

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

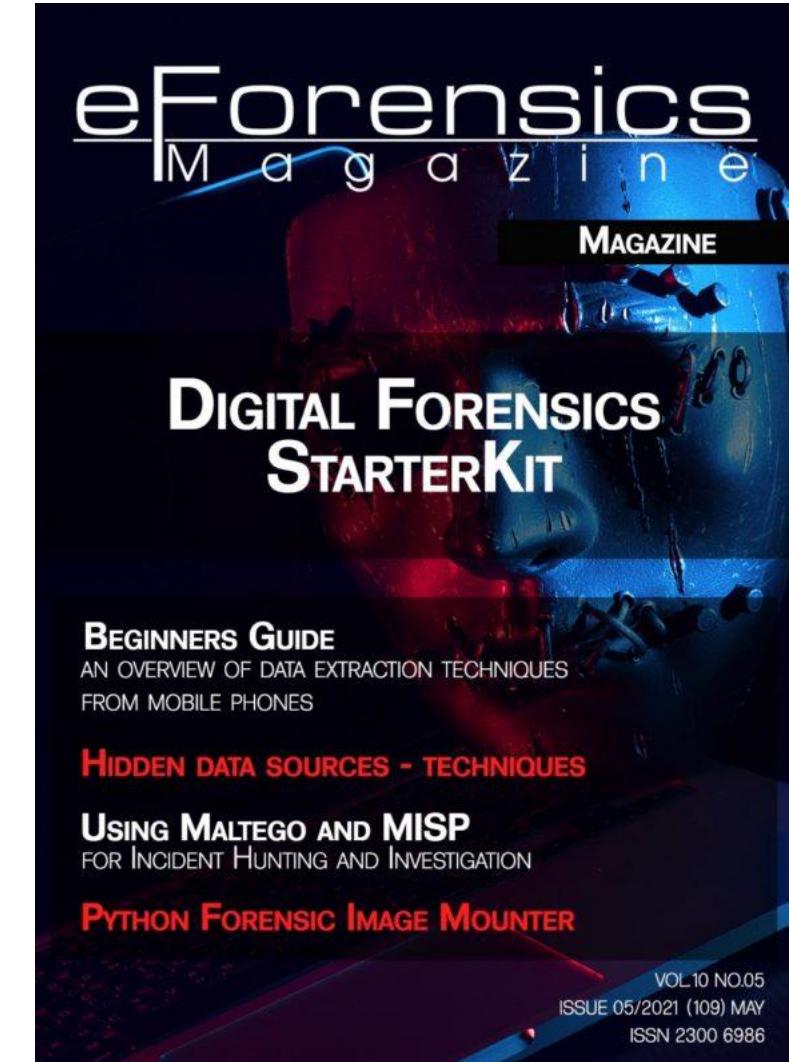
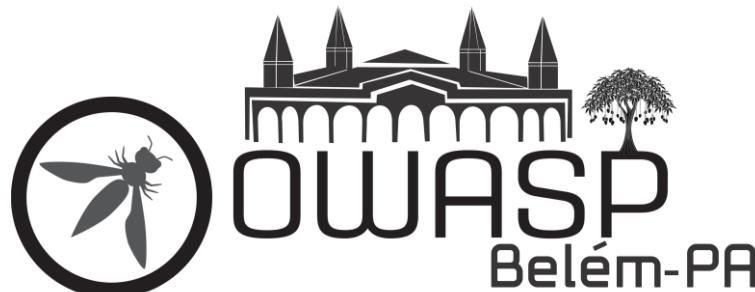
Curso técnico em processamento de dados;

Graduação - Redes Computadores;

Pós em Redes computadores;

Pós em Ethical Hacking CyberSecurity;

Pós em graduando Forense Computacional ;





SIEM

DLP

WAF

Firewall

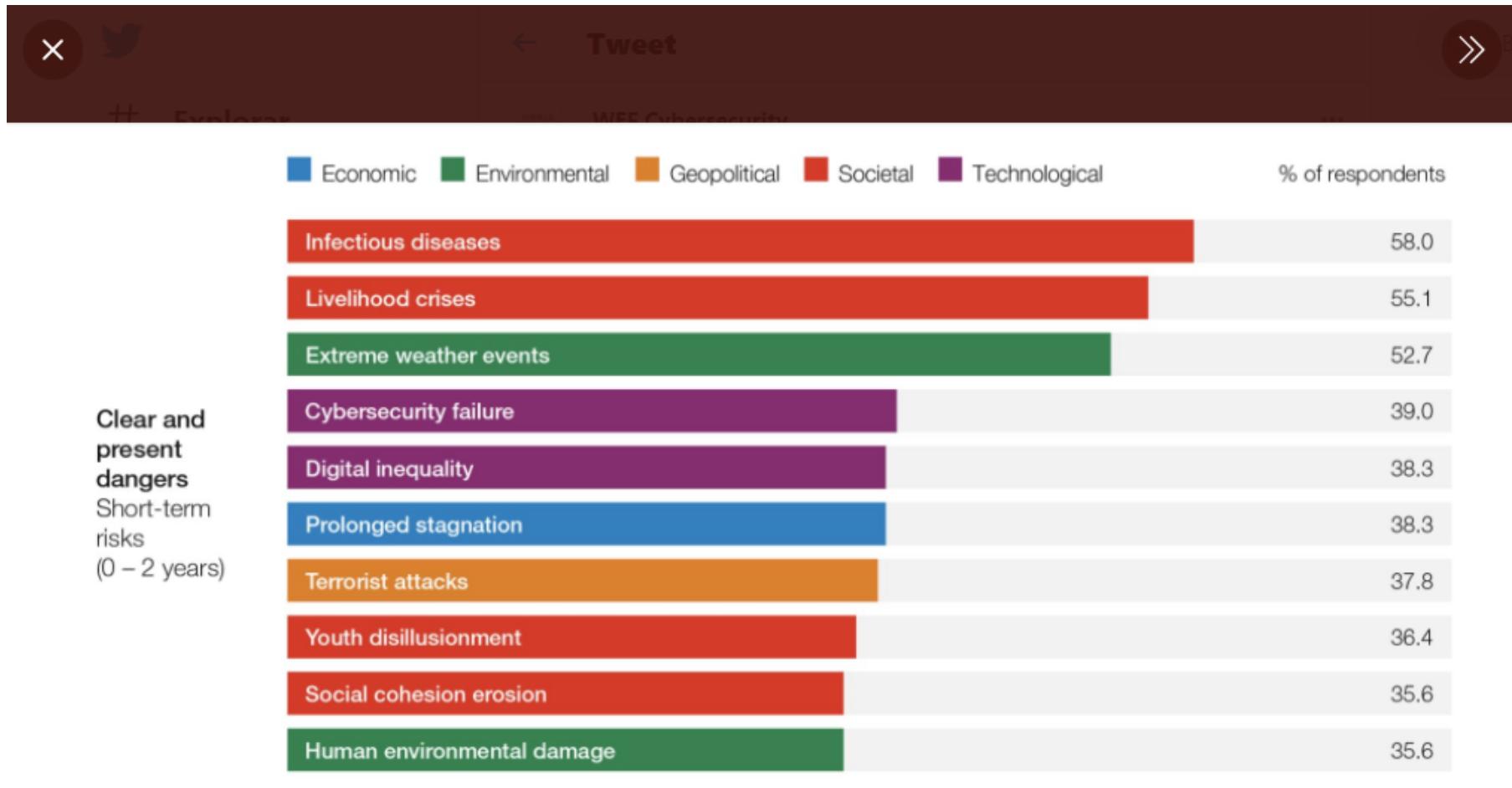
Endpoint Security

IDS/IPS

Proxy + Filtro de conteúdo



THE DEVELOPER'S CONFERENCE



WEF Cybersecurity
@WEFCybersec

...

Yet again, #Cybersecurity remains a top of mind risk in the @wef 's #globalisks Report 2021 [weforum.org/reports/the-gl...](https://weforum.org/reports/the-global-risks-report-2021/)

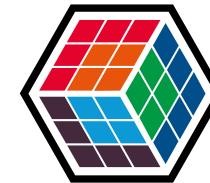
4:47 PM · 19 de jan de 2021 · TweetDeck

14 Retweets 3 Tweets com comentário

17 Curtidas



Estimativa de danos 2025.



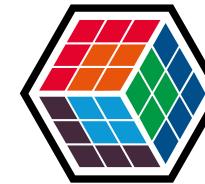
THE
DEVELOPER'S
CONFERENCE



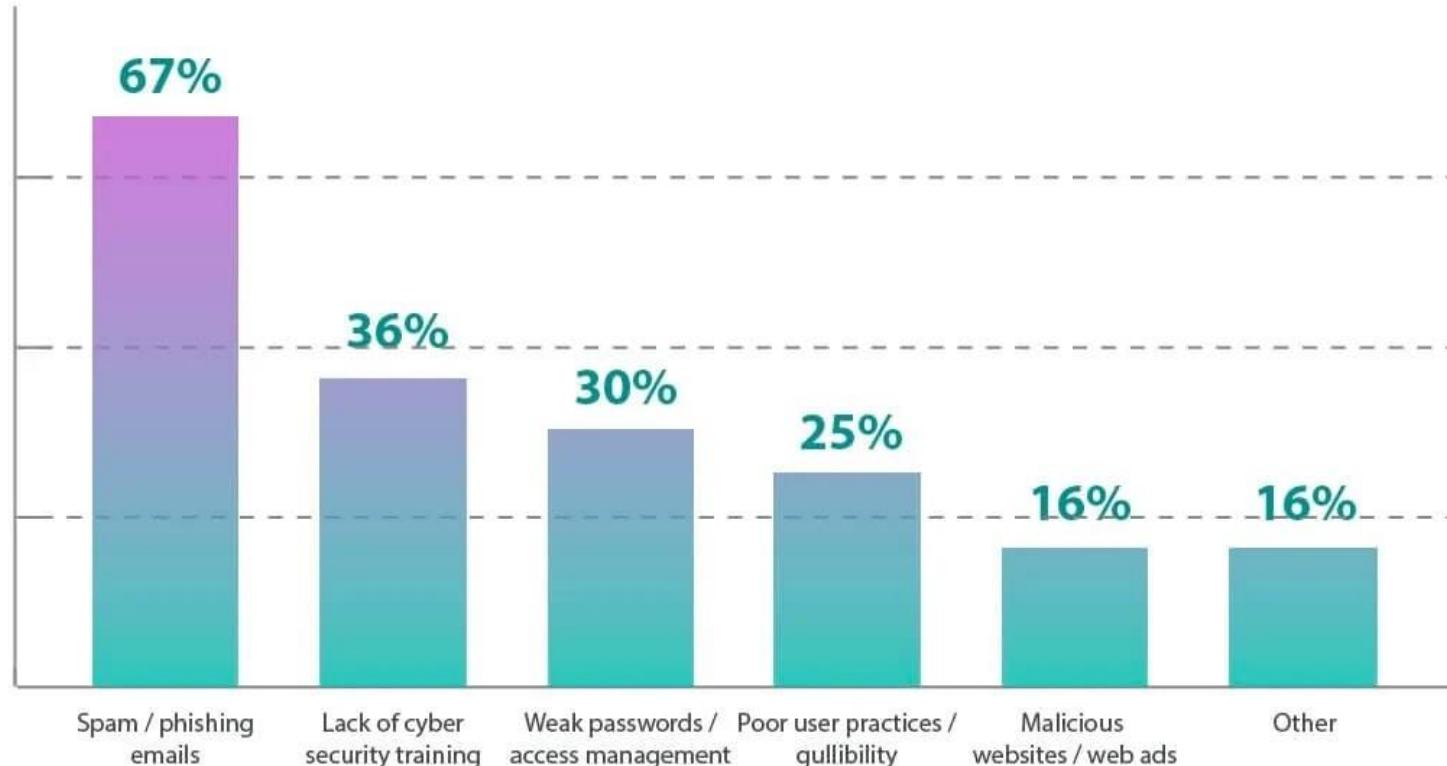
<https://cybersecurityventures.com>

MOST COMMON METHODS OF RANSOMWARE INFECTIONS IN NORTH AMERICA

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



THE
DEVELOPER'S
CONFERENCE



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



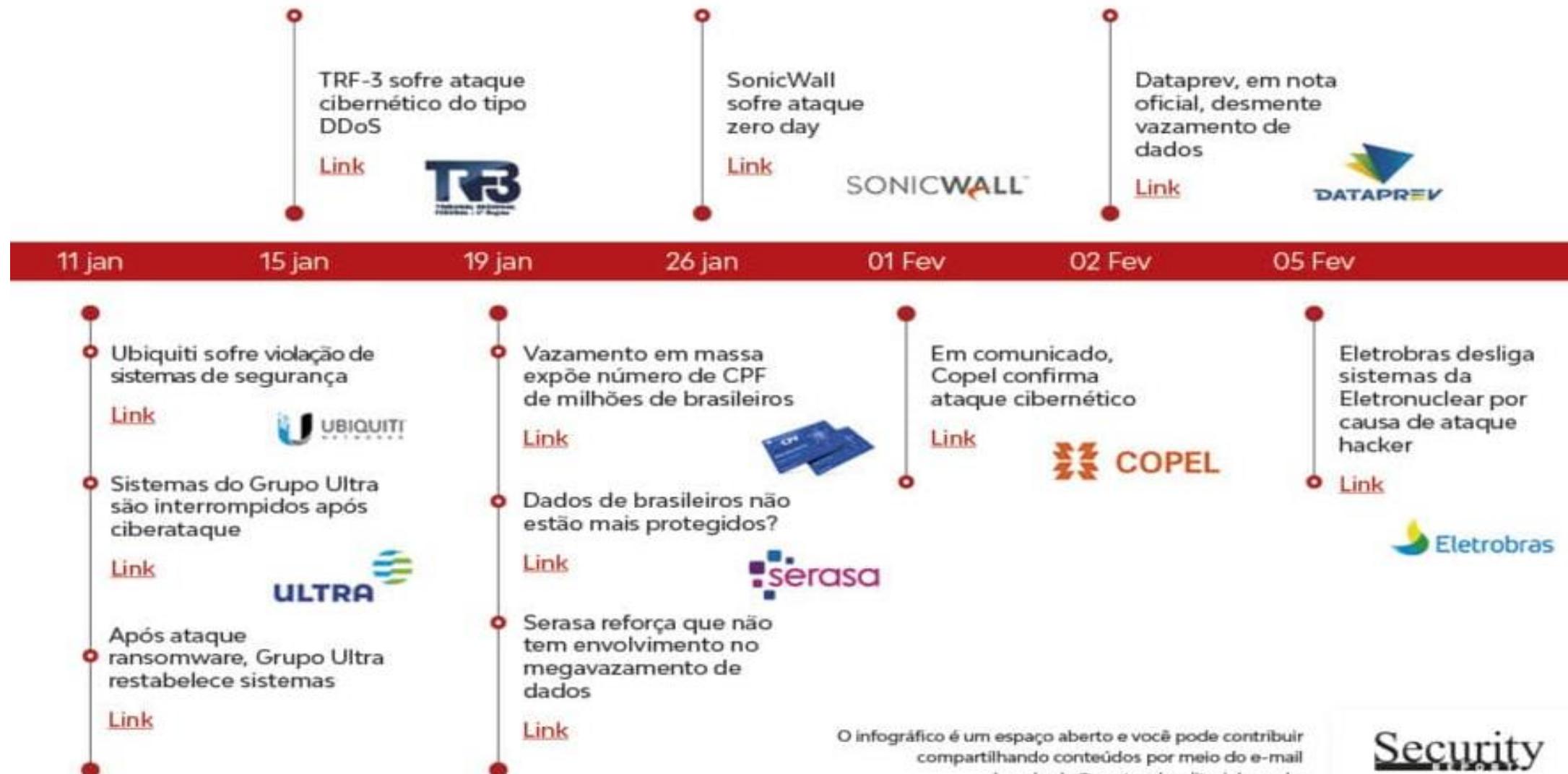
THE
DEVELOPER'S
CONFERENCE



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



Security

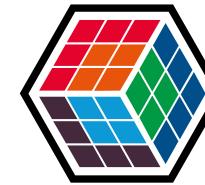
Resposta a incidentes



“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



THE
DEVELOPER'S
CONFERENCE



Etapas de resposta a incidentes



THE
DEVELOPER'S
CONFERENCE

NIST

- 1.Preparação
- 2.Detecção e Análise
- 3.Contenção, erradicação e recuperação
- 4.Atividade Pós-Incidente

SANS

- 1.Preparação
- 2.Identificação
- 3.Contenção
- 4.Erradicação
- 5.Recuperação
- 6.Lições aprendidas



THE
DEVELOPER'S
CONFERENCE

The screenshot shows a web browser window with the URL <https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response>. The page features a top navigation bar with links for AT&T Business, AT&T Cybersecurity, Products, Solutions, Partners, Resources (which is highlighted in blue), and AT&T Alien Labs. There is also a 'Get price' button. A banner in the center reads 'TO INCIDENT RESPONSE' with a green alien head icon below it. To the right of the banner is a 'share it:' section with icons for LinkedIn, Facebook, Twitter, and Reddit. The background of the main content area has a dark, wavy, map-like pattern with numbers like 1200, 1300, and 1400.

Introduction: Insider's Guide to Incident Response

This incident response (IR) guide contains insider secrets. Pass it on

The fight to protect your company's data isn't for the faint of heart. As an embattled IT warrior, with more systems, apps, and users to support than ever before, keeping everything up and running is a battle in itself. When it comes to preventing the worst-case scenario from happening, you need all the help you can get, despite your super-hero status.

That's why we've developed this guide. We've collected and curated decades of infosec war stories and *baccer intelligence*—from across the galaxy—so that you're better armed in the fight against

Achieve Faster, More Accurate Response Work

This insider's guide is an in-depth look at fundamental strategies of efficient and effective incident response for security teams that need to do more with less in today's rapidly changing threat landscape. [Download your copy now.](#)



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



THE
DEVELOPER'S
CONFERENCE

MISP
Threat Sharing



MALTEGO

Maltego CE



Maltego Community Edition 4.2.15

Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

Number of Results: 12 50 256 10k Privacy Mode Normal Quick Find Find in Files Entity Selection

Home Start Page Transform Hub

Maltego Transform Hub

Maltego Community Edition - Not licensed

[REFRESH] [UPDATE]

56 Hub items total | 0 Hub items installed (0 Transforms)

FILTER [RESET] : [ALL] [NOT INSTALLED] [INSTALLED] Sort by: [DEFAULT] [NEWEST] [NAME]

TRANSFORM HUB PARTNERS 56/56 shown

New

Featured

Featured Data Bundle

- Standard Transforms CE** by Maltego Technologies
Free Standard OSINT Transforms
- CaseFile Entities** by Paterva
Useful entities for modeling investigations.
- AliasDB** by ShadowDragon
Database of Defacements and the Aliases that took attribution
- ATT&CK - MISP** by MISP Project
Query data from MISP. Pivot on MITRE ATT&CK Intrusion Sets, Techniques, Tools and more.
- Blockchain.info (Bitcoin)** by Paterva
For visualizing the Bitcoin blockchain.
- CipherTrace (Large Bundle)** by Maltego Technologies
Cryptocurrency forensics and anti money laundering (AML) intelligence. This is the ...
- CipherTrace** by Maltego Technologies
- Cisco Threat Grid** by Cisco Threat Grid
- Clearbit** by Christian Heinrich

Be the first to try out our on-demand courses!
GET EARLY ACCESS

Tailored Training
On-demand Courses

MISP- (Malware Information Sharing Platform)

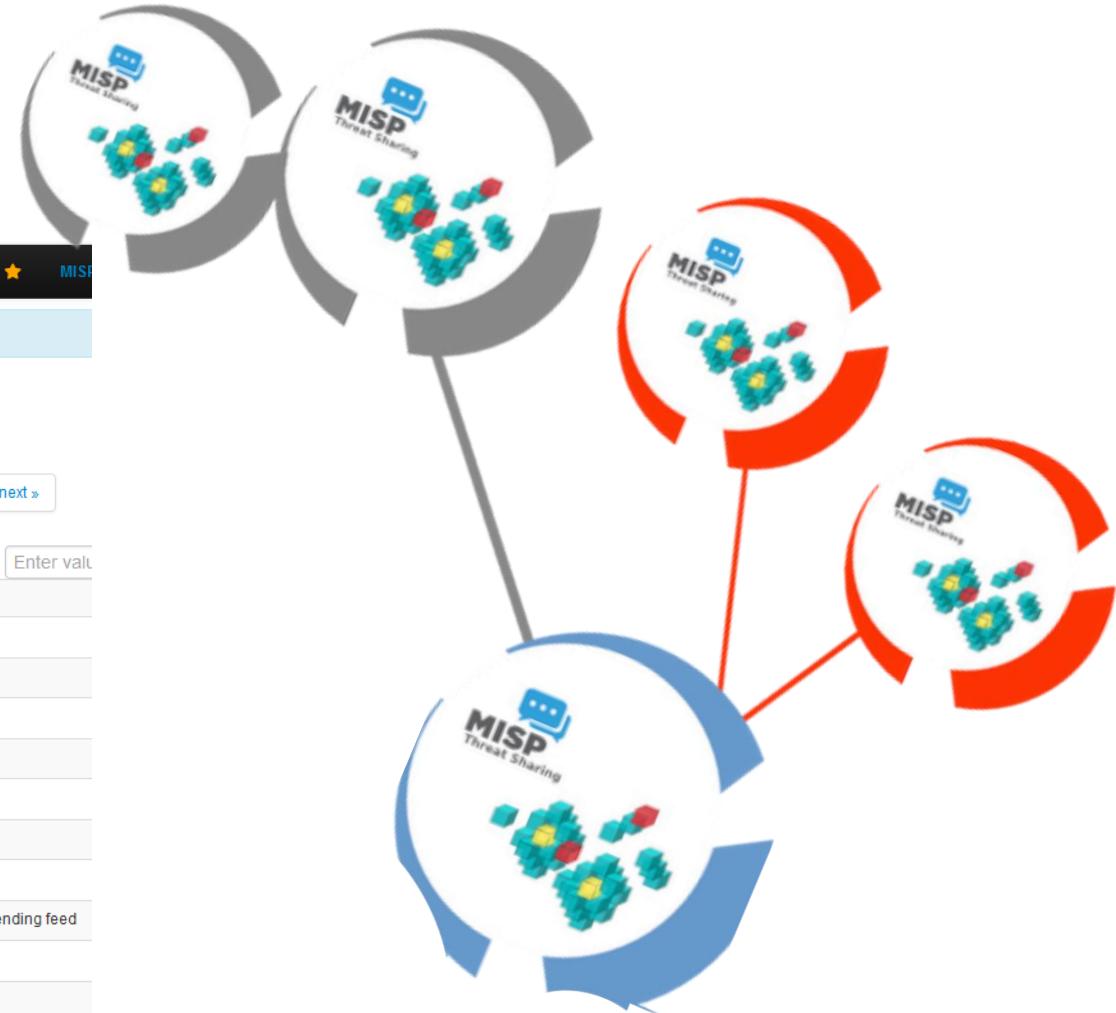
Home Event Actions Galaxies Input Filters Global Actions Sync Actions ★ MIS

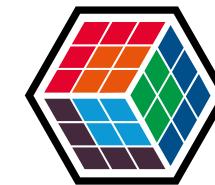
Welcome! Last login was on Sun, 18 Apr 21 16:10:20 -0300

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »

<input type="checkbox"/>		Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Info
<input type="checkbox"/>		2021-05-26		65929		Sandbox, Malware	17		2021-05-26	Cuckoo Sandbox analysis #33396
<input type="checkbox"/>		2021-05-26		65928		Sandbox, Malware	17		2021-05-26	Cuckoo Sandbox analysis #33393
<input type="checkbox"/>		2021-05-26		65927		Sandbox, Malware	14		2021-05-26	Cuckoo Sandbox analysis #33394
<input checked="" type="checkbox"/>		2021-05-26		65926			9		2021-05-26	OpenCTI.BR MHN URL Droppers feed
<input type="checkbox"/>		2021-05-26		65925		Sandbox, Malware	43		2021-05-26	Cuckoo Sandbox analysis #33390
<input type="checkbox"/>		2021-05-26		65924		Sandbox, Malware	14		2021-05-26	Cuckoo Sandbox analysis #33392
<input type="checkbox"/>		2021-05-26		65922		Sandbox, Malware	38		2021-05-26	Cuckoo Sandbox analysis #33389
<input checked="" type="checkbox"/>		2021-05-26		65923			49		2021-05-26	OpenCTI.BR MHN Dionaea Malware Sending feed
<input type="checkbox"/>		2021-05-26		65921		Sandbox, Malware	14		2021-05-26	Cuckoo Sandbox analysis #33391
<input checked="" type="checkbox"/>		2021-05-26		65920			207		2021-05-26	OpenCTI.BR CensysScanners feed

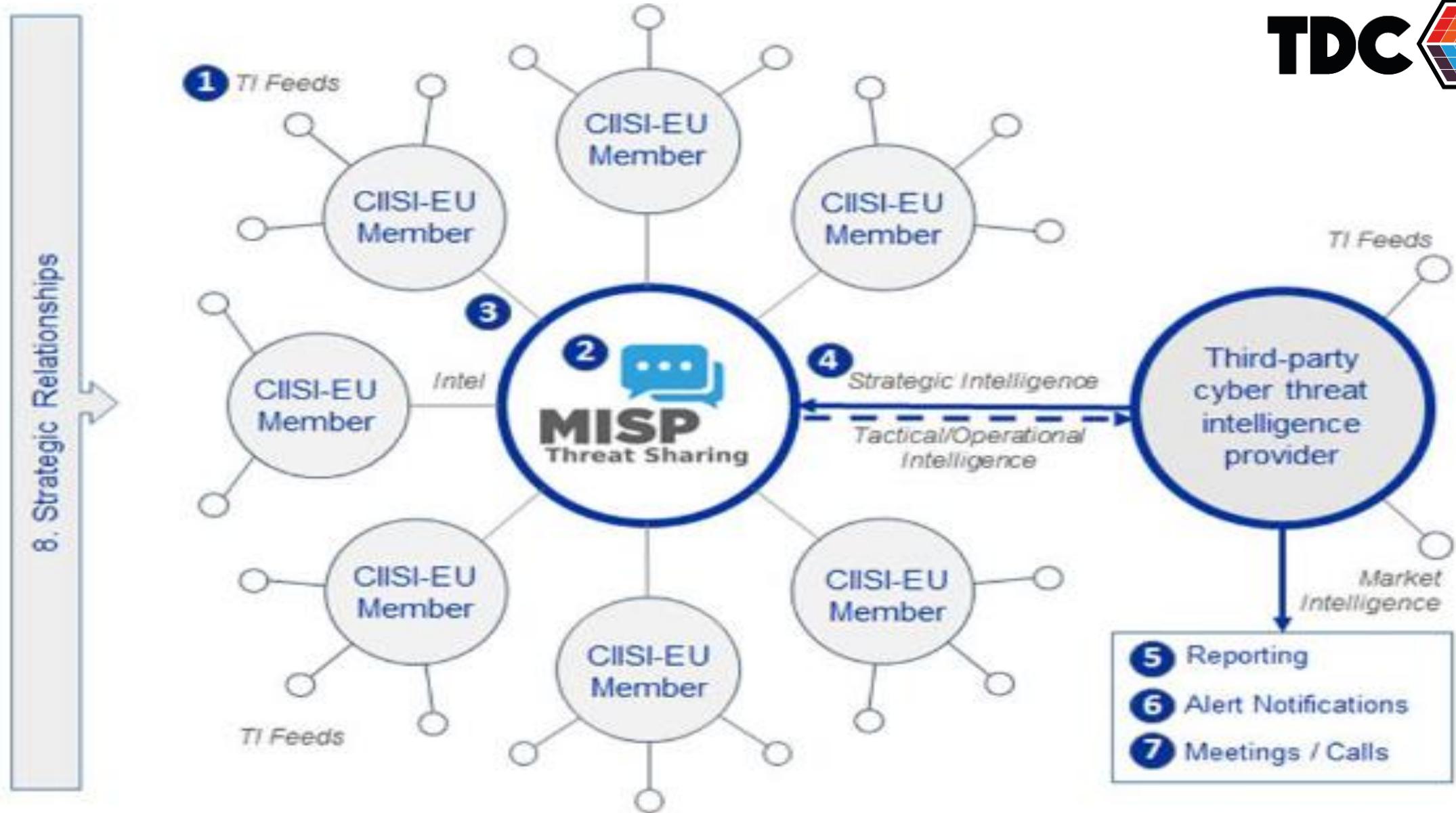




THE
DEVELOPER'S
CONFERENCE

Demo





OpenCTIBr



THE
DEVELOPER'S
CONFERENCE



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

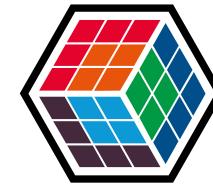
Disponibilizamos diariamente em nosso repositório no Github, informações de ameaças cibernéticas no formato Threat Feeds.

Sandbox Analysis

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

<https://www.opencti.net.br>

Mitre-Att&ck

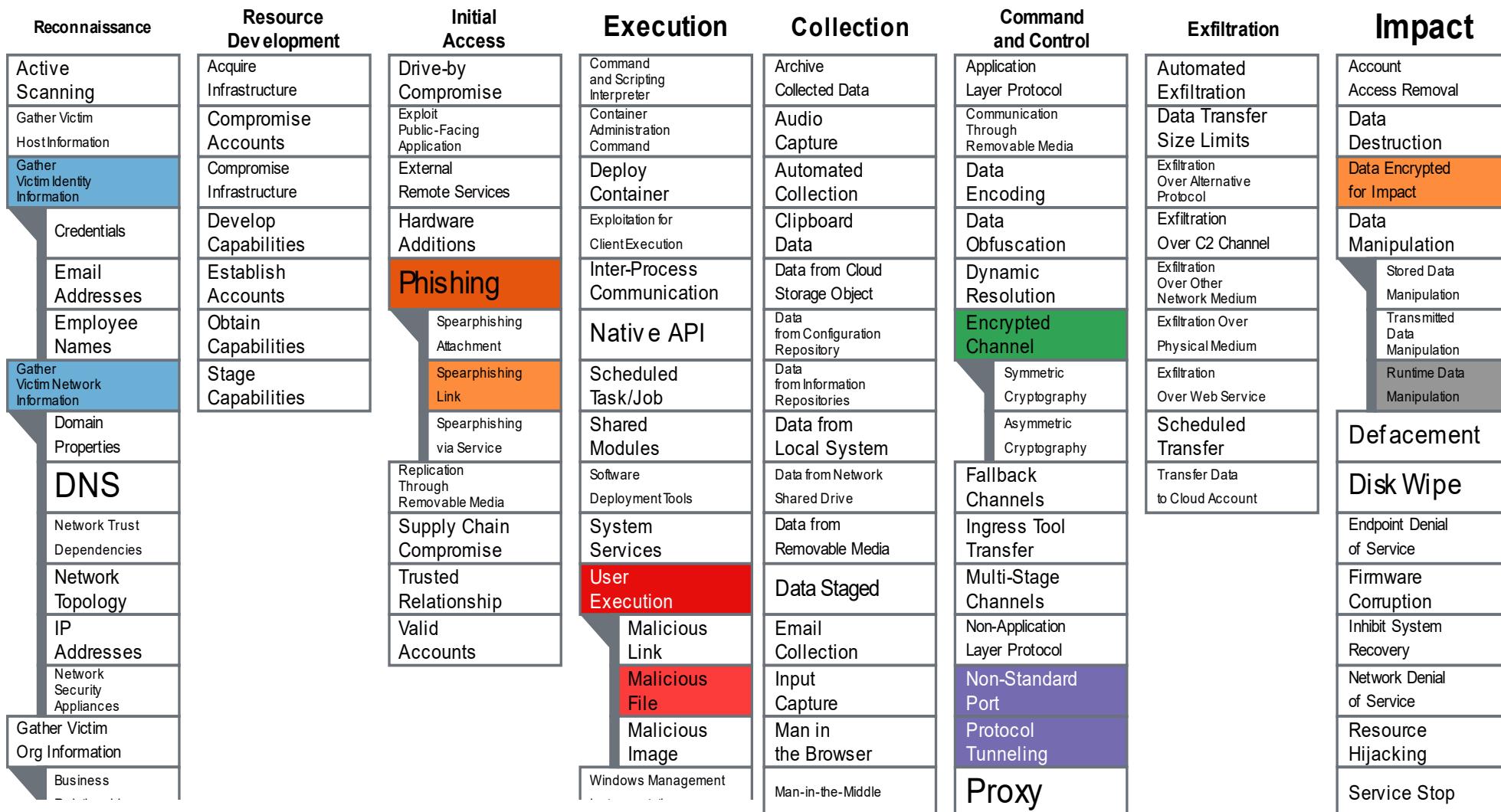


THE
DEVELOPER'S
CONFERENCE

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Dashboard	Cloud Service Discovery	Remote Services (0/6)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Process	Direct Volume Access	Input Capture (0/4)	Container and Resource Discovery	Container and Resource Discovery	Replication Through Removable Media
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Scheduled Task/Job (0/7)	Scheduled Task/Job (0/7)	Create or Modify System Process (0/4)	Domain Policy Modification (0/2)	Man-in-the-Middle (0/2)	Domain Trust Discovery	Domain Trust Discovery	Software Deployment Tools
Search Open Technical Databases (0/5)	Supply Chain Compromise (0/3)	Shared Modules	Shared Modules	Create Account (0/3)	Escape to Host	Execution Guardrails (0/1)	File and Directory Discovery	File and Directory Discovery	Taint Shared Content
Search Open Websites/Domains (0/2)	Trusted Relationship	Software Deployment Tools	Software Deployment Tools	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Network Service Scanning	Use Alternate Authentication
Search Victim-Owned Websites	Valid Accounts (0/4)	System Services (0/2)	System Services (0/2)	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Network Sniffing	Network Share Discovery	
		User Execution (0/3)	User Execution (0/3)	External Remote Services	Hijack Execution	Hide Artifacts	OS Credential Dumping		



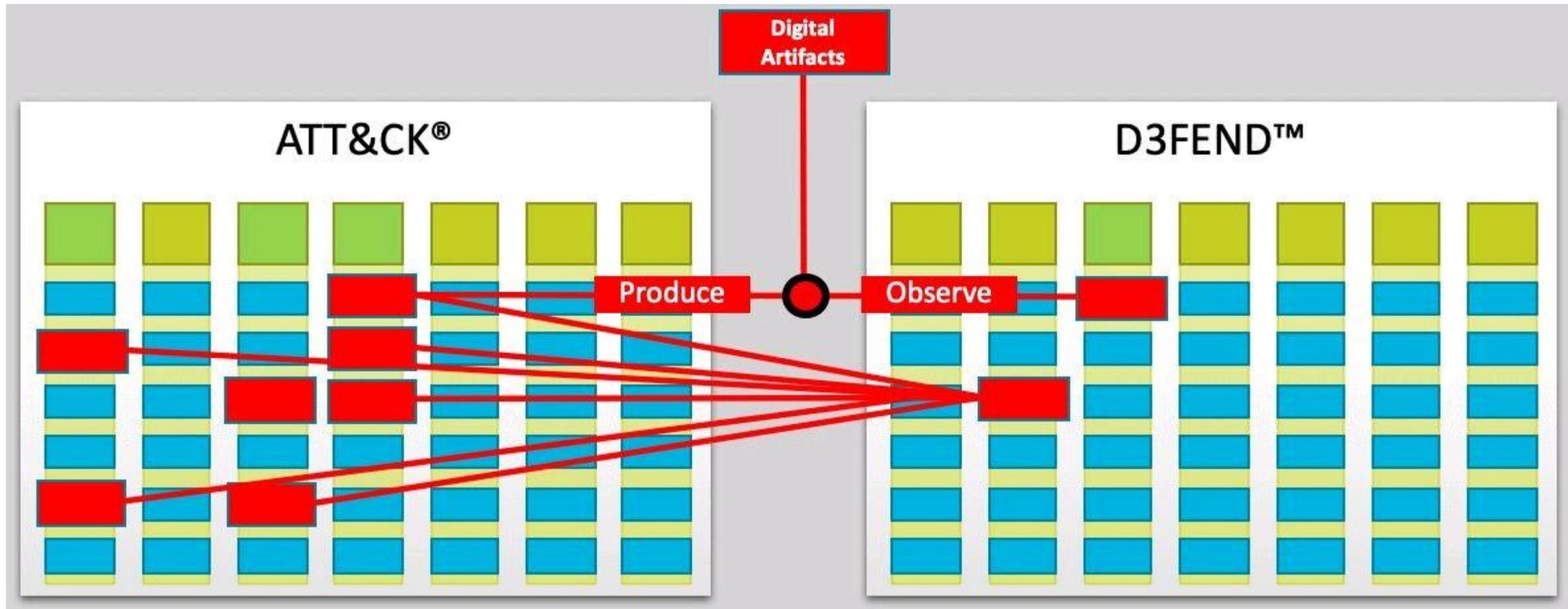
THE DEVELOPER'S CONFERENCE



<https://d3fend.mitre.org/>



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

LOGO

Política de Segurança da Informação

Formulário de Incidente Segurança da Informação



THE
DEVELOPER'S
CONFERENCE

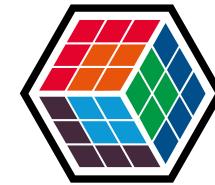
Nome da Empresa

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

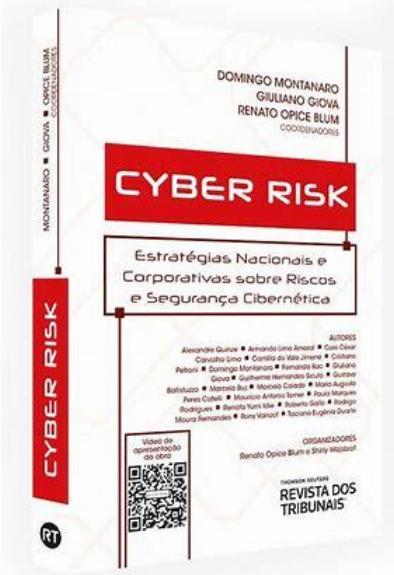
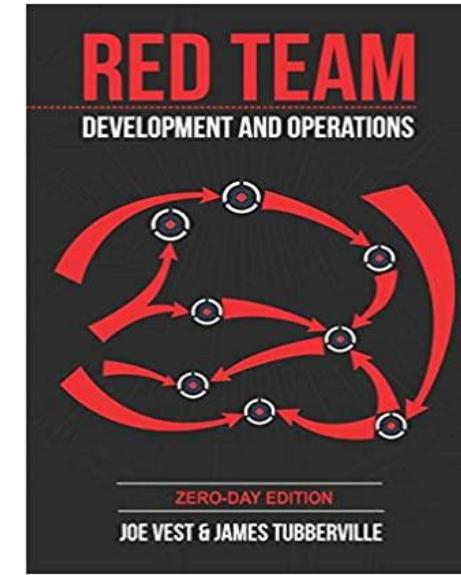
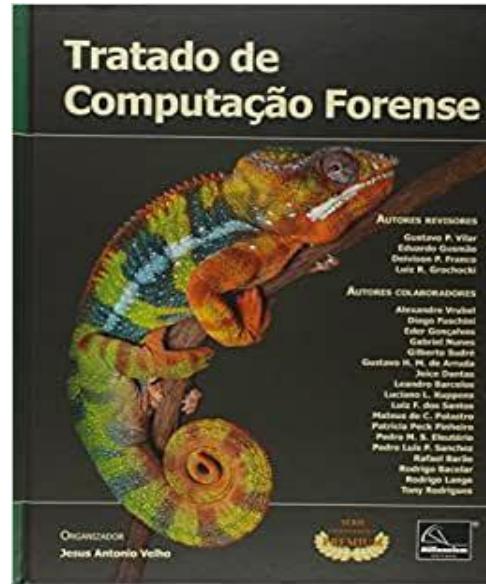
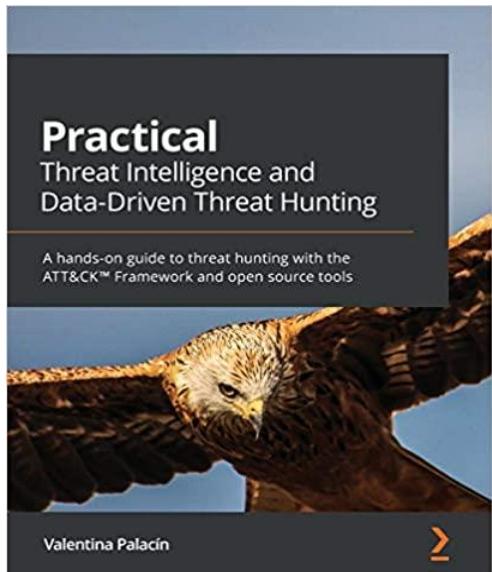
Data do Incidente:	Hora do Incidente:
Quem foi notificado:	Hora da notificação:
<i>Descrição do Incidente:</i>	

- <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

