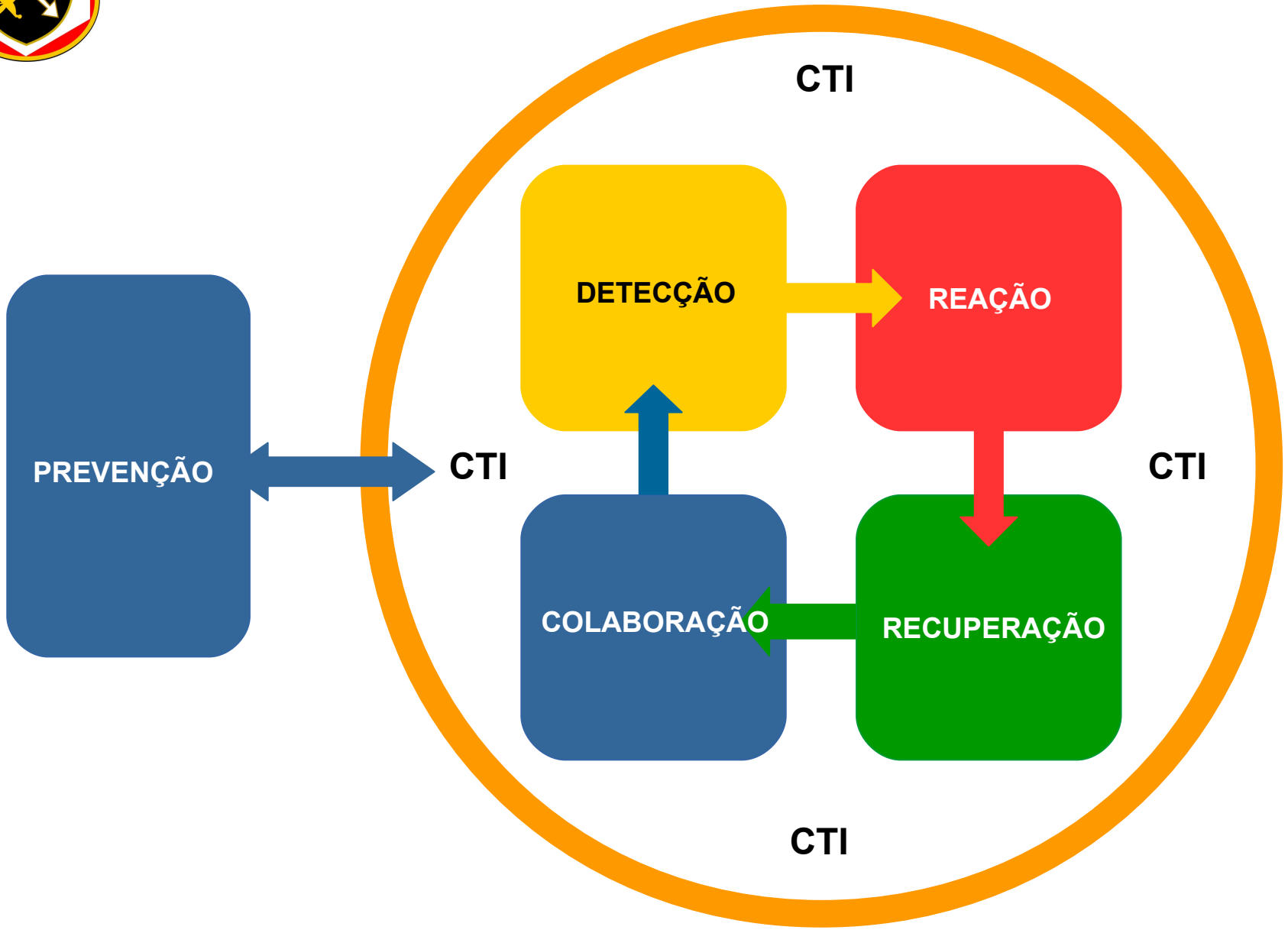
Nível de Alerta Cibernético

GESTÃO DE RISCOS (ÍNDICE DE RISCO CIBERNÉTICO) + **ANÁLISE DE INCIDENTES** = **CONSCIÊNCIA SITUACIONAL**

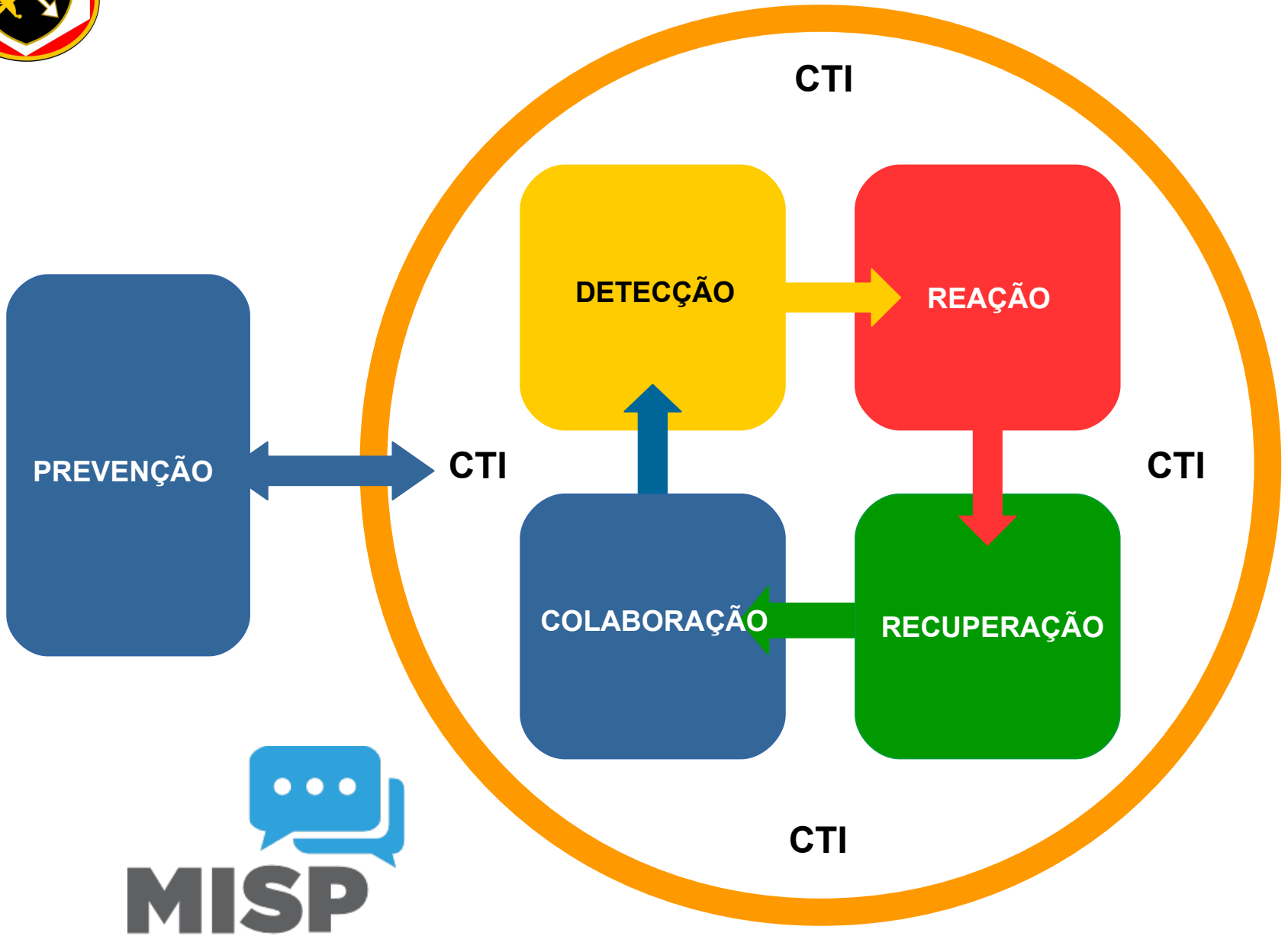
- Muito Alto
- Alto
- Médio
- Moderado
- Baixo

Classificação dada ao estado em que se encontra o Espaço Cibernético de interesse do MD e das FA, no tocante à possibilidade de **concretização de ameaças cibernéticas**.

Quando a prevenção falha...

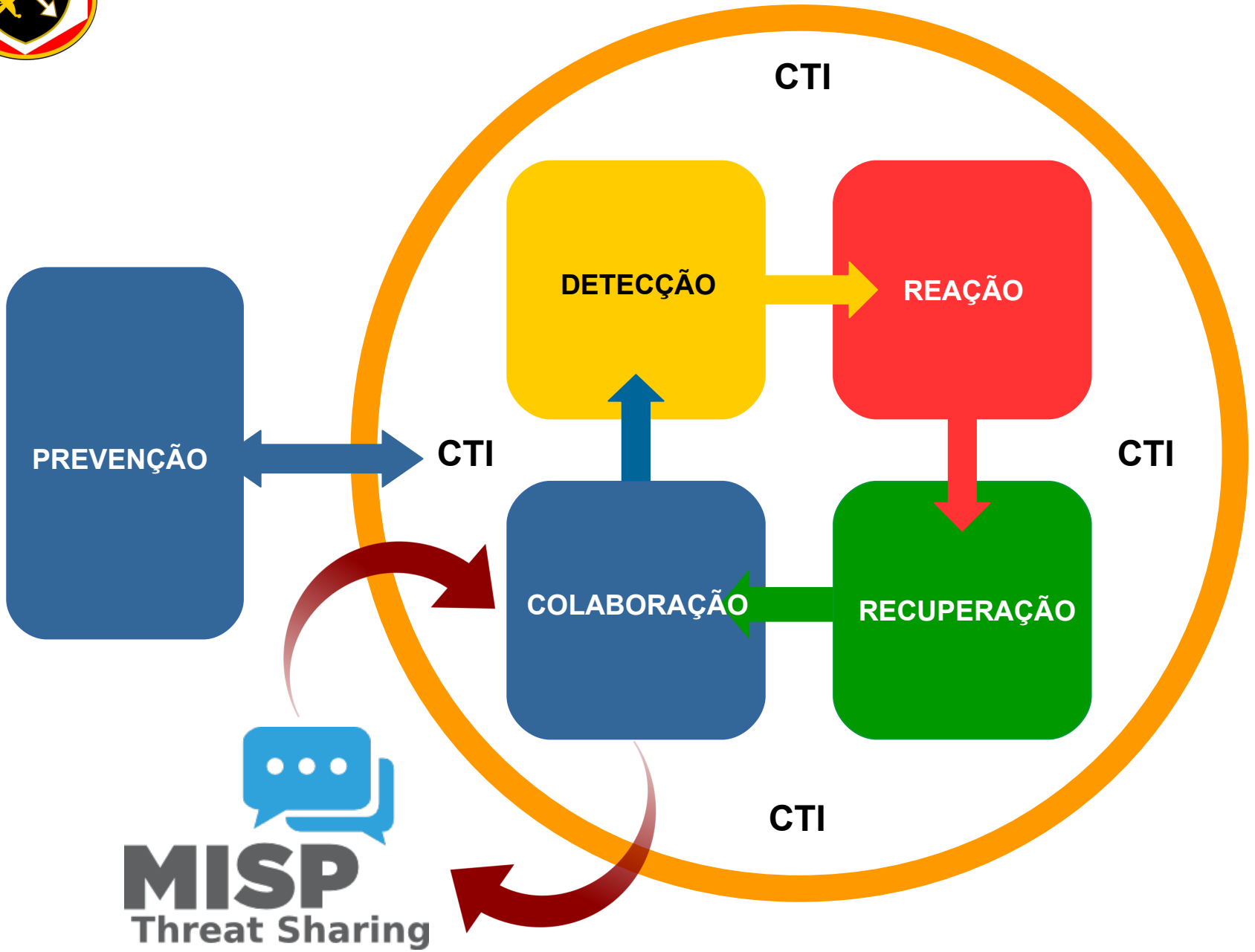


Quando a prevenção falha...

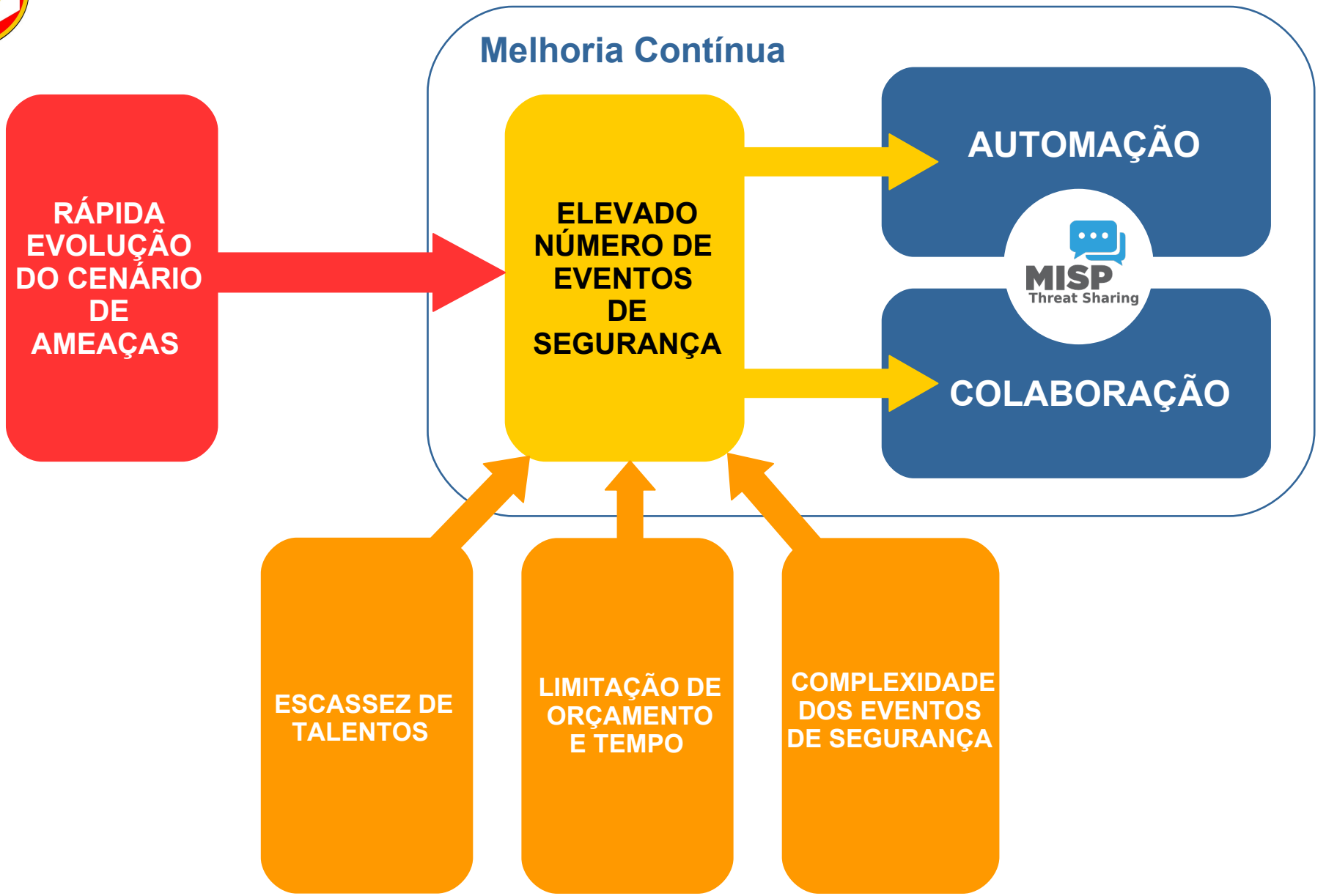


MISP
Threat Sharing

Quando a prevenção falha...



Para reduzir o tempo de reação!



Fatos...

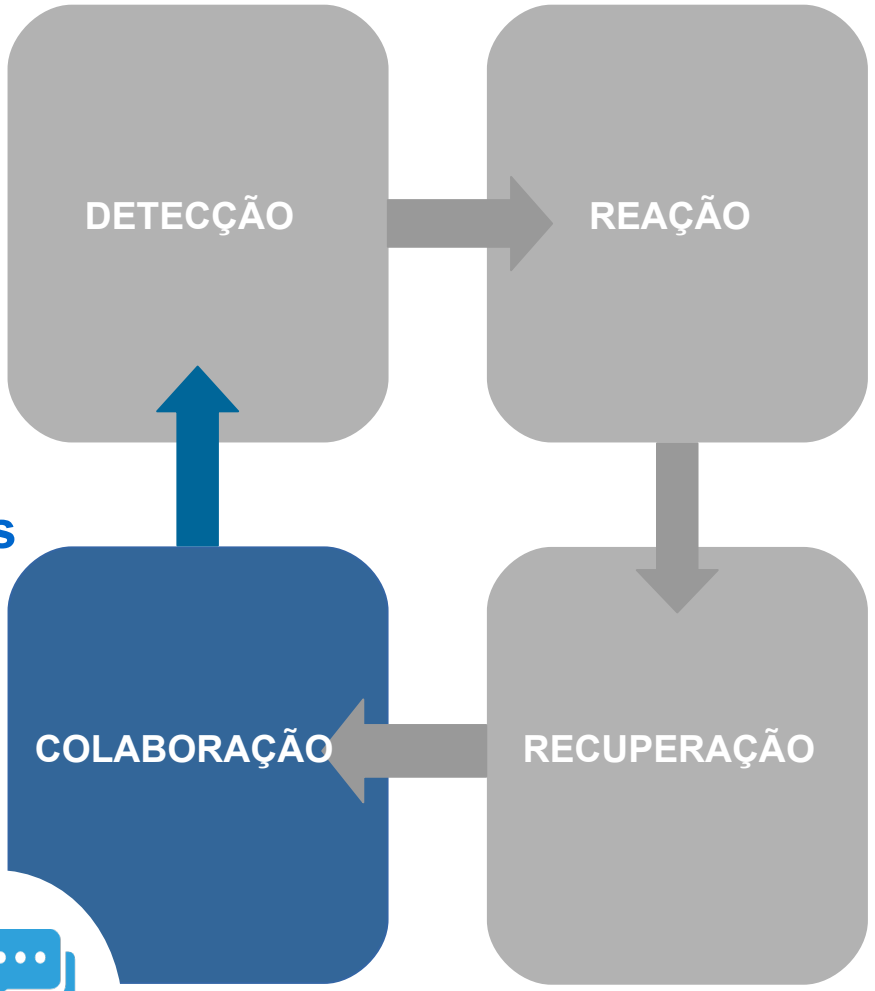
✓ Inteligência de Ameaças + Análise Forense Digital + Resposta a Incidentes = **Trabalho de Equipe**

✓ Nós devemos buscar o **impulsionamento** dessas atividades e **aprimorá-las** continuamente

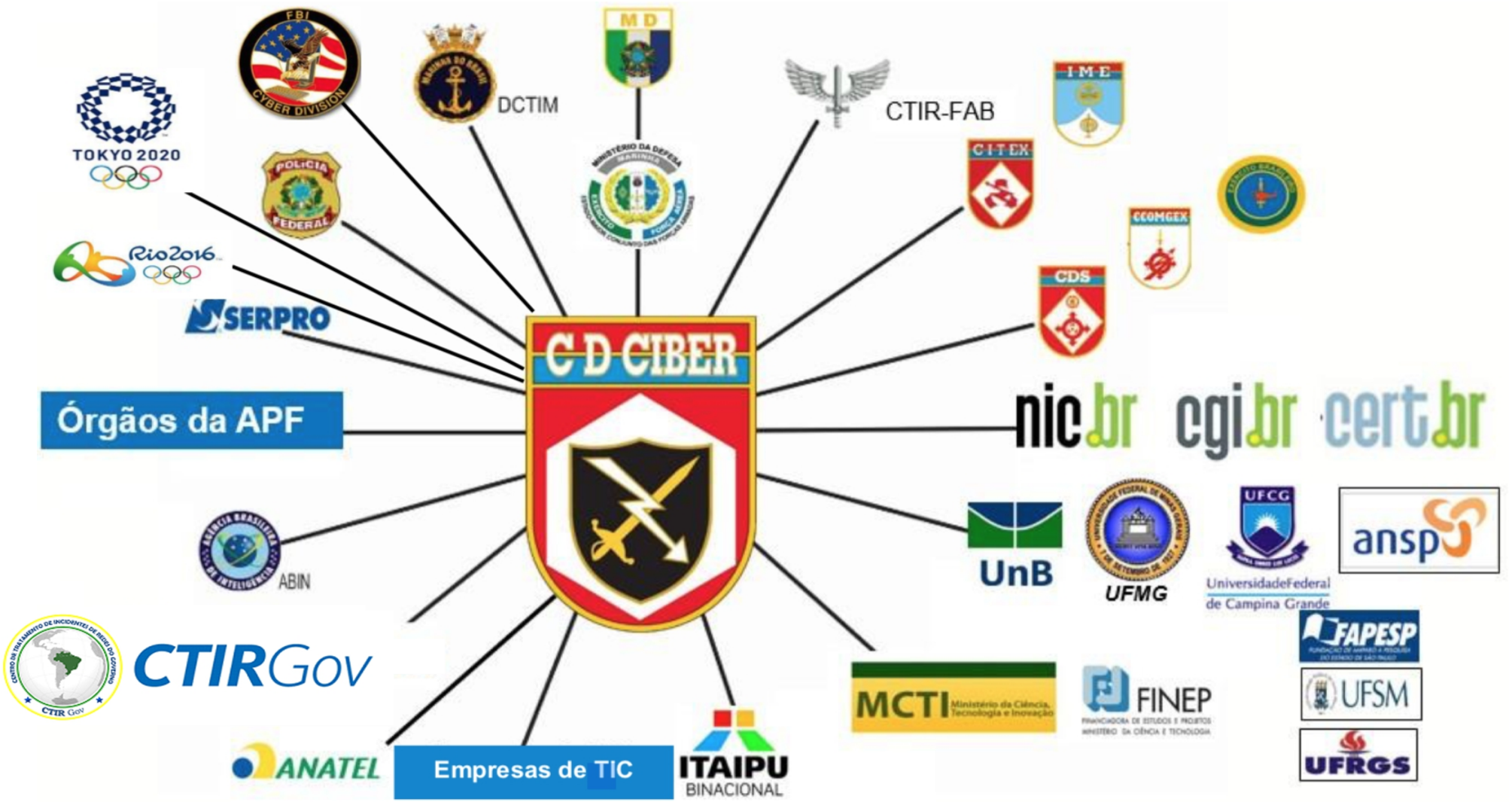
✓ Graças à equipe de operações é possível a obtenção de **estatísticas** significativas

Compartilhar é se importar!
Minha detecção é sua prevenção!

- Investigação realizada, **IOC's coletados** e resposta adequada feita.
- É hora de descansar? **Não!**
- Alguns, se não todos os IOC's, devem ser **compartilhados**.
- Eles podem ser **úteis para outras instituições se defenderem**.
- Espera-se que outras instituições criem **IOC's complementares** que eram desconhecidos para nós.



Rede de Colaboração Cibernética



Malware Information Sharing Platform and Threat Sharing

- ✓ Início do uso da plataforma em 2012
- ✓ Cristophe Vandeplas – CERT Belga
- ✓ _https://github.com/MISP/MISP
- ✓ _http://www.misp-project.org

CIRCL
MISP
Threat Sharing

O que é MISP Threat Sharing ?

- O Malware Information Sharing Plataform and Threat Sharing (MISP) é uma solução de software de código aberto para coletar, armazenar, distribuir e compartilhar **indicadores de segurança e ameaças cibernéticas.**
- O MISP foi projetado por e para **analistas de incidentes, especialistas em engenharia reversa de malware e profissionais de segurança** para dar suporte às suas operações do dia-a-dia e compartilhar informações estruturadas de maneira eficiente.

Principais funcionalidades do MISP Threat Sharing

✓ Compartilhamento de informações estruturadas ou não dentro da comunidade de segurança (**IOC e threat sharing**).

✓ Correlacionamento automático, importação de texto livre, distribuição e colaboração de eventos.

✓ Suporte a vários formatos para exportação: IDS/IPS (Suricata, Snort), SIEM, Host Scanners (OpenIOC, STIX, CSV, Yara), plataformas de análise (Maltego), dentre outras.

✓ Compartilhamento de indicadores para otimizar a **detecção e bloqueio de ameaças** como também obter a **inteligência da ameaça**.

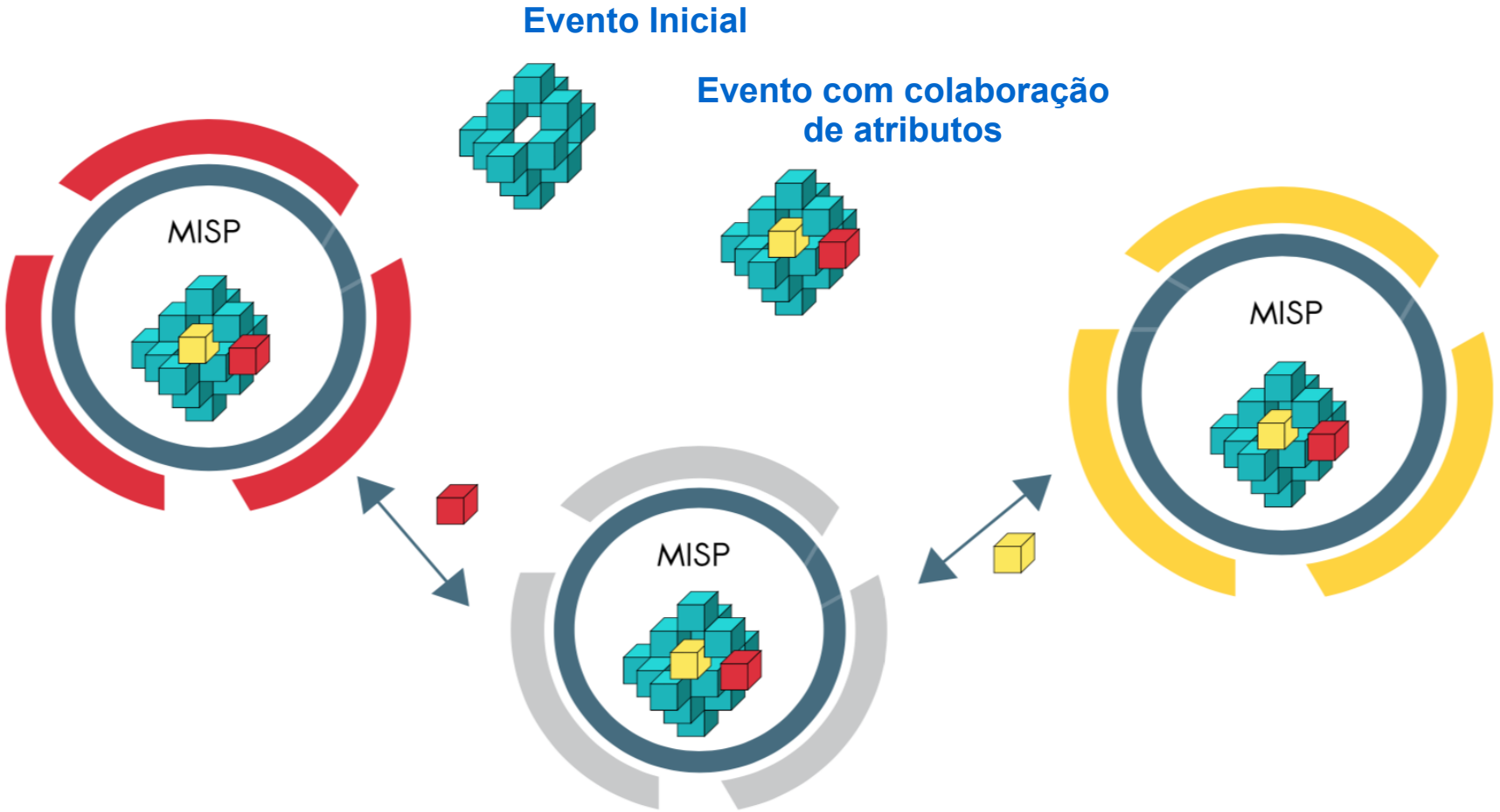
Quais os benefícios do MISP Threat Sharing ?

- ✓ **Eliminar a duplicação** de trabalho analítico.
- ✓ Detectar de forma mais eficiente as ameaças.
- ✓ Melhorar a inteligência e a atribuição de ameaças. (**visão holística versus de uma única organização**)
- ✓ Permitir a interoperabilidade. (**Padronização dos protocolos** de compartilhamento)
- ✓ Dar suporte à automação por intermédio de recursos de **importação e exportação de IOC's**.

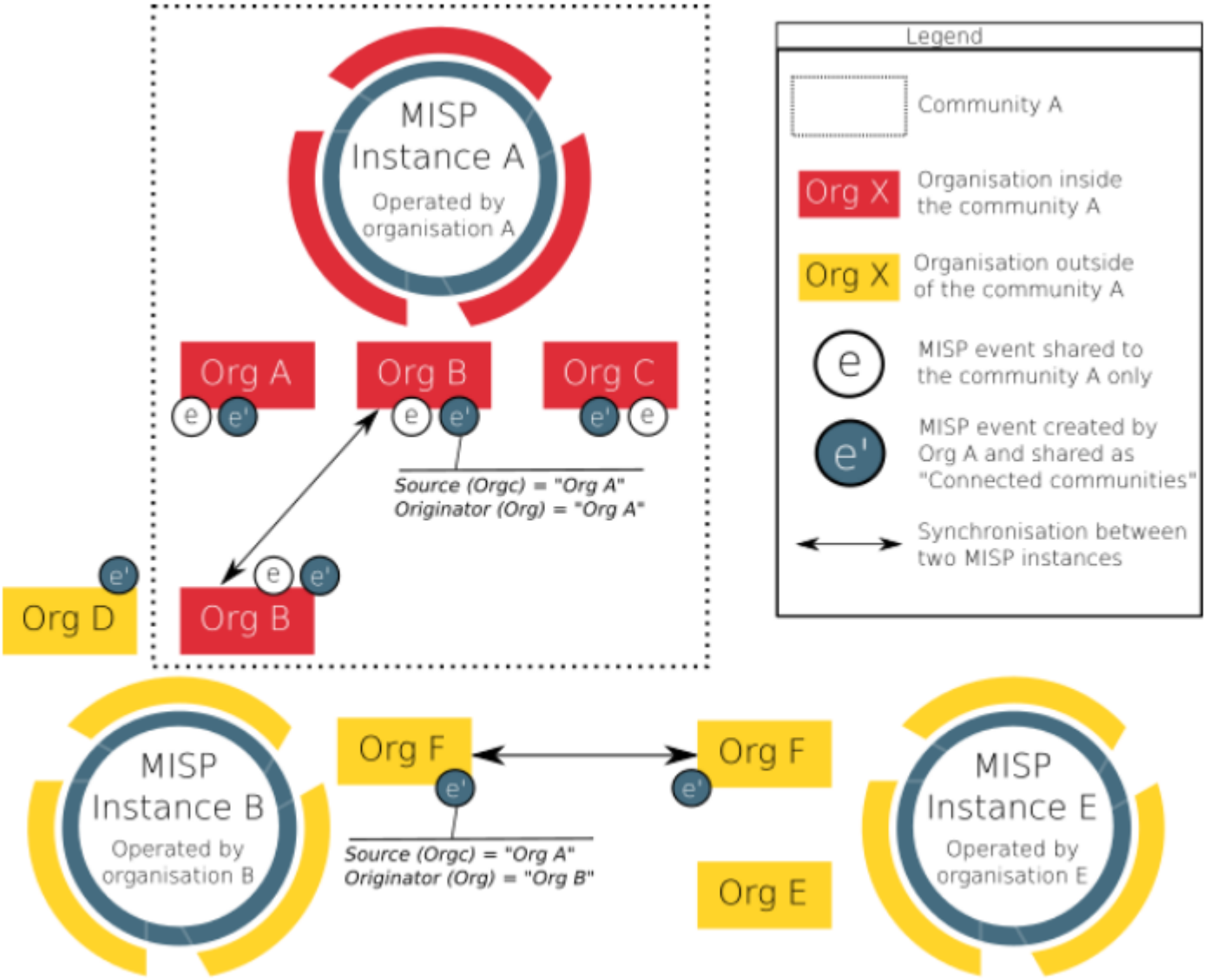
Overview do Projeto MISP

- ✓ Projeto desenvolvido em PHP e Python
- ✓ Módulos (Python) para expandir as funcionalidades (importação e exportação)
- ✓ Taxonomias (JSON) para adicionar categorias e marcação global
- ✓ Listas de avisos (JSON) para detectar possíveis falsos positivos
- ✓ Galaxy (JSON) para adicionar agentes de ameaças, ferramentas ou "inteligência"

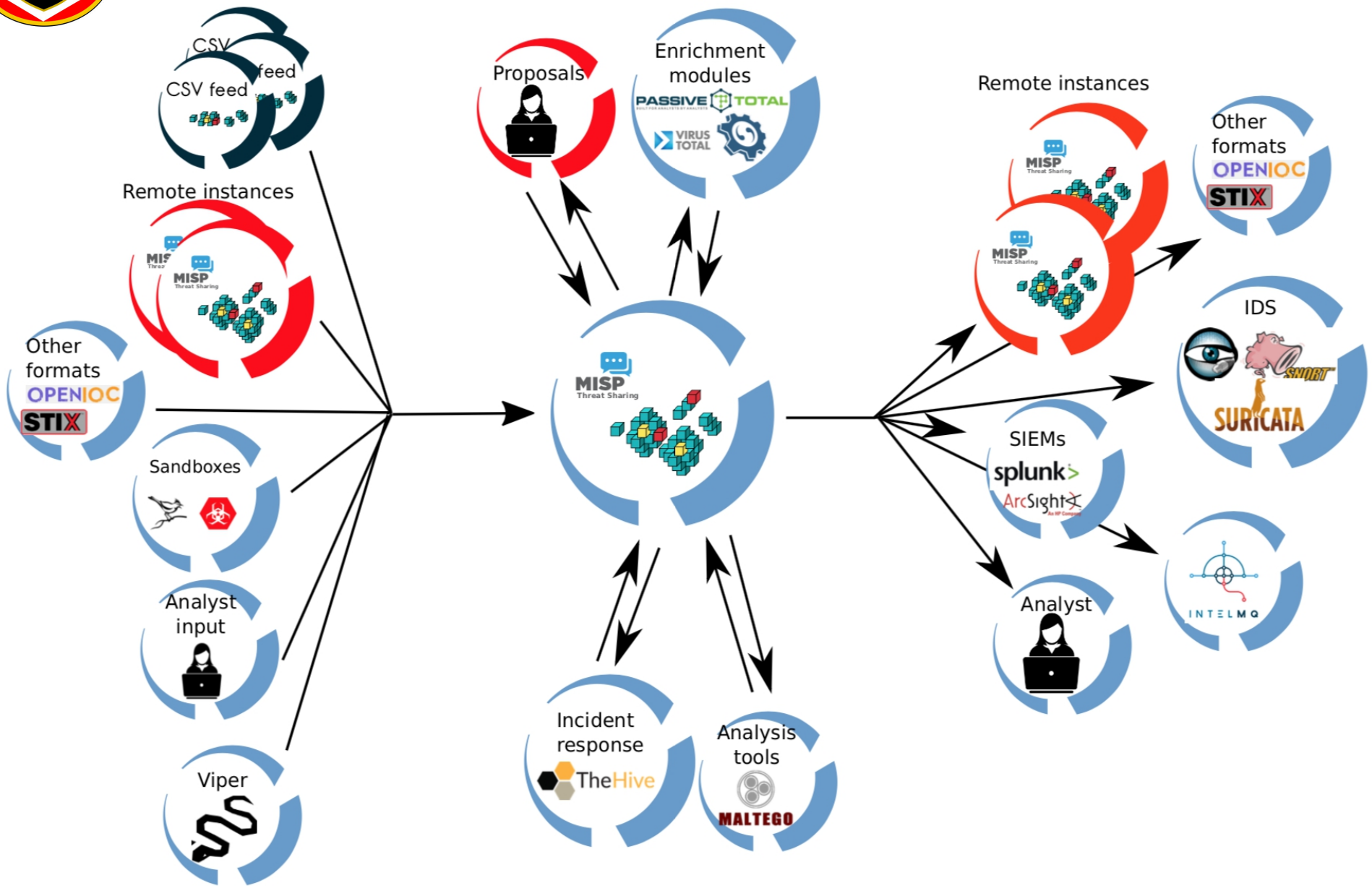
Modelo de colaboração entre instâncias



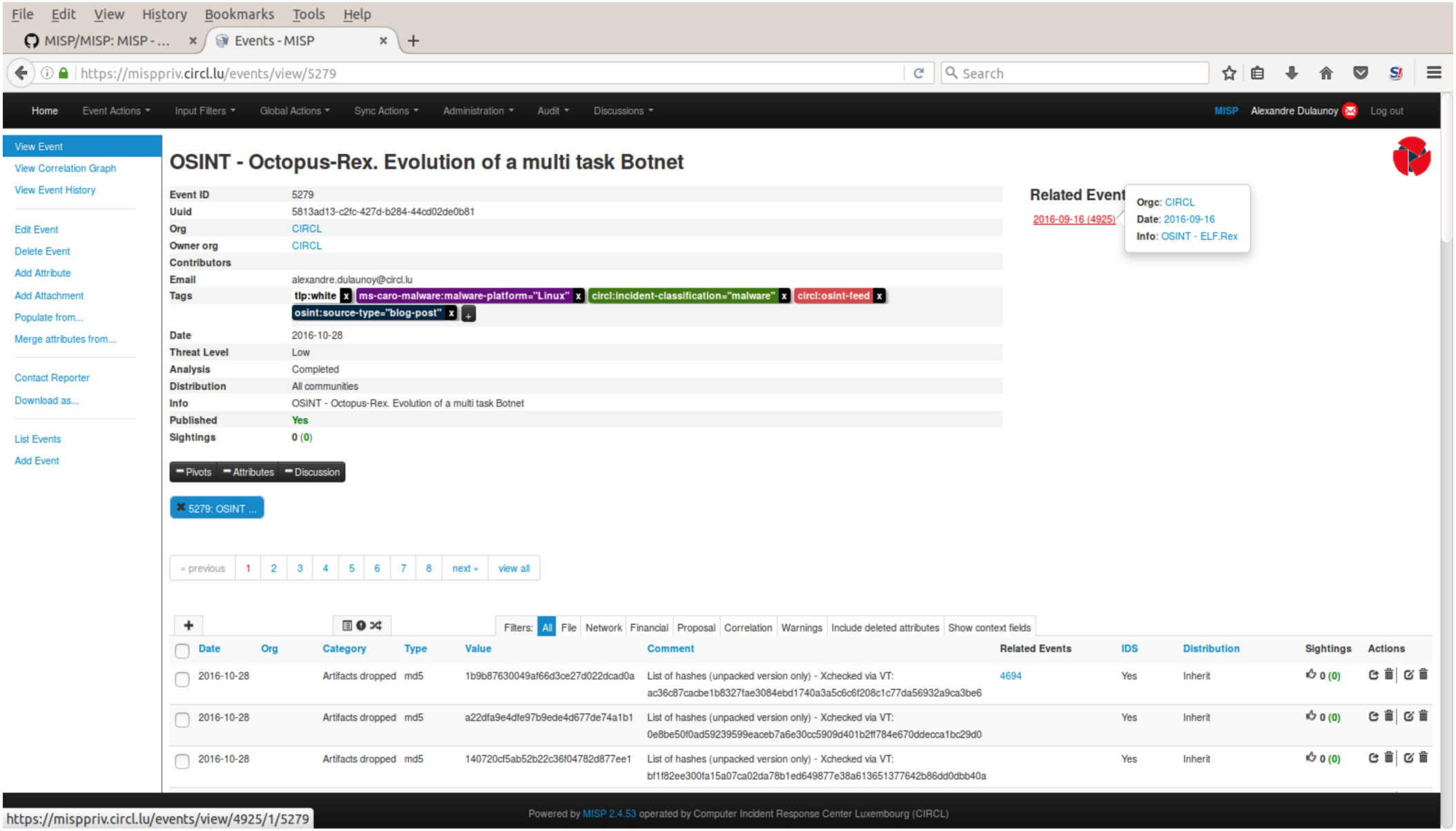
Sincronização entre instâncias



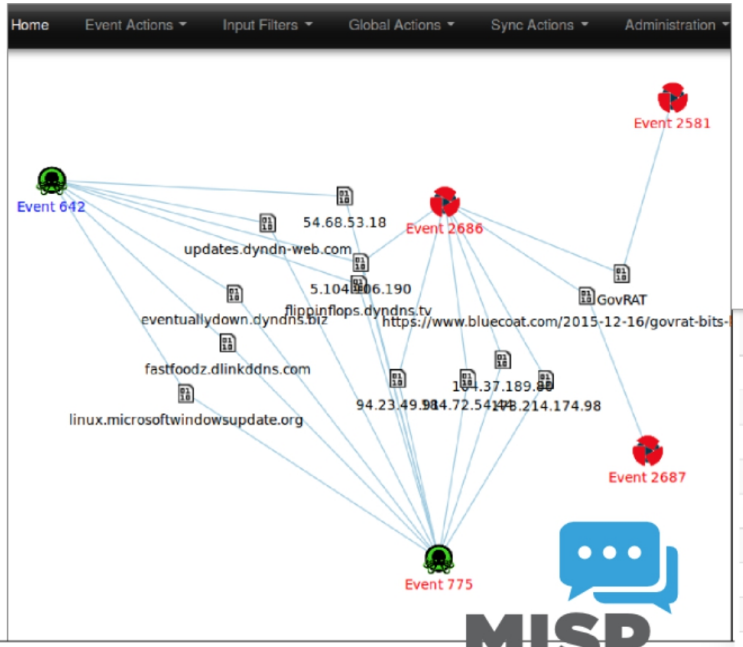
Fluxo de informações



Workflow


File Edit View History Bookmarks Tools Help
MISP/MISP: MISP - ...
Events - MISP
https://misppriv.circl.lu/events/view/5279
Search
Home Event Actions Input Filters Global Actions Sync Actions Administration Audit Discussions
MISP Alexandre Dulaunoy Log out
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from...
Merge attributes from...
Contact Reporter
Download as...
List Events
Add Event
OSINT - Octopus-Rex. Evolution of a multi task Botnet
Event ID 5279
Uuid 5813ad13-c2fc-427d-b284-44cd02de0b81
Org CIRCL
Owner org CIRCL
Contributors
Email alexandre.dulaunoy@circl.lu
Tags tlp:white ms-caro-malware:malware-platform="Linux" circl:incident-classification="malware" circl:osint-feed osint:source-type="blog-post"
Date 2016-10-28
Threat Level Low
Analysis Completed
Distribution All communities
Info OSINT - Octopus-Rex. Evolution of a multi task Botnet
Published Yes
Sightings 0 (0)
Related Event
2016-09-16 (4925)
Orgc: CIRCL
Date: 2016-09-16
Info: OSINT - ELF.Rex
Pivots Attributes Discussion
5279: OSINT ...
« previous 1 2 3 4 5 6 7 8 next » view all
Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields
Date Org Category Type Value Comment Related Events IDS Distribution Sightings Actions
2016-10-28 Artifacts dropped md5 1b9b87630049af66d3ce27d022dcad0a List of hashes (unpacked version only) - Xchecked via VT: ac36c87cacbe1b8327fae3084ebd1740a3a5c6c6f208c1c77da56932a9ca3be6 4694 Yes Inherit 0 (0)
2016-10-28 Artifacts dropped md5 a22dfa9e4dfe97b9ede4d677de74a1b1 List of hashes (unpacked version only) - Xchecked via VT: 0e8be50f0ad59239599eaceb7a6e30cc5909d401b2ff784e670ddecca1bc29d0 Yes Inherit 0 (0)
2016-10-28 Artifacts dropped md5 140720cf5ab52b22c36f04782d877ee1 List of hashes (unpacked version only) - Xchecked via VT: bf1f82ee300fa15a07ca02da78b1ed649877e38a613651377642b86dd0dbb40a Yes Inherit 0 (0)
https://misppriv.circl.lu/events/view/4925/1/5279
Powered by MISP 2.4.53 operated by Computer Incident Response Center Luxembourg (CIRCL)

Correlação de Eventos



TLP Taxonomy Library

Id	3
Namespace	tlp
Description	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
Version	1
Enabled	Yes (disable)

« previous next »

Filter

Tag	Expanded	Events	Tag	Action
tip:red	(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	
tip:amber	(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	
tip:green	(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	
tip:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	
tip:ex:chr	(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	

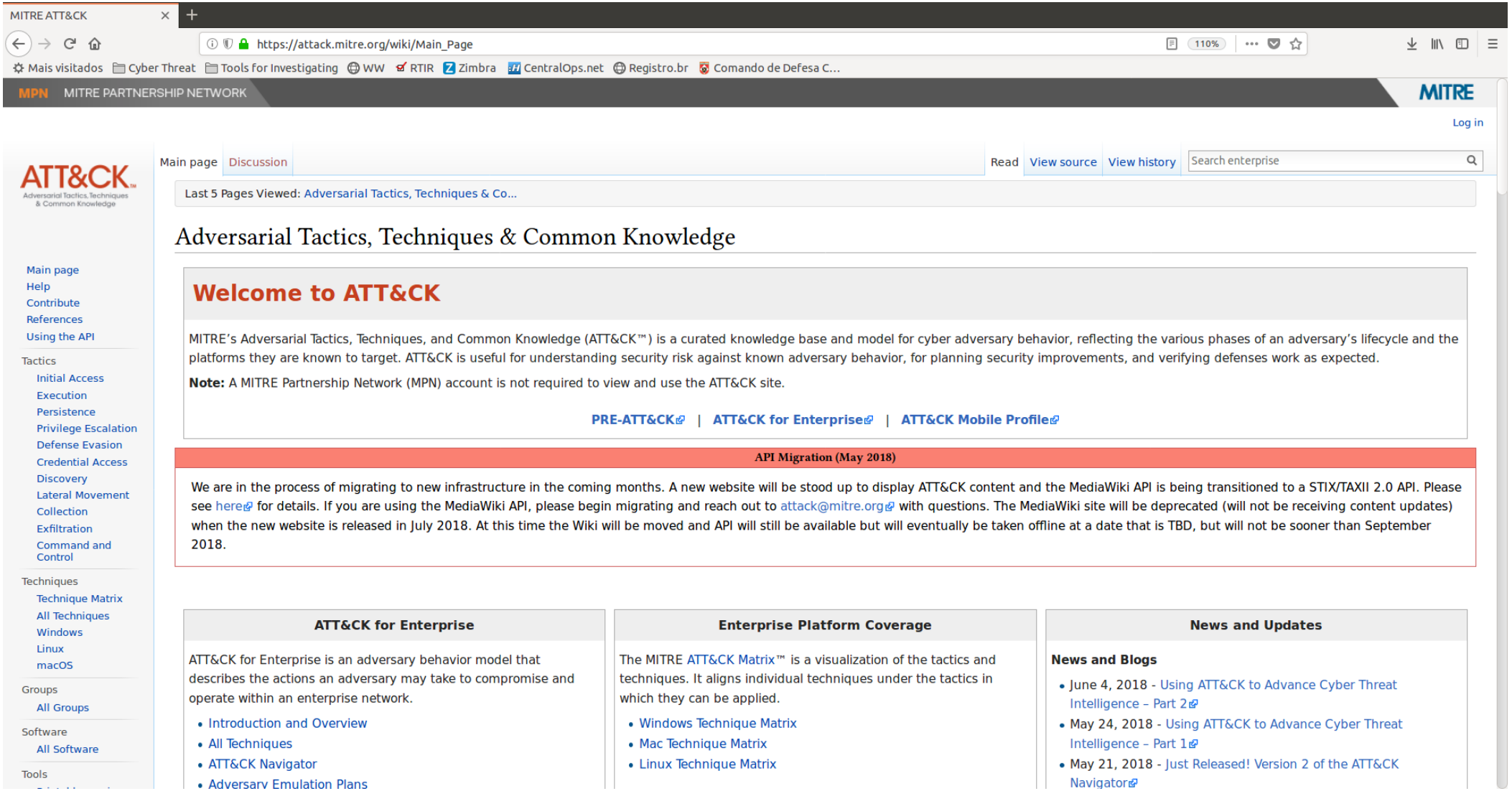
Id	Exportable	Name	Taxonomy	Tagged events	Actions
6	✖	APT		31	
7	✖	Actionable:NO		5	
3	✖	TLP:AMBER	tlp	131	
8	✖	TLP:EX:CHR	tlp	11	
5	✖	TLP:GREEN	tlp	550	
4	✖	TLP:RED	tlp	3	
2	✖	TLP:WHITE	tlp	531	
10	✖	TO:HIDE		2	
9	✖	TODO		9	
11	✖	TODO:VT-ENRICHMENT		8	
1	✖	Type:OSINT		832	
18	✔	admiralty-scale:information-credibility="1"	admiralty-scale	0	
19	✔	admiralty-scale:information-credibility="2"	admiralty-scale	0	
20	✔	admiralty-scale:information-credibility="3"	admiralty-scale	0	
21	✔	admiralty-scale:information-credibility="4"	admiralty-scale	0	
22	✔	admiralty-scale:information-credibility="5"	admiralty-scale	0	
23	✔	admiralty-scale:information-credibility="6"	admiralty-scale	0	

Ecossistema

- Malware
- Network
- Threat Info
- Forensic data
- TTP
- Finance / Fraud
- IoC
- Enrichment
- API
- Import/Export
- IR Platforms
- Security devices

MISP

MISP 2.4.93 released (aka ATT&CK integration)



MISP 2.4.93 released (aka ATT&CK integration)

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

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

Comunidades

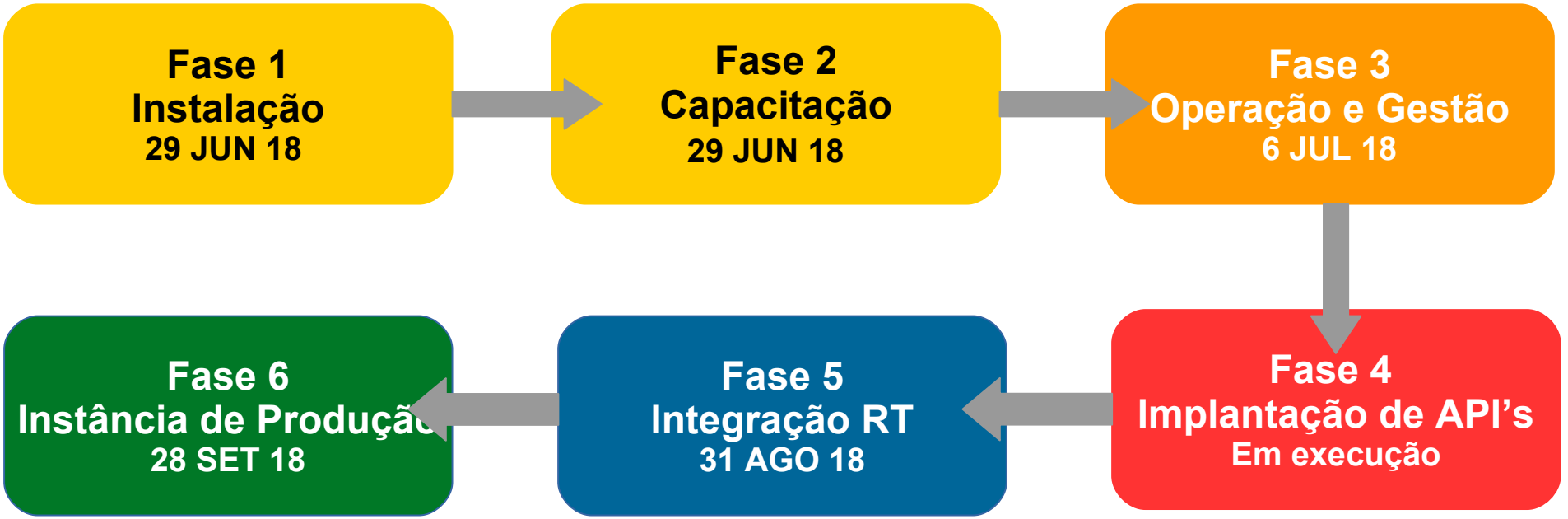
Comunidades Nacionais (propostas)

Instância do MISP
CTIR Militar

Instância do MISP
CTIR Gov
(APF e Estruturas Estratégicas)

CTIR Gov

Plano de Trabalho para Implantação



Reuniões de Especialistas

- Objetivo: trocas de **lições aprendidas** sobre a implantação, operação, suporte, segurança e infraestrutura.
- Foi criado um **Grupo de WhatsApp** com especialistas de vários setores de infraestrutura estratégica (órgãos de governo da APF, financeiro, telecomunicações e energia).
- A 1ª reunião foi realizada em **12 JUL 18** no **CTIR Gov** com a presença do militares do CDCiber, CTIR Gov e BRB.
- Próxima reunião agendada para **300930 AGO 2018.**

Conclusão

O segredo do compartilhamento de informações **é compartilhar mais (e melhor)** do que seus adversários!

Conclusão

- O MISP **é apenas uma ferramenta**. O que importa são as suas práticas de compartilhamento.

- Transparência nos processos de colaboração entre diversas equipes de segurança que podem **interconectar e sincronizar** as informações entre elas.

Centro de Defesa Cibernética

Forte Marechal Rondon
Estrada Parque do Contorno, Rodovia DF-001, km 05
Setor Habitacional Taquari - Lago Norte
Brasília - Distrito Federal
CEP: 71.559-902 - Brasília/DF
(61) 3415-3702
(61) 3415-3600