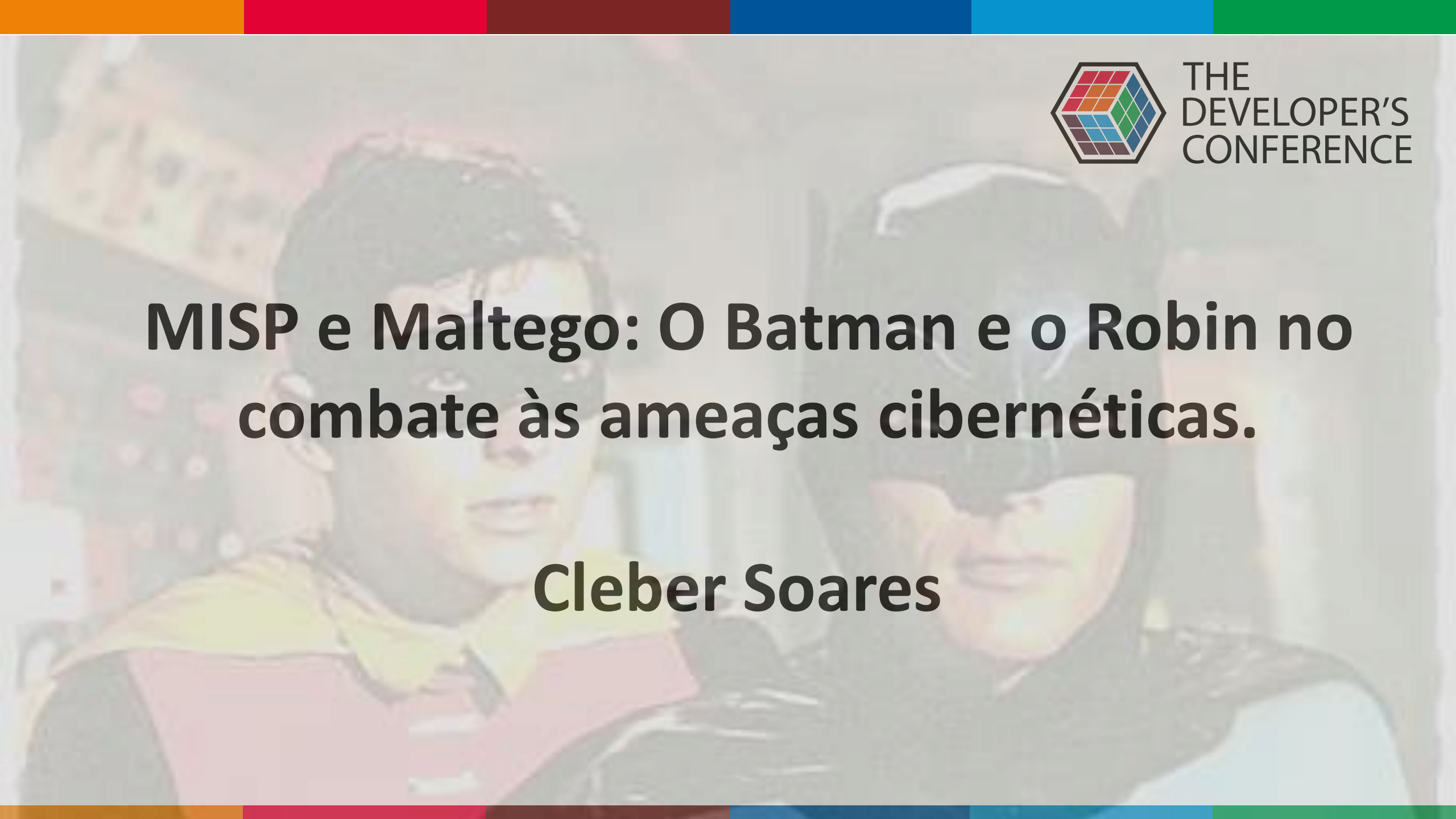
THE DEVELOPER'S CONFERENCE

Trilha – SOFTWARE SECURITY

Cleber Soares



THE DEVELOPER'S CONFERENCE

MISP e Maltego: O Batman e o Robin no combate às ameaças cibernéticas.

Cleber Soares

Csoares@localhost:~#Whoami

THE DEVELOPER'S CONFERENCE

Curso técnico em processamento de dados;

Graduação - Redes Computadores;

Pós em Redes computadores;

Pós em Ethical Hacking CyberSecurity;

Pós em graduando Forense Computacional ;

OWASP Belém-PA

DIFORSEC


SIEM
DLP
WAF
Firewall
Endpoint Security
IDS/IPS
Proxy + Filtro de conteúdo

WEF Cybersecurity
@WEFCybersec

Yet again, #Cybersecurity remains a top of mind risk in the @wef 's #globalrisks Report 2021 weforum.org/reports/the-gl...

4:47 PM · 19 de jan de 2021 · TweetDeck

14 Retweets **3** Tweets com comentário

17 Curtidas

https://twitter.com/WEFCybersec/status/1351617299162288128

Estimativa de danos 2025.

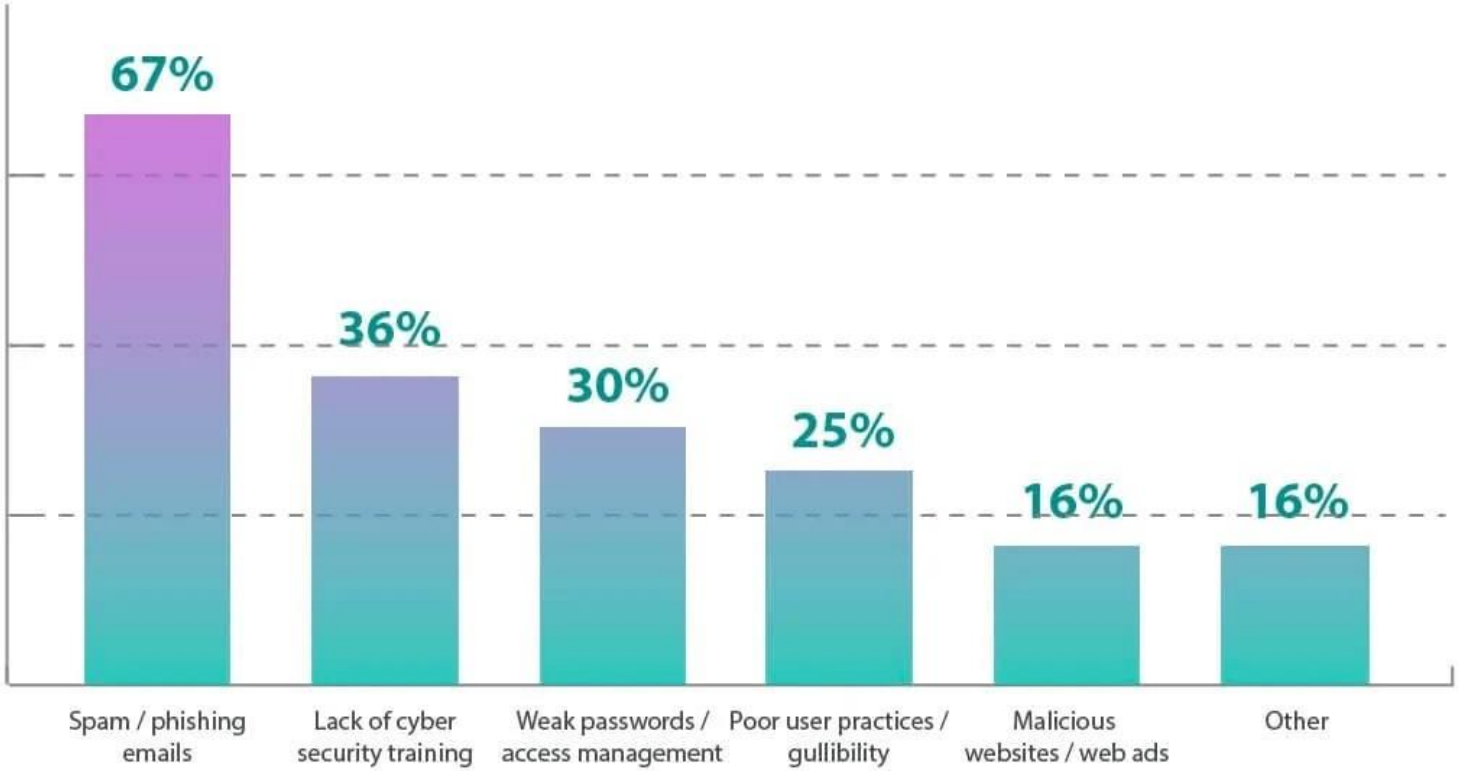
THE DEVELOPER'S CONFERENCE

https://cybersecurityventures.com

MOST COMMON METHODS OF RANSOMWARE INFECTIONS IN NORTH AMERICA

THE DEVELOPER'S CONFERENCE

Based on MSPs reporting attacks on organizations. (Some were targeted by more than one method.)



Managed Service Providers were asked which were the most common ransomware delivery methods they've seen for their clients

SafetyDetectives

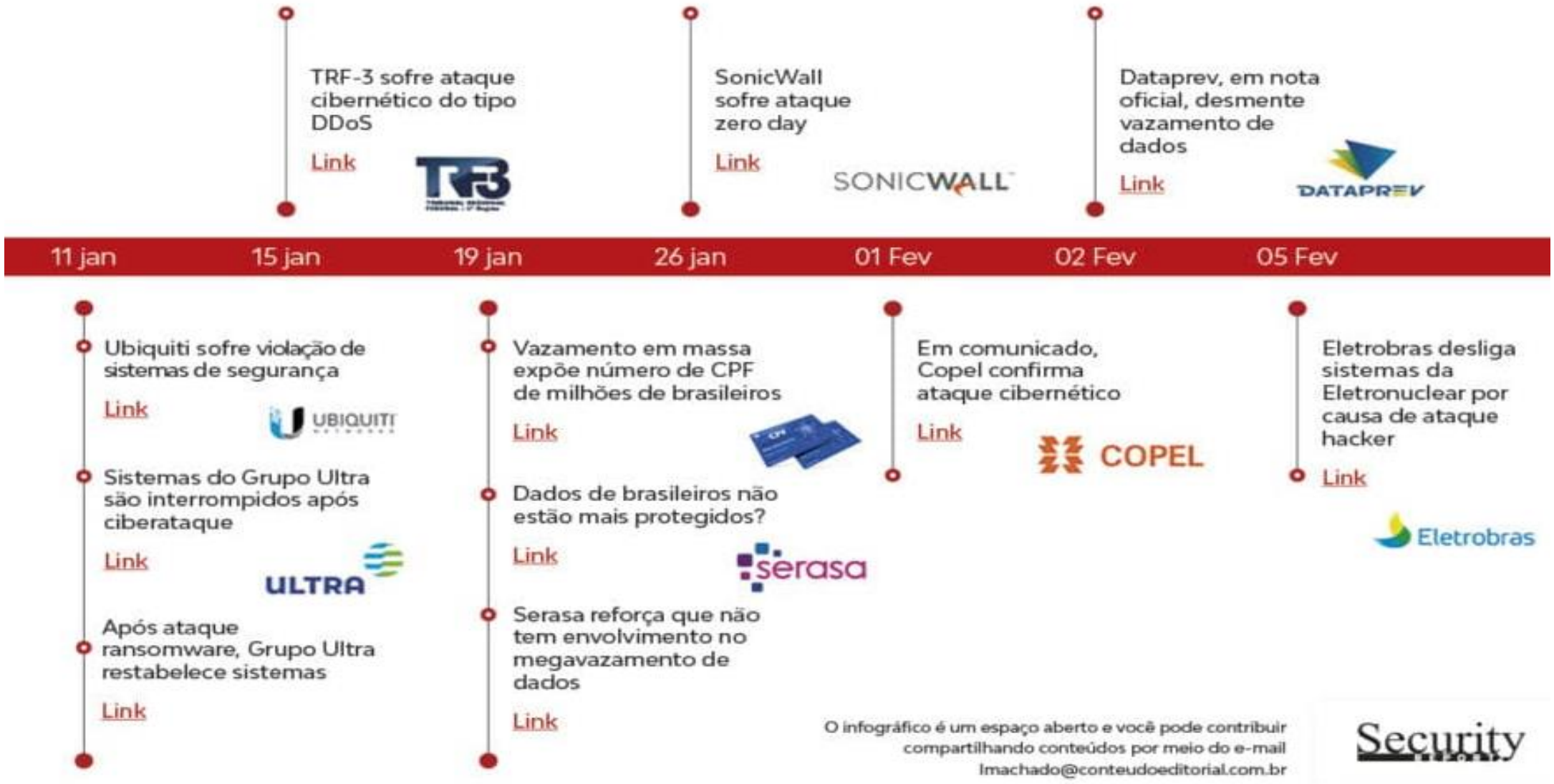
https://purplesec.us/cyber-security-trends-2021/

THE DEVELOPER'S CONFERENCE

Incidente de segurança

"Incidente de segurança é qualquer evento indesejado ou inesperado que seja confirmado ou sob suspeita, relacionado a comprometer a segurança de sistemas de computação, de redes e dos dados pessoais, expondo-os a acessos não autorizados, modificações de sistema sem o consentimento."

PAINEL DE INCIDENTES CIBERNÉTICOS 2021



https://www.securityreport.com.br/

Resposta a incidentes

THE DEVELOPER'S CONFERENCE

"É um conjunto de metodologias que visam conter e minimizar os impactos de um incidente cibernético, sejam fruto de um ataque, mal uso, ou mesmo um desastre de grandes proporções."

Joas Antonio

Metodologias resposta incidente

NIST

SANS

ISO
27035

Etapas de resposta a incidentes

THE DEVELOPER'S CONFERENCE

NIST	SANS
1.Preparação	1.Preparação
2.Detecção e Análise	2.Identificação
3.Contenção, erradicação e recuperação	3.Contenção
	4.Erradicação
	5.Recuperação
4.Atividade Pós-Incidente	6.Lições aprendidas

https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response

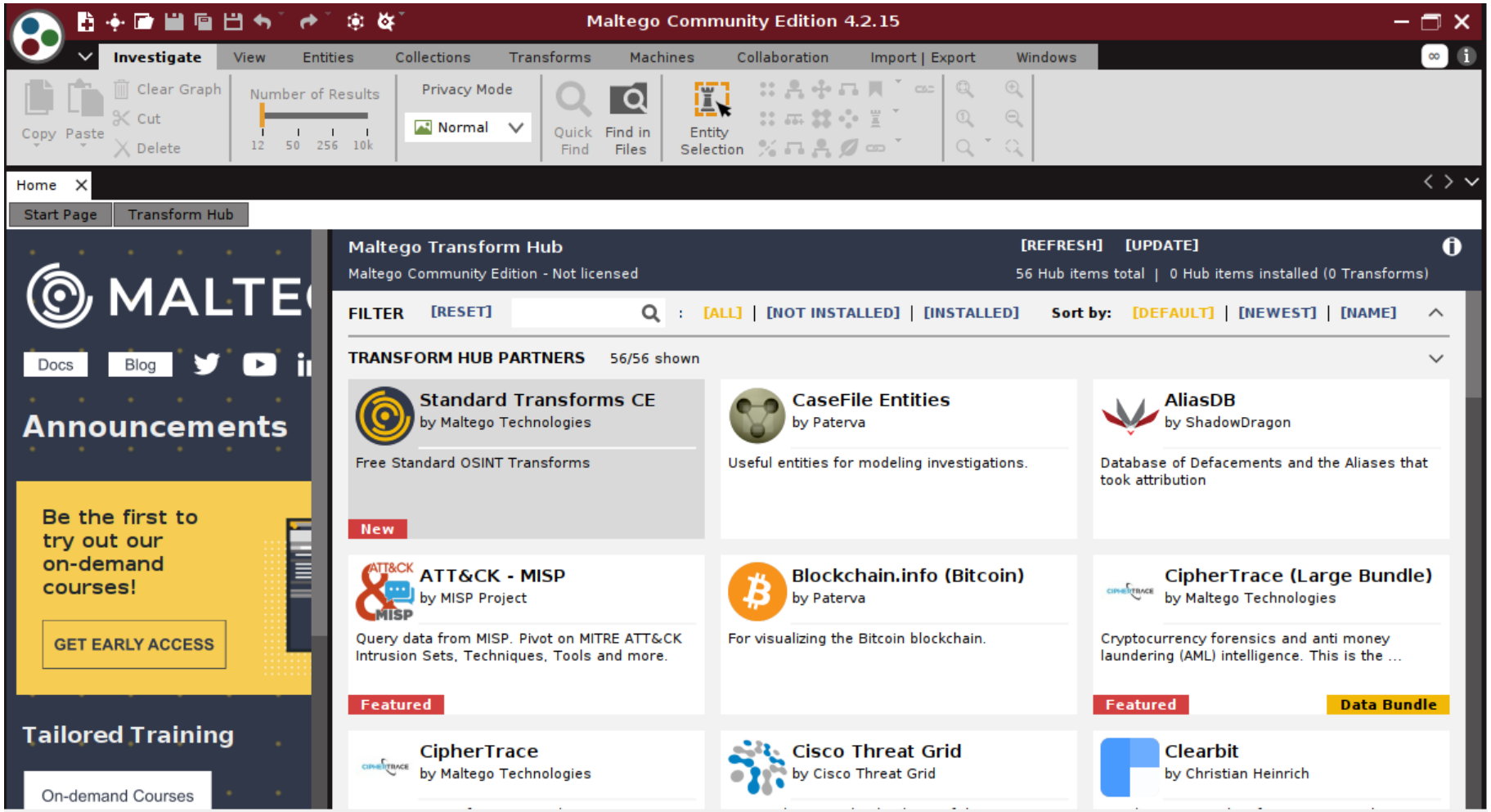
THE
DEVELOPER'S
CONFERENCE

MISP
Threat Sharing

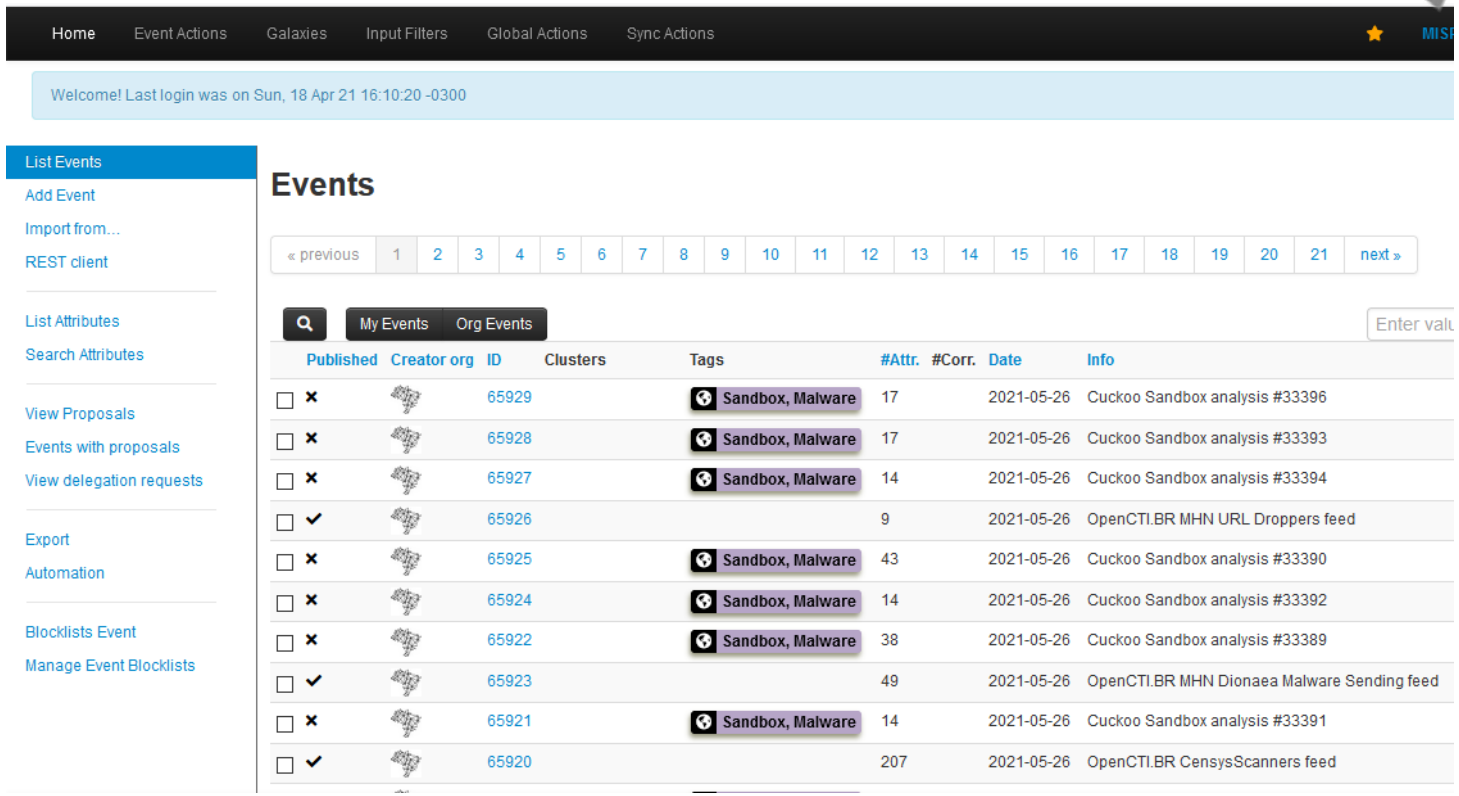
MALTEGO

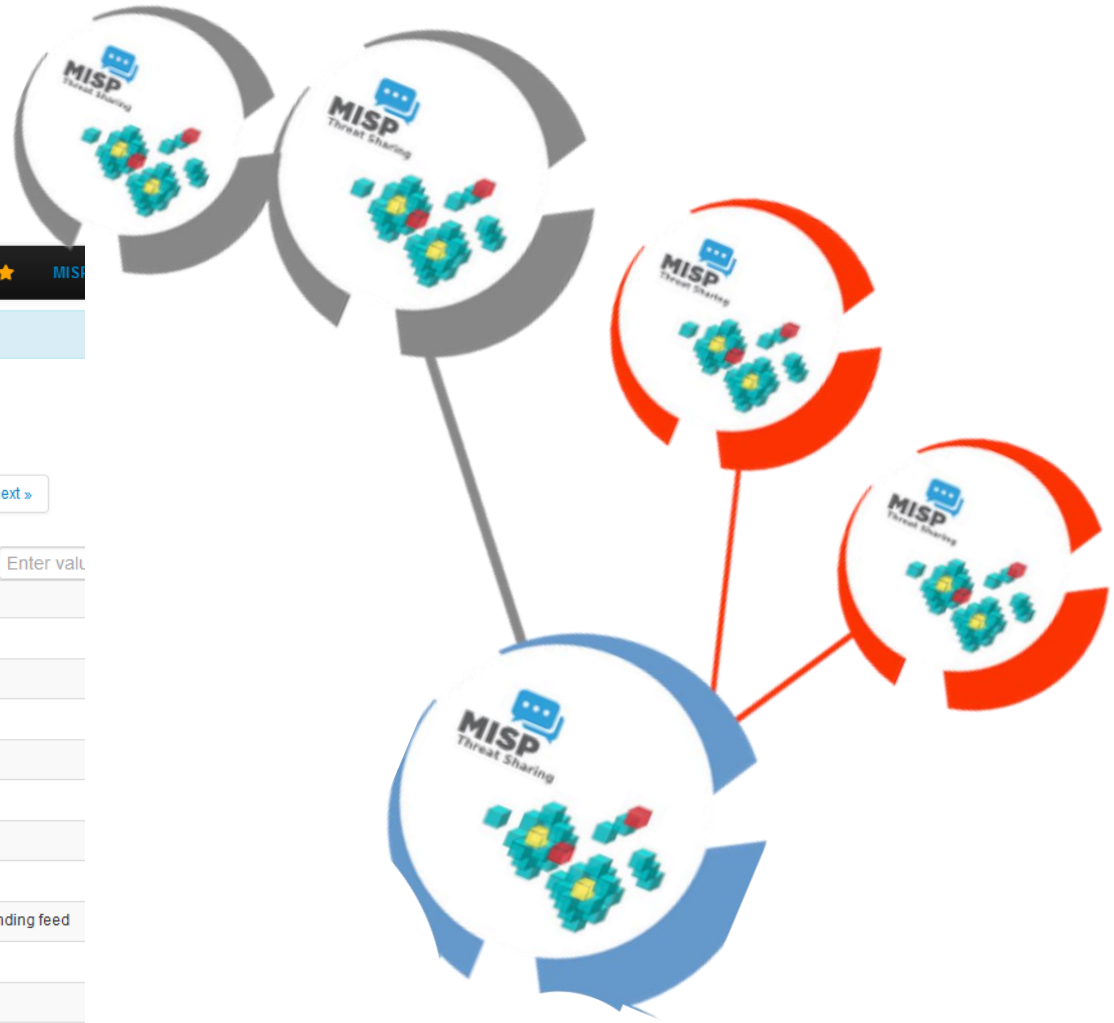
Maltego CE

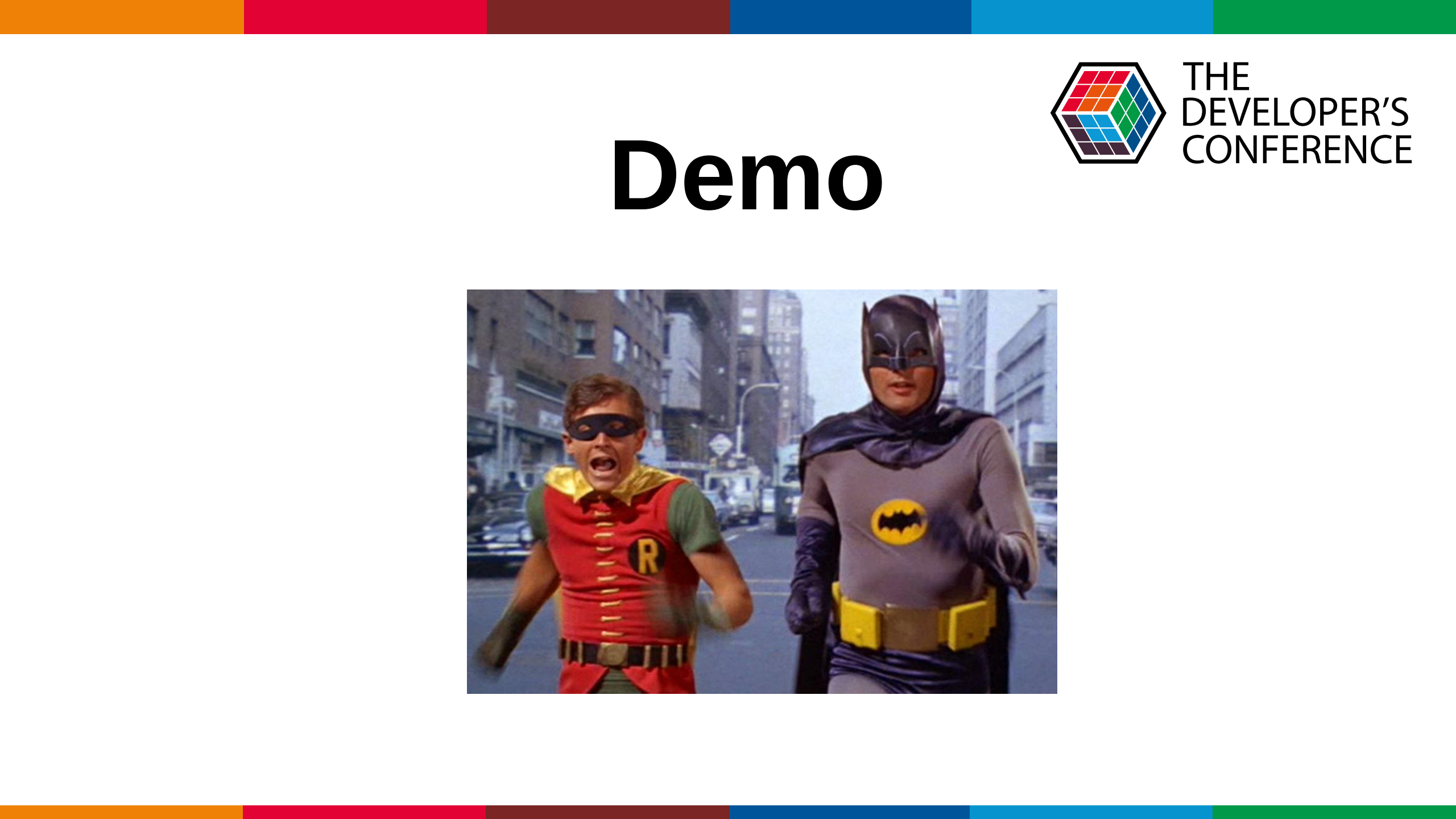
THE DEVELOPER'S CONFERENCE



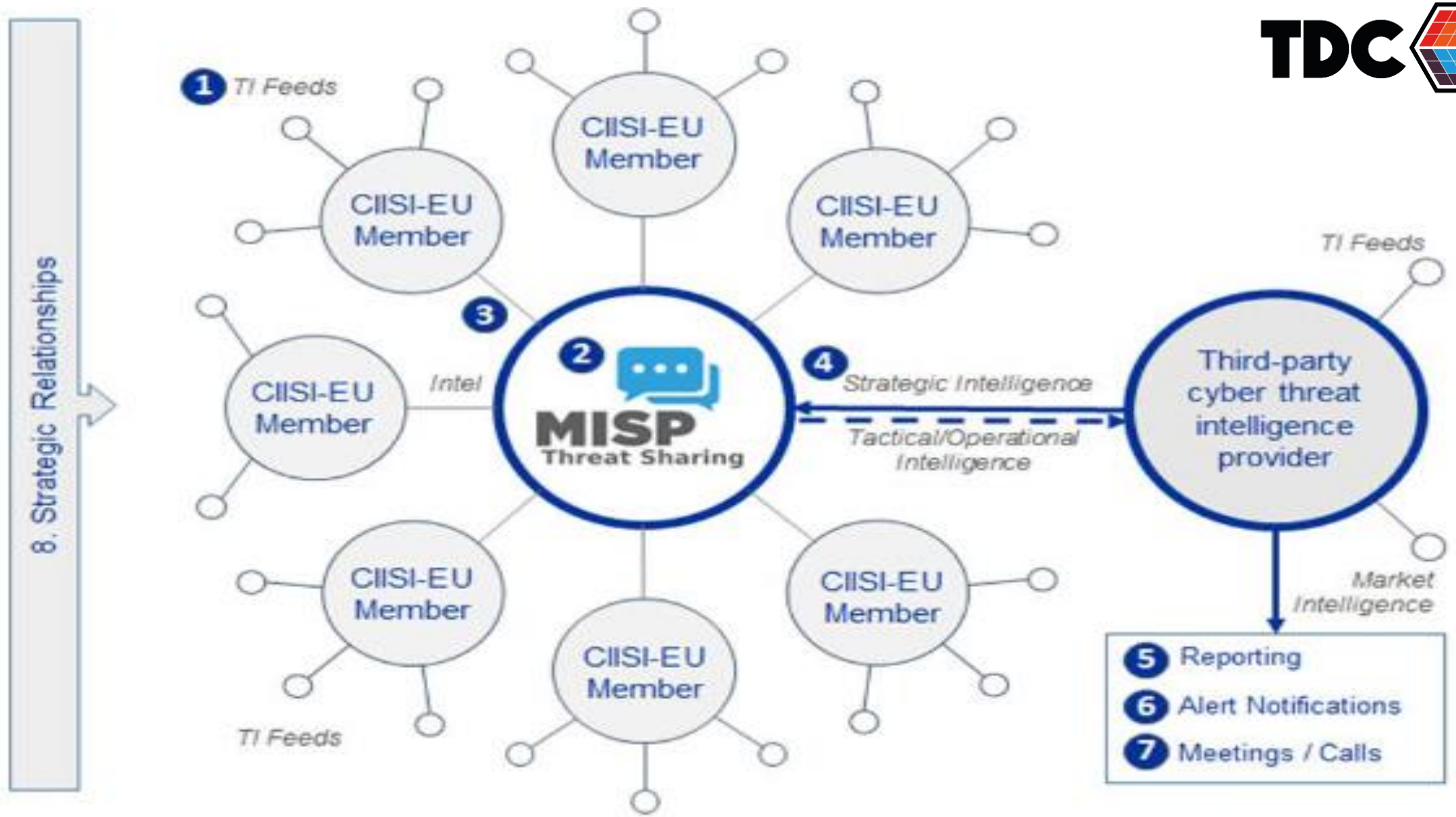
MISP- (Malware Information Sharing Platform)







Demo



https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ciisi-eu_practical_example.pdf

OpenCTIBr

THE DEVELOPER'S CONFERENCE

OpenCTI

Um projeto sem fins lucrativos, mantido por entusiastas e profissionais da área de segurança de TI, que visa contribuir e incentivar o compartilhamento de informações sobre ameaças cibernéticas na comunidade brasileira.

ThreatDB

Centralizamos e contextualizamos as ameaças reportadas por diferentes fontes através do MISP (Malware Information Sharing Platform).

Threat Feeds

Disponibilizamos diariamente em nosso repositório no Github, informações de ameaças cibernéticas no formato Threat Feeds.

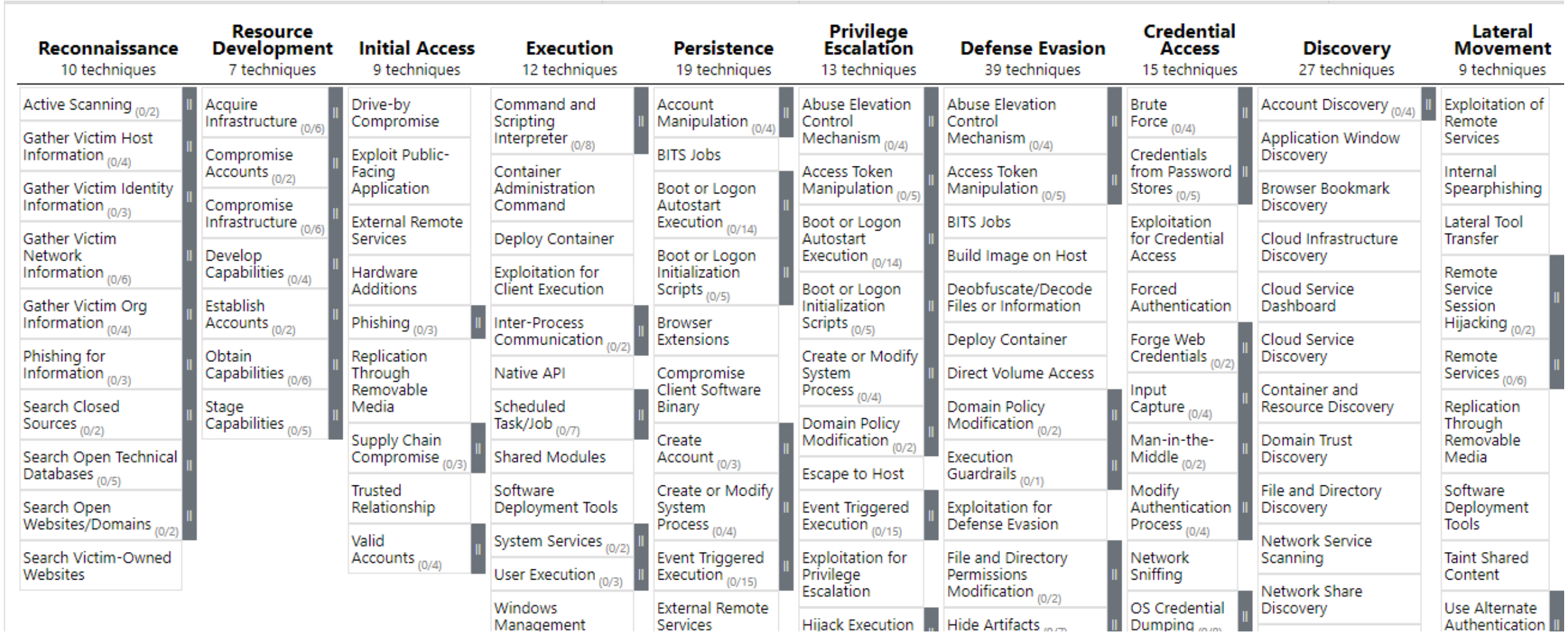
Sandbox Analysis

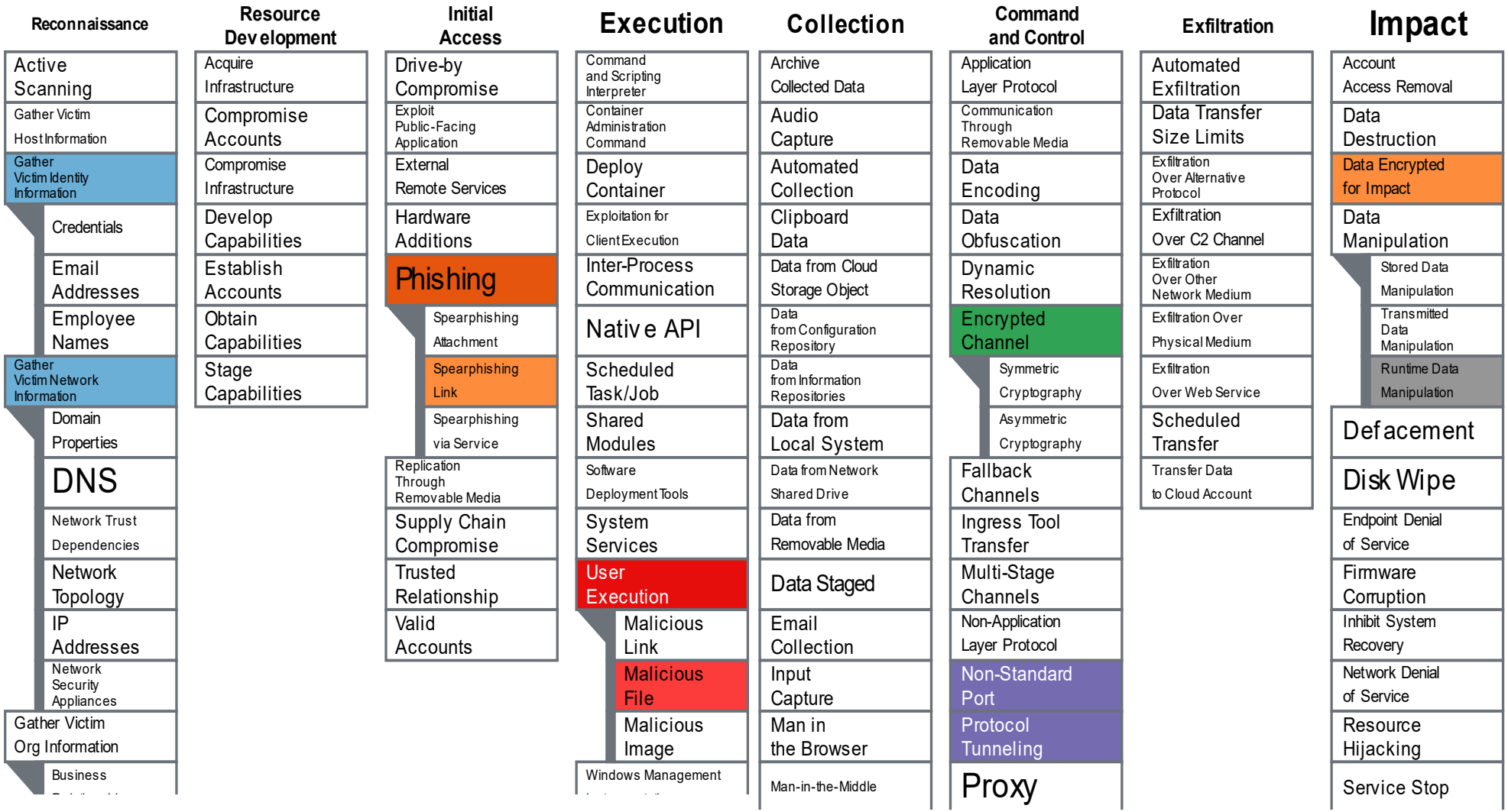
Um ambiente projetado para automação de análise de malware em grandes quantidades.

https://www.opencti.net.br

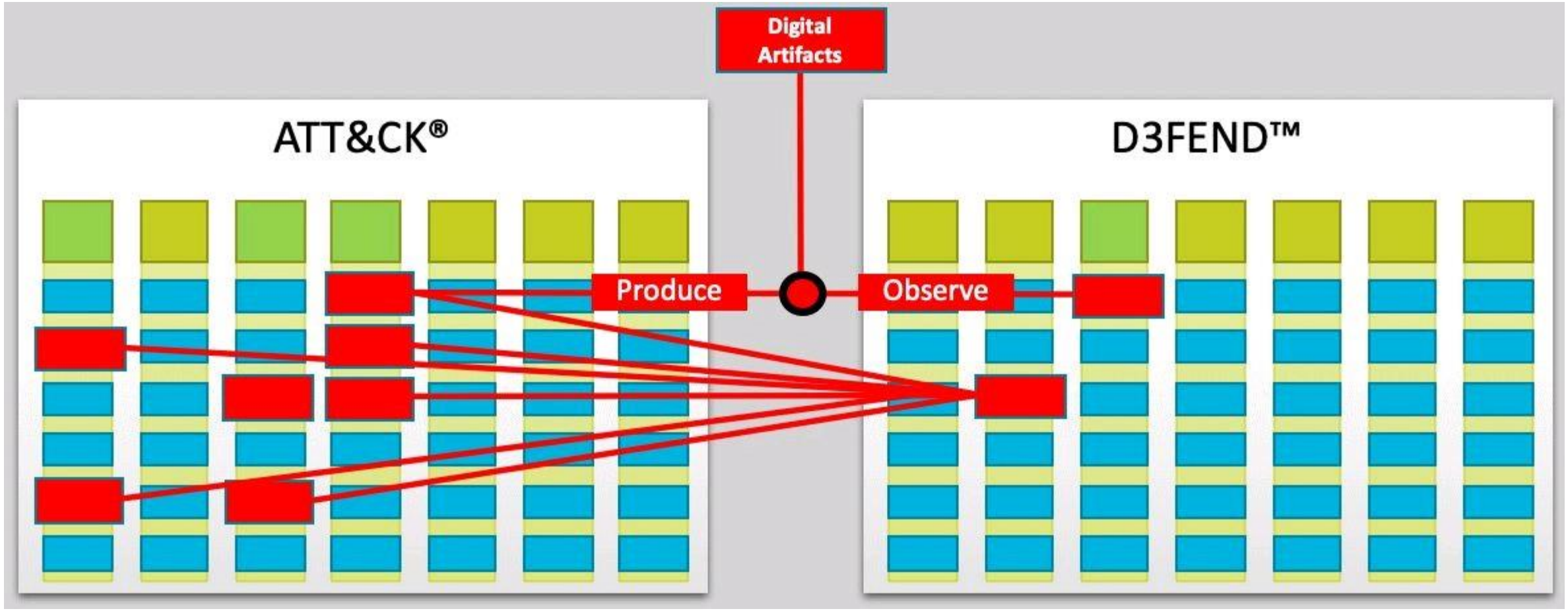
Mitre-Att&ck

THE DEVELOPER'S CONFERENCE




Reconnaissance
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Credentials
Email Addresses
Employee Names
Gather Victim Network Information
Domain Properties
DNS
Network Trust Dependencies
Network Topology
IP Addresses
Network Security Appliances
Gather Victim Org Information
Business
Resource Development
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Malicious Link
Malicious File
Malicious Image
Windows Management
Collection
Archive Collected Data
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Man-in-the-Middle
Command and Control
Application Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Symmetric Cryptography
Asymmetric Cryptography
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Exfiltration
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account
Impact
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Stored Data Manipulation
Transmitted Data Manipulation
Runtime Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop

https://d3fend.mitre.org/



CSIRT (Computer Security Incident Response Team)

THE DEVELOPER'S CONFERENCE

- **Tratamento de incidentes;**
- **Notificação de Incidentes;**
- **Análise de Incidentes;**
- **Suporte à resposta a incidentes;**
- **Gerenciamento de vulnerabilidades;**
- **Educação e treinamento em segurança da informação;**

Modelo de plano de resposta a incidentes

THE DEVELOPER'S CONFERENCE

LOGO

Política de Segurança da Informação

Formulário de Incidente Segurança da Informação

Nome da Empresa

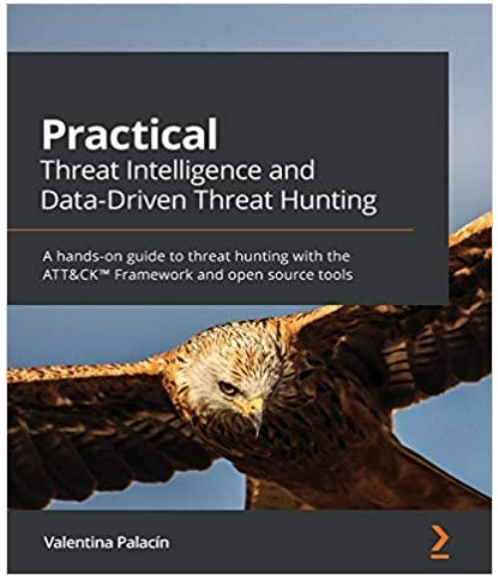
FORMULÁRIO PARA RELATAR UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO OU AÇÂO SUSPEITA		
Local:		Nome do Departamento:
Nome do remetente:	Telefone/ramal:	E-mail:

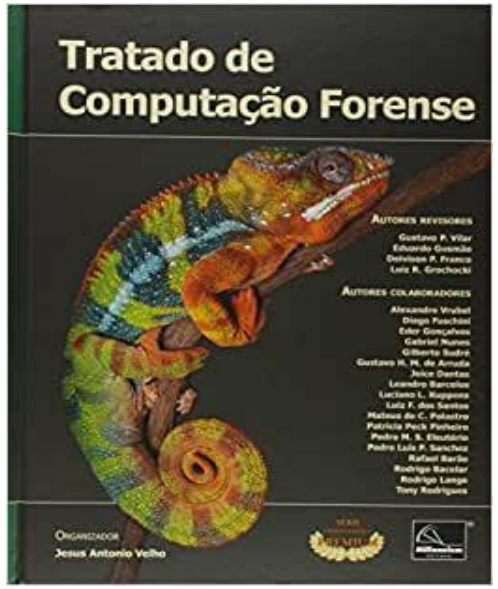
Data do Incidente:	Hora do Incidente:
Quem foi notificado:	Hora da notificação:
Descrição do Incidente:	

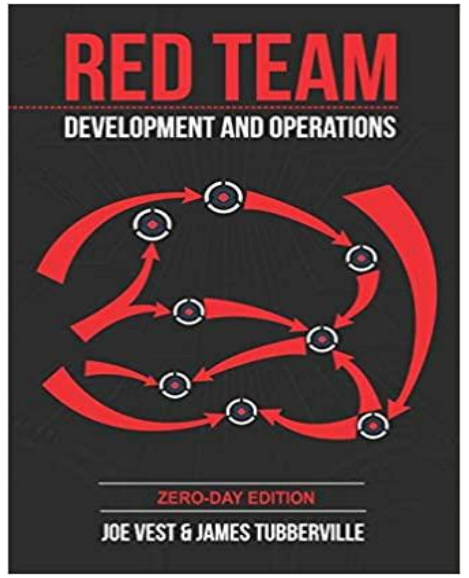
- https://www.socbrazil.com/downloads/
- https://purplesec.us/wp-content/uploads/2020/11/NIST-800-171-Incident-Response-Plan-Template.pdf

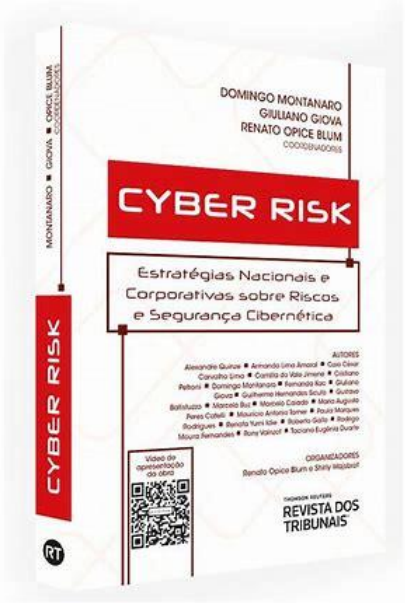
Algumas Referencias

THE DEVELOPER'S CONFERENCE









- https://www.misp-project.org/
- https://www.maltego.com/misp
- https://github.com/MISP/MISP-maltego

THE DEVELOPER'S CONFERENCE

Dúvidas?

Obrigado!!!

cleber.phishing@gmail.com