

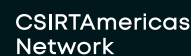
# IV JORNADAS STIC & CONGRESO ROOTED CON

CAPÍTULO PANAMÁ

## Cosas que nunca te dije

**MITRE**  
ATT&CK™

ORGANIZADORES

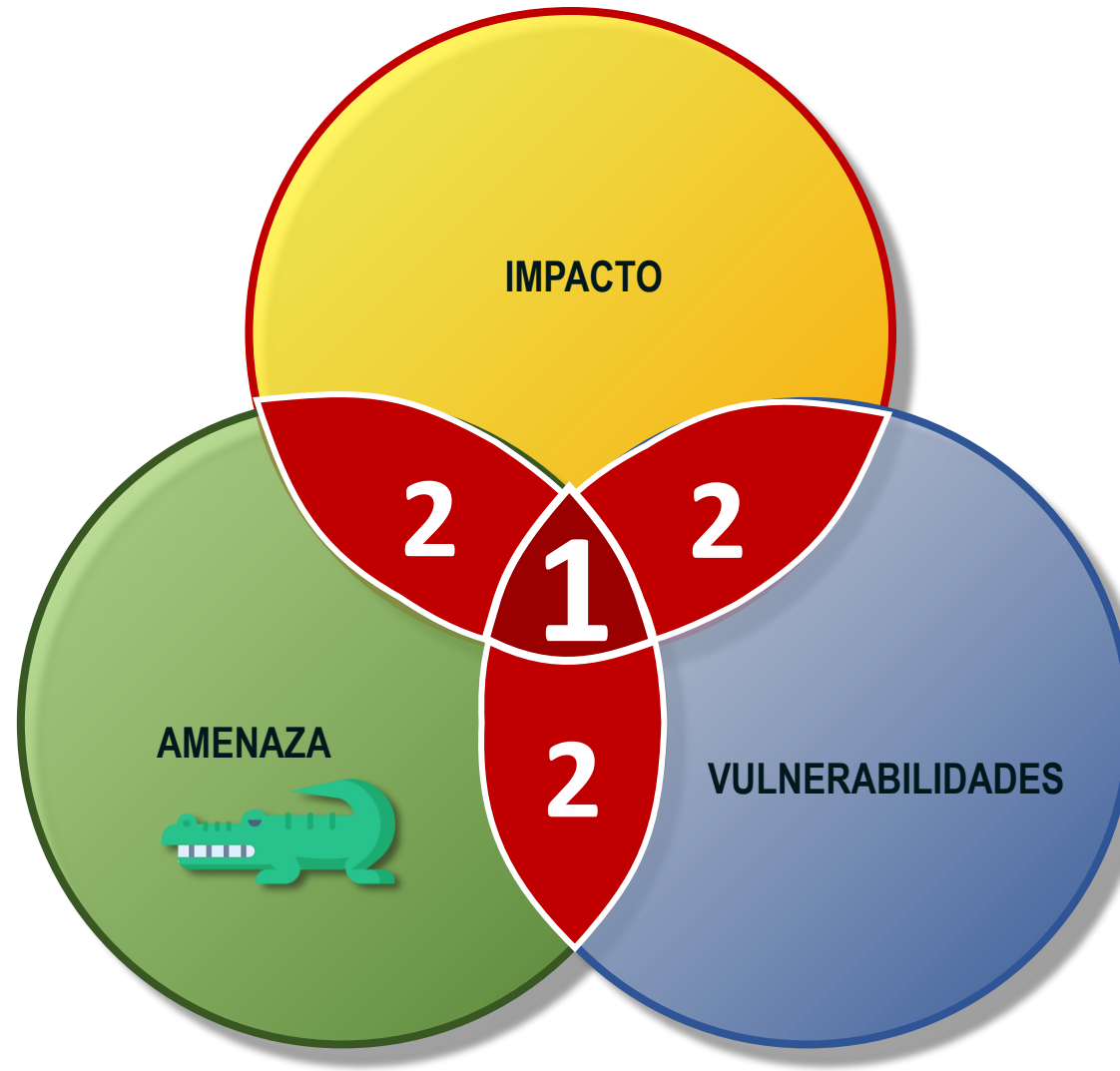


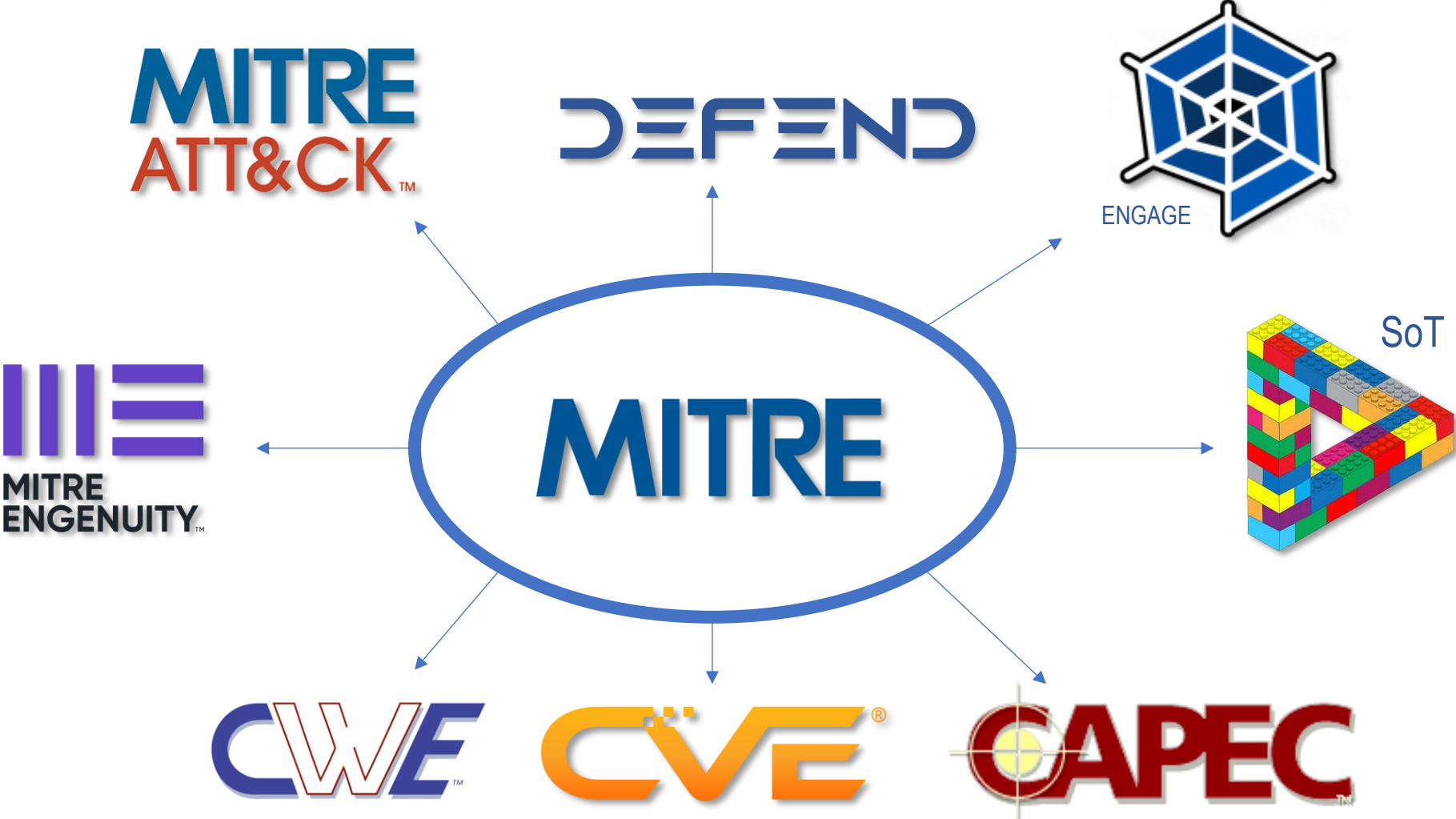
APOYO INSTITUCIONAL

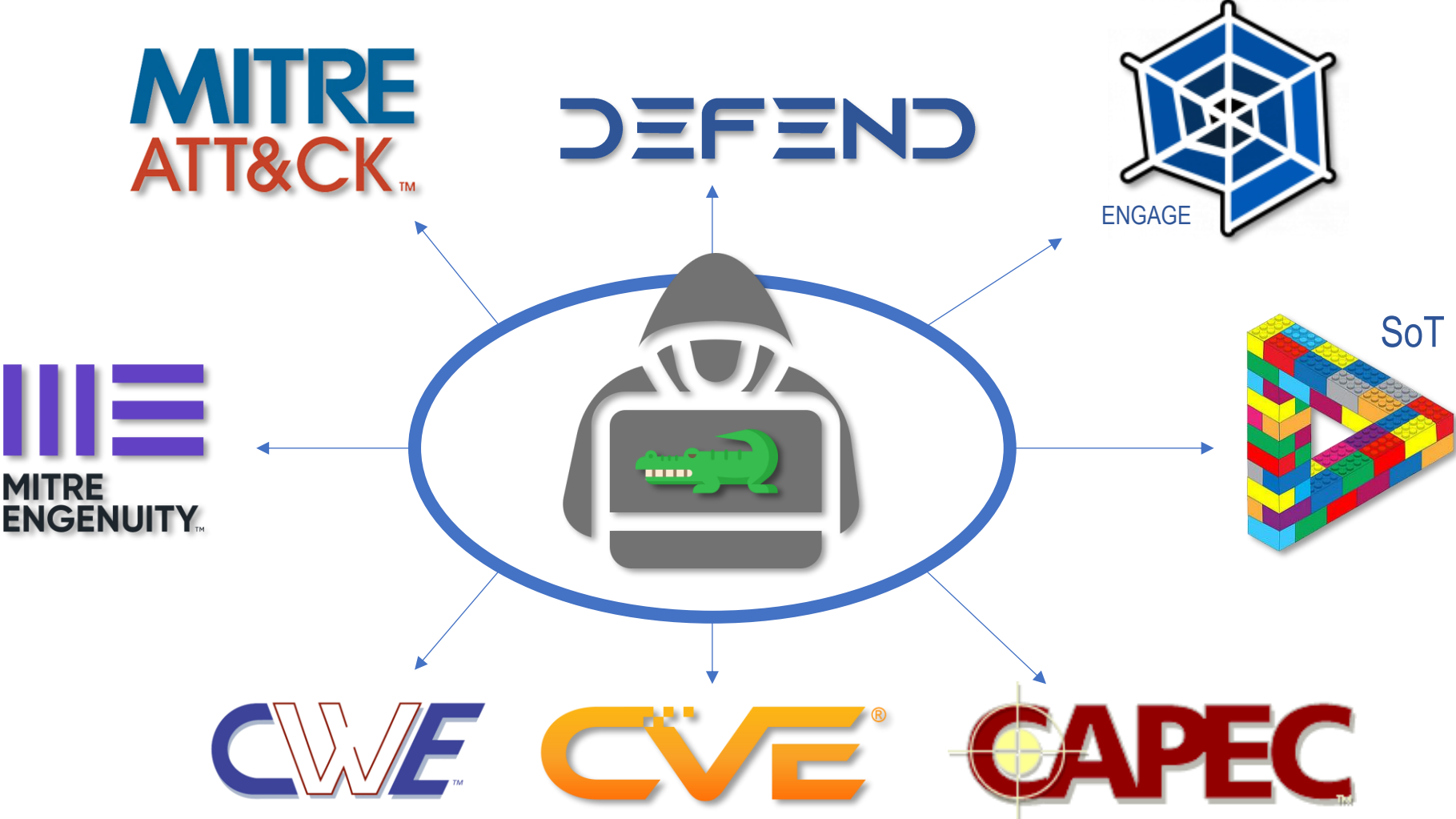
COLABORADORES



# RIESGO = VULNERABILIDADES \* AMENAZA \* IMPACTO









# MITRE WORLD



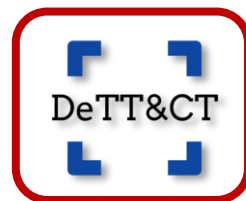
**MITRE**  
**ATT&CK**™



CREF Navigator →||←



MICRO  
Emulation Plans



#STIC**PANAMÁ**





# ALL YOU NEED IS ♥ LOGS



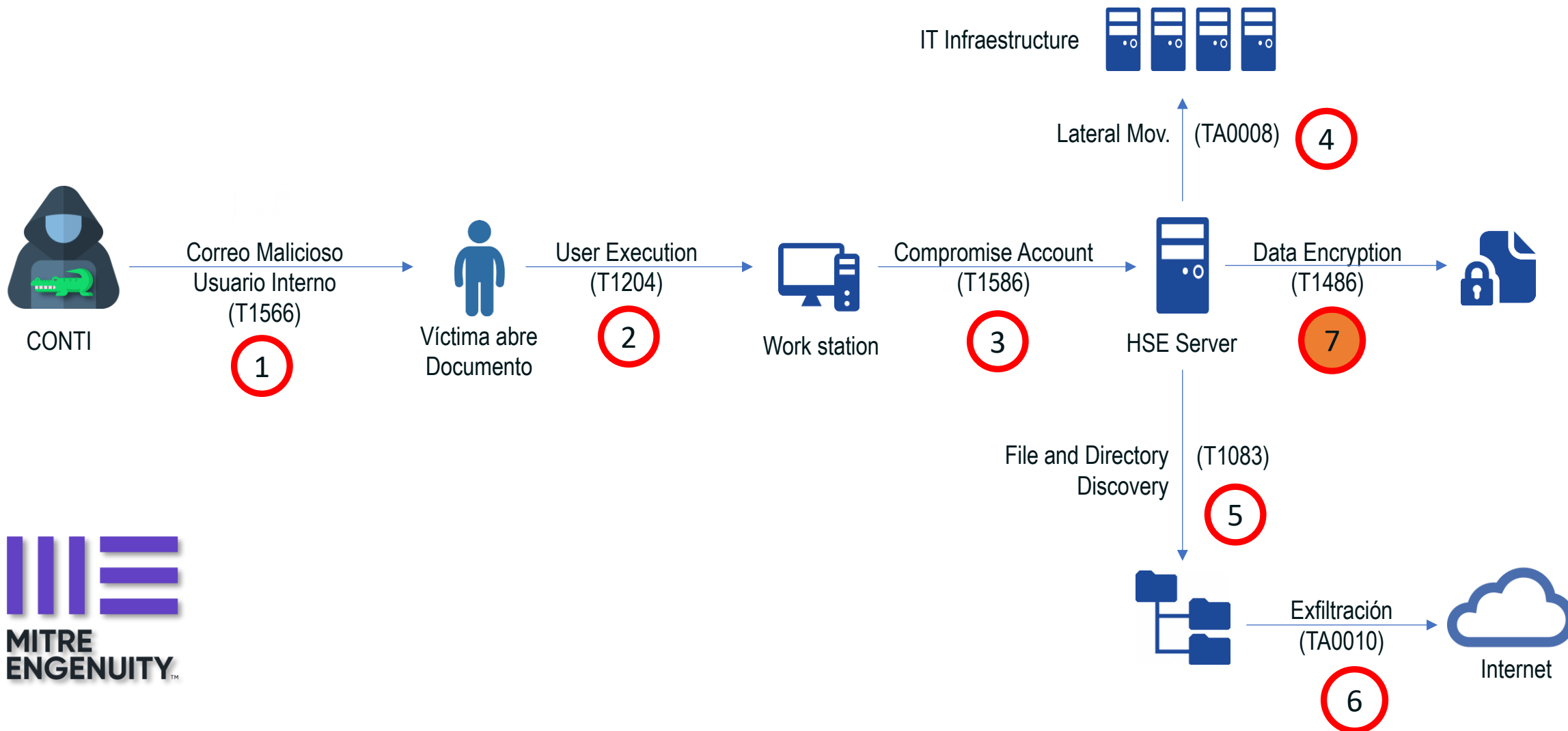
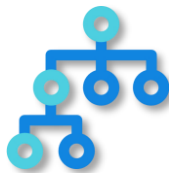
- 
- Visibilidad
  - Detección







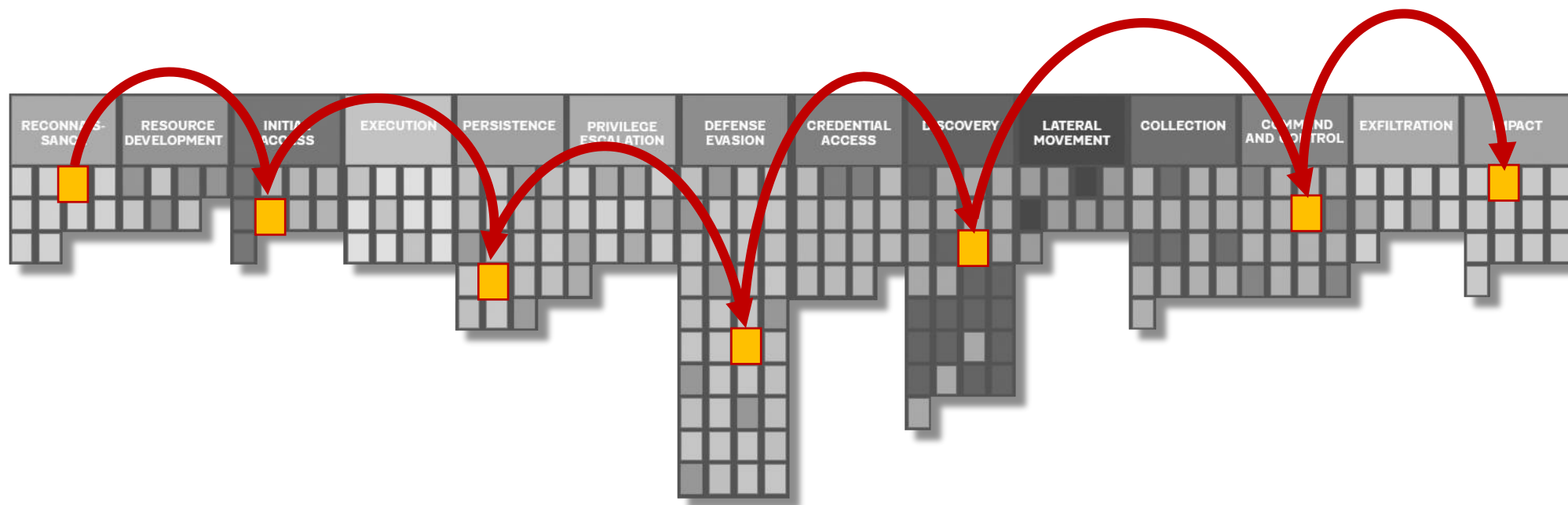
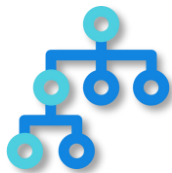
# Attack Flow

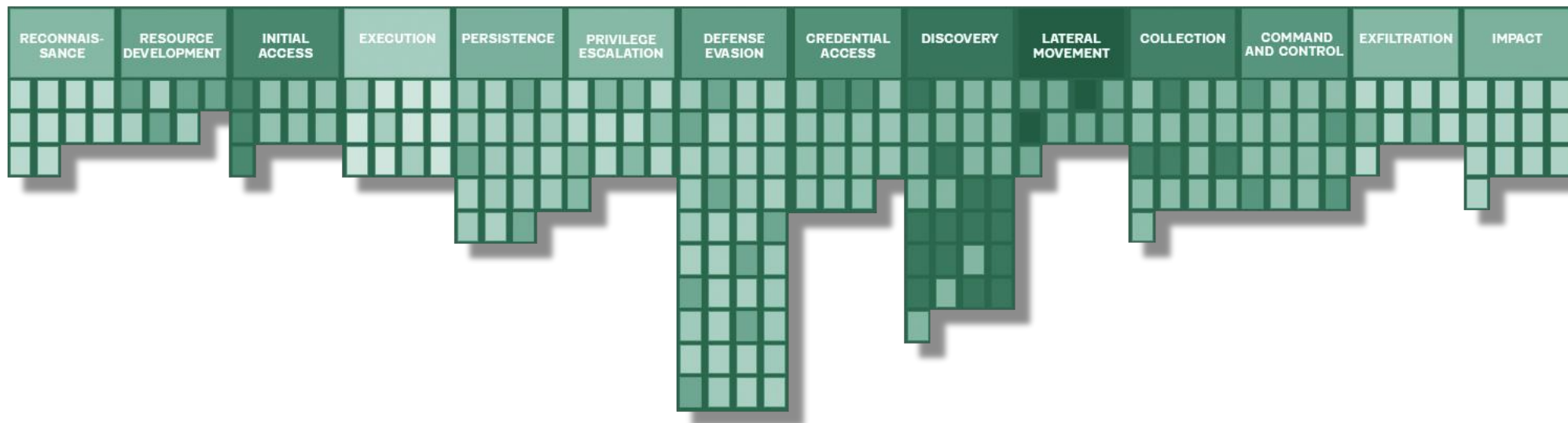


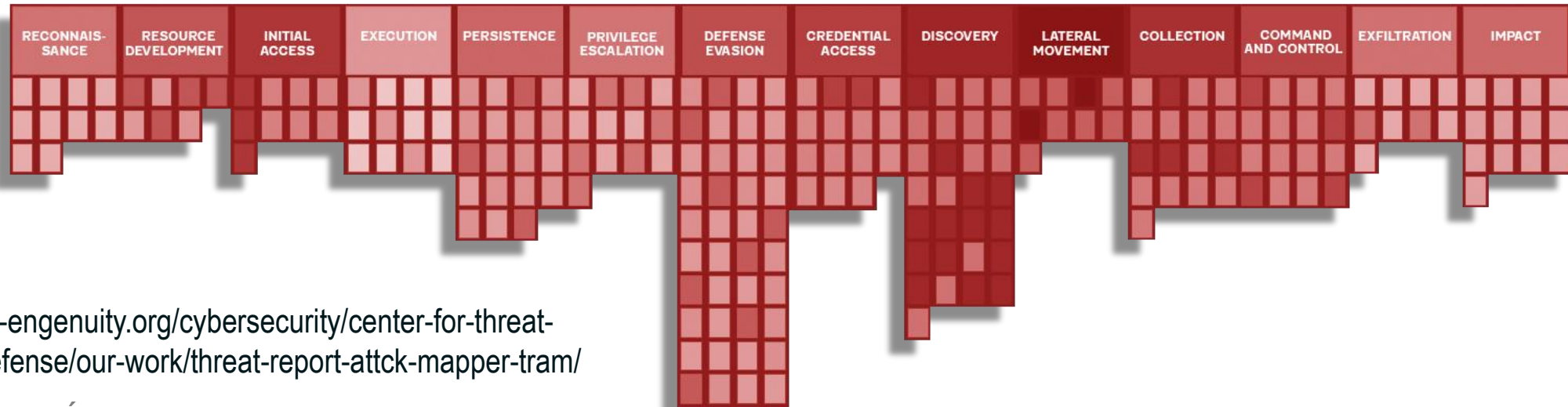
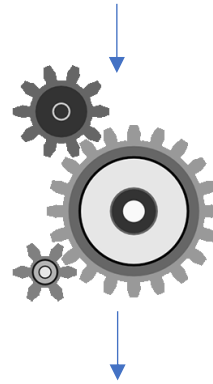




# Attack Flow







<https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/threat-report-attck-mapper-tram/>

#STICPANAMÁ



---

# Demo time!!



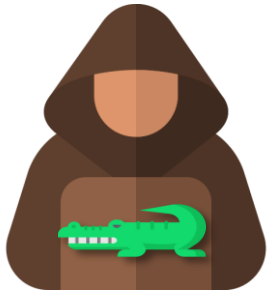




# Resumiendo



## CONTROLES VS CAPACIDADES





# MITRE goodies

Browser address bar: <https://start.me/p/oniQRD/mitreando>

Mis páginas - MITREando TTX BAS CTI

Buscar en la web

### MITRE.org

Vivimos un mundo en conflicto. MITRE aplica el pensamiento sistémico para resolver los desafíos de las amenazas de ciberseguridad.

- The MITRE Corporation
- MITRE ATT&CK™
- MITRE D3FEND - Matrix
- MITRE Engage
- MITRE Engenuity

### ATT&CT 3rd-part Open Source Tools - Prevention

- UNIT 42 PLAYBOOK VIEWER
- Comodo MITRE Kill Chain – Comodo Tech Talk
- Splunk - attack range
- Purple Sharp
- Juniper Networks - Visualizing MITRE Tactic and Techniques
- MITRE ATT&CK Heatmap for Splunk

### Adversary Emulation Tools

Echa un vistazo a mi página de BAS: <https://start.me/p/diOp11/bas>

- Atomic-Red-Team
- DumpsterFire toolset
- FireDrill
- MORDOR Datasets
- Infection Monkey
- RTA - Red Team Automation
- Stratus Red Team
- MeTTA
- Blue Team Training Toolkit (BT3)
- Detection-Lab

### Informes, Estudios, papers, ...

### + Artículos

### YouTube Videos

### MITRE official Tools

Herramientas desarrolladas por MITRE

- ATLAS \*
- ATT&CK® Navigator \*
- BRAWL
- BZAR
- Calculator - Top ATT&CK Techniques
- CALDERA \*
- CAR - Cyber Analytics Repository
- CAREt - The CAR Exploration Tool
- CASCADE Server
- CREF Navigator \*

### MITRE Engenuity

- CTID - CENTER FOR THREAT-INFORMED DEFENSE
- ATT&CK Flow
- Micro Emulation Plans
- Cybersecurity R&D Funding and Threat Evaluations
- NIST 800-53 Control Mappings
- ATT&CK Workbench
- ATT&CK® EVALUATIONS
- THREAT REPORT ATT&CK MAPPER (TRAM)

### Tools to interact with ATT&CK

Nada de corta-pegar, saca todo el jugo a ATT&CK

- [DeTT&CT] (rabobank)
- MITRE - Assistant
- CISA - Decoder
- Teaching blue, red or yellow
- Welcome to pyattck's Documentation — pyattck 2.0.0 documentation

### Graphic Tools

### MITRE - 'alfajitas'

### ATT&CK Open Source Tools - CTI

### ATT&CK Open Source Tools - Hunting

### Getting Started with ATT&CK

- Getting Started with ATT&CK: Threat Intelligence
- ATT&CK vs. Cyber Kill Chain vs. Diamond Model
- MITRE ATT&CK Framework for Beginners

### ATT&CK en Español

- Comenzar a usar ATT&CK y la APT38 [I] - Inteligencia sobre Amenazas ~ Segu-Info - Ciberseguridad d...
- Matrices y herramientas de MITRE ATT&CK ~ Segu-Info
- MITRE lanza "Adversary Emulation Library" con escenarios de emulación gratuitos ~ Segu-Info - Ciber...
- Un acercamiento práctico a integrar ATT&CK y D3FEND de MITRE - Think Big Empresas
- D3FEND, la otra cara de la moneda ATT&CK - Think Big Empresas
- Cómo utilizar MITRE ATT&CK: un repositorio de técnicas y procedimientos de ataques y defensas | WeL...
- Pyattck: paquete para interactuar con el framework MITRE ATT&CK - Blog EHCGroup
- MITRE lanza 'Adversary Emulation Library' para proporcionar planes de emulación gratuitos.

### Mapping detection: ATT&CK + DeTT&CT

- DeTT&CT - wiki
- Modelado práctico de amenazas y defensas Blue Team con MITRE ATT&CK - YouTube
- DeTT&CT: Mapping detection to MITRE ATT&CK - NVISO Labs
- DeTT&CT: Mapping your Blue Team to MITRE ATT&CK™ — MB Secure
- ¿Estás sacando el máximo partido a MITRE ATT&CK?: Análisis de la visibilidad del SOC — Parte I | by Ru...
- ¿Estás sacando el máximo partido a MITRE ATT&CK?: Análisis de la visibilidad del SOC — Parte II | by Ru...
- Ismael Valenzuela - Modelado Practico de Amenazas y Defensas
- 1.- Detecciones y análisis de riesgos con ATT&CK
- 2.- Detecciones y Análisis de Riesgos con ATT&CK Parte 2
- 3.- Detecciones y análisis de riesgos con ATT&CK Parte 3
- 4.- Detecciones y Análisis de Riesgos: Edición Ransomware
- DeTT&CT: Mapping Your Blue Team To MITRE ATT&CK - Ruben Bouman and Marcus Bakker - YouTube
- MITRE DeTT&CT - Data Source Visibility and Mapping
- MITRE Practical Use Cases

### Pre-ATT&CK articles

- 15 Ways MITRE's PRE-ATT&CK Tactics Protect You - ITEGRITI
- What's MITRE PRE-ATT&CK and How to Use it in Threat Intelligence? | by SOCRadar® Cyber Threat Int...

### MITRE Navigator

### MITRE Shield [deprecated]

### MITRE CALDERA



Emilio Rico  
Security Advisor at **trc**



@Emilio\_RR



Emilio Rico Ruiz



<https://github.com/3MlioRR>

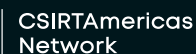


# IV JORNADAS STIC & CONGRESO ROOTED CON

CAPÍTULO PANAMÁ

# GRACIAS

ORGANIZADORES



APOYO INSTITUCIONAL

COLABORADORES