IV JORNADAS STIC & CONGRESO ROOTED CON

CAPÍTULO **PANAMÁ**

Cosas que nunca te dije

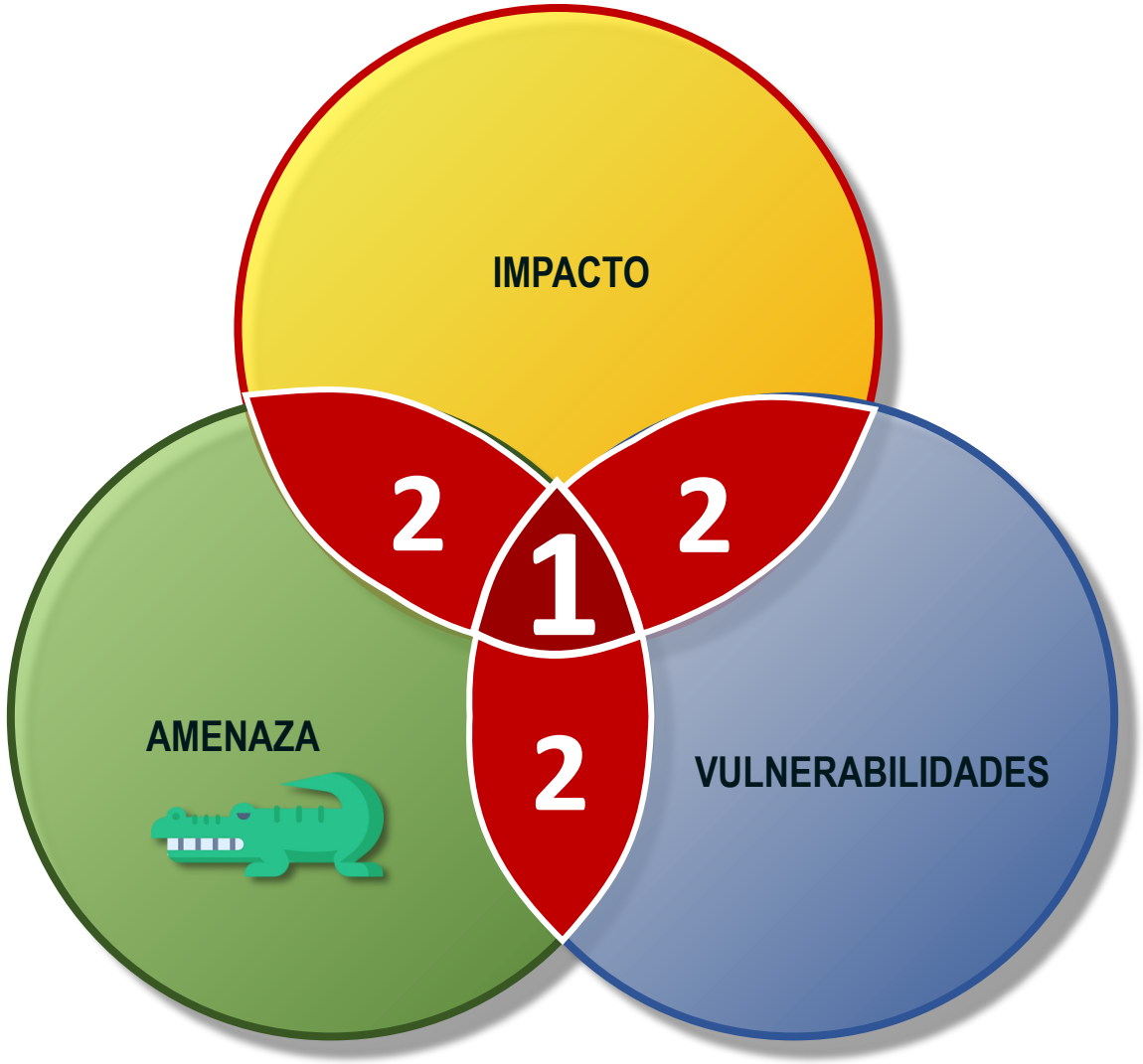
MITRE ATT&CK™

ORGANIZADORES

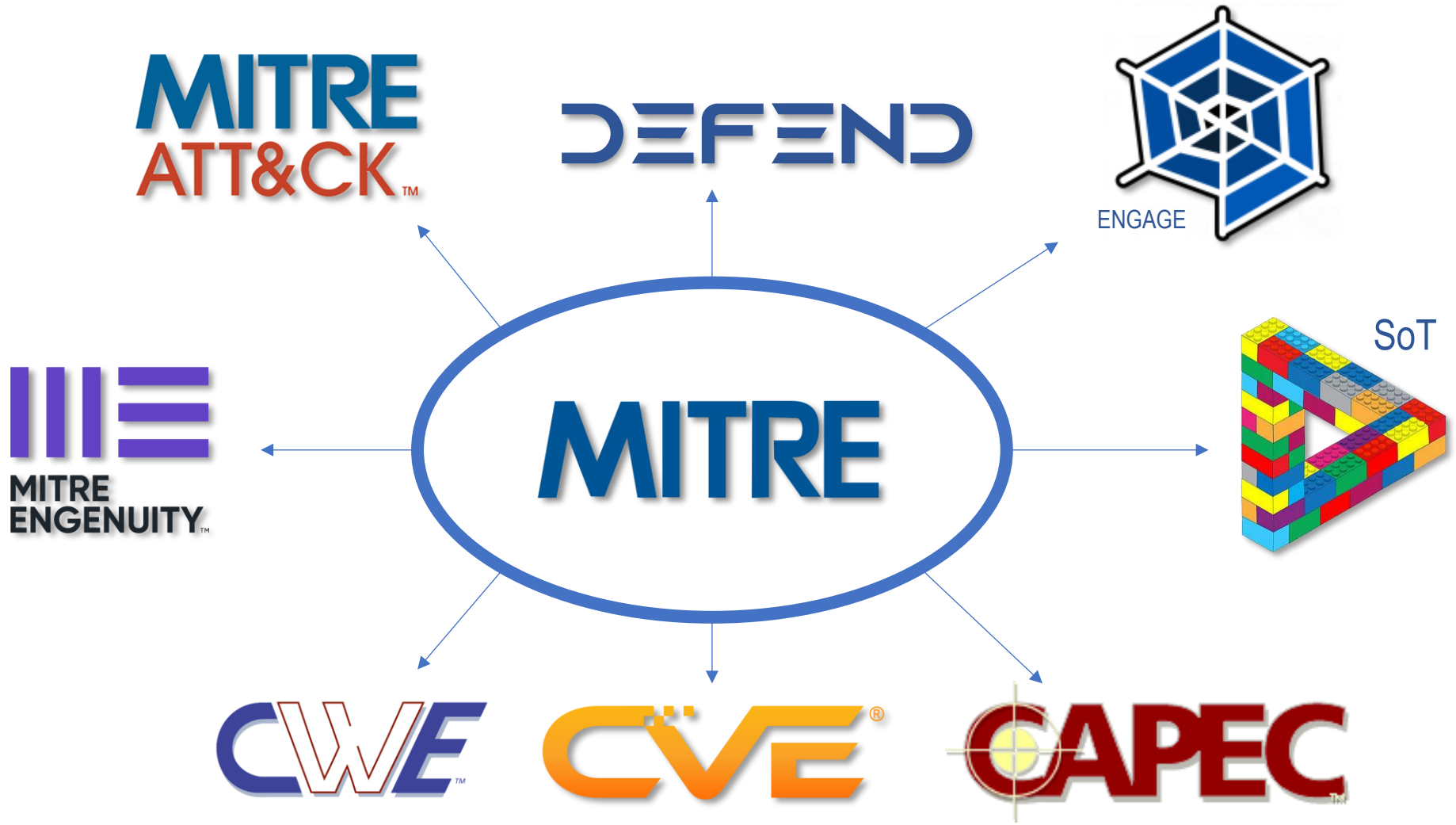
APOYO INSTITUCIONAL

COLABORADORES

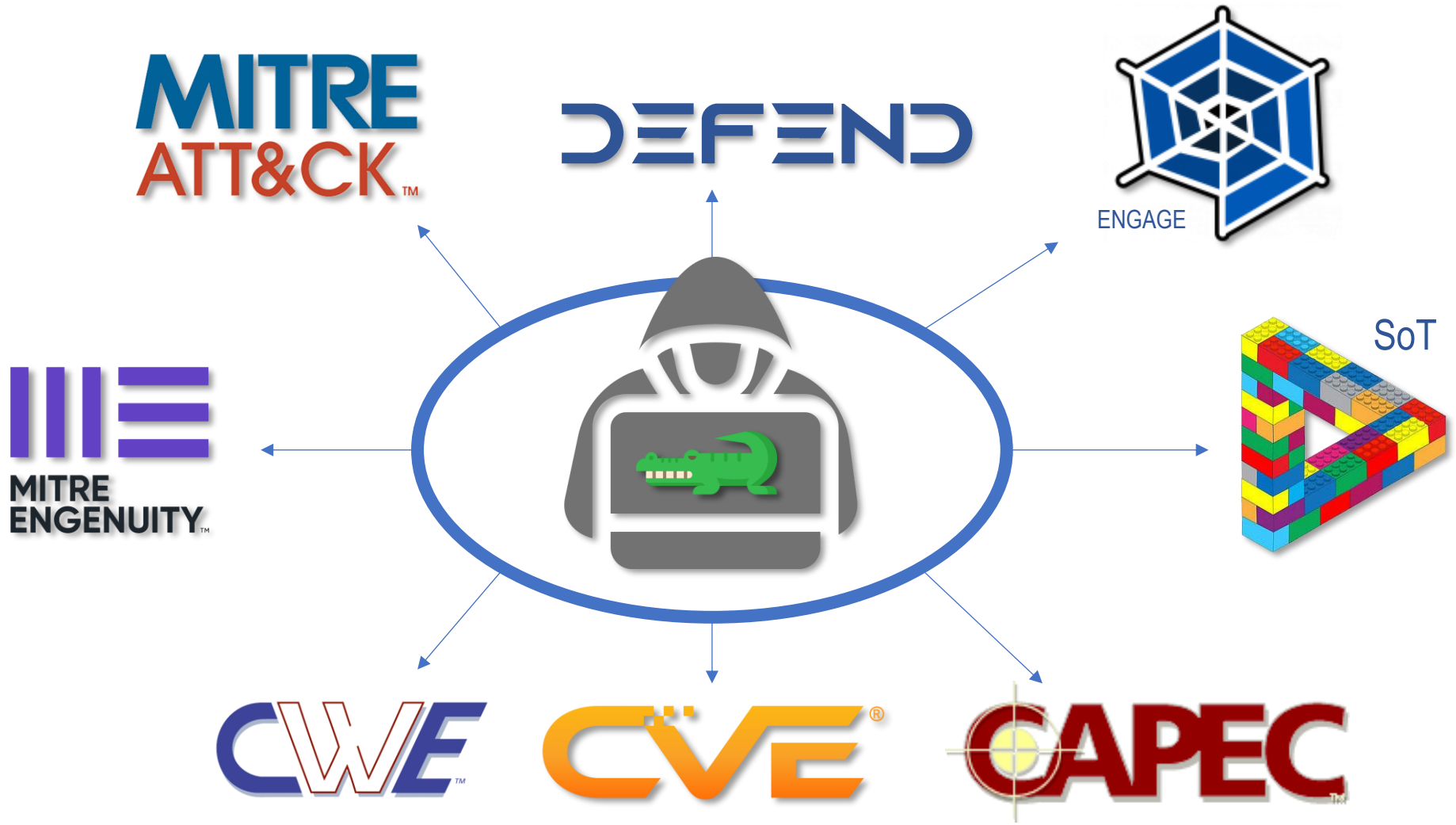
RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



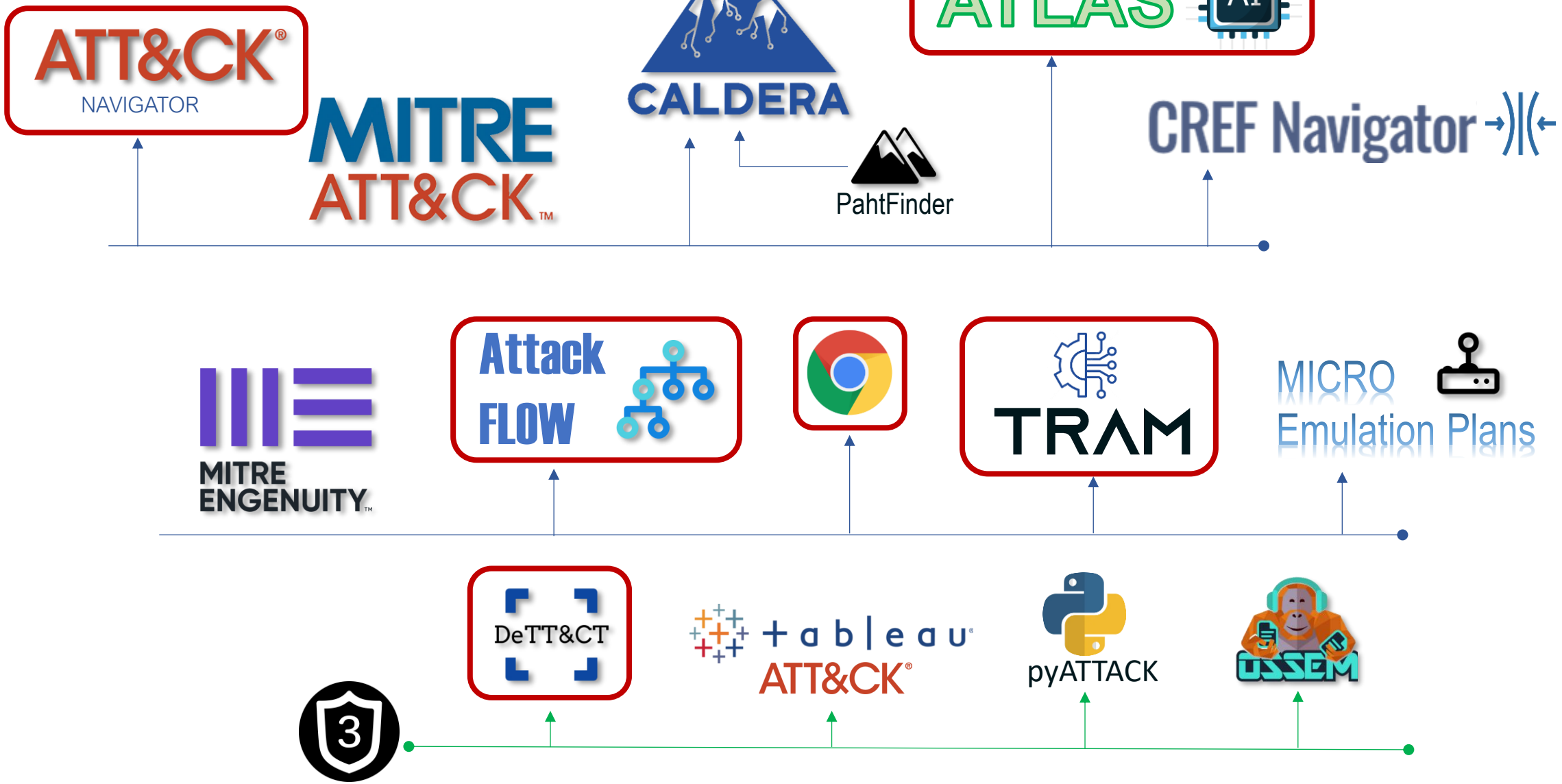
MITRE WORLD


MITRE ATT&CK™
DEFEND
ENGAGE
MITRE ENGENUITY™
MITRE
SoT
CWE™
CVE®
CAPEC™

MITRE WORLD

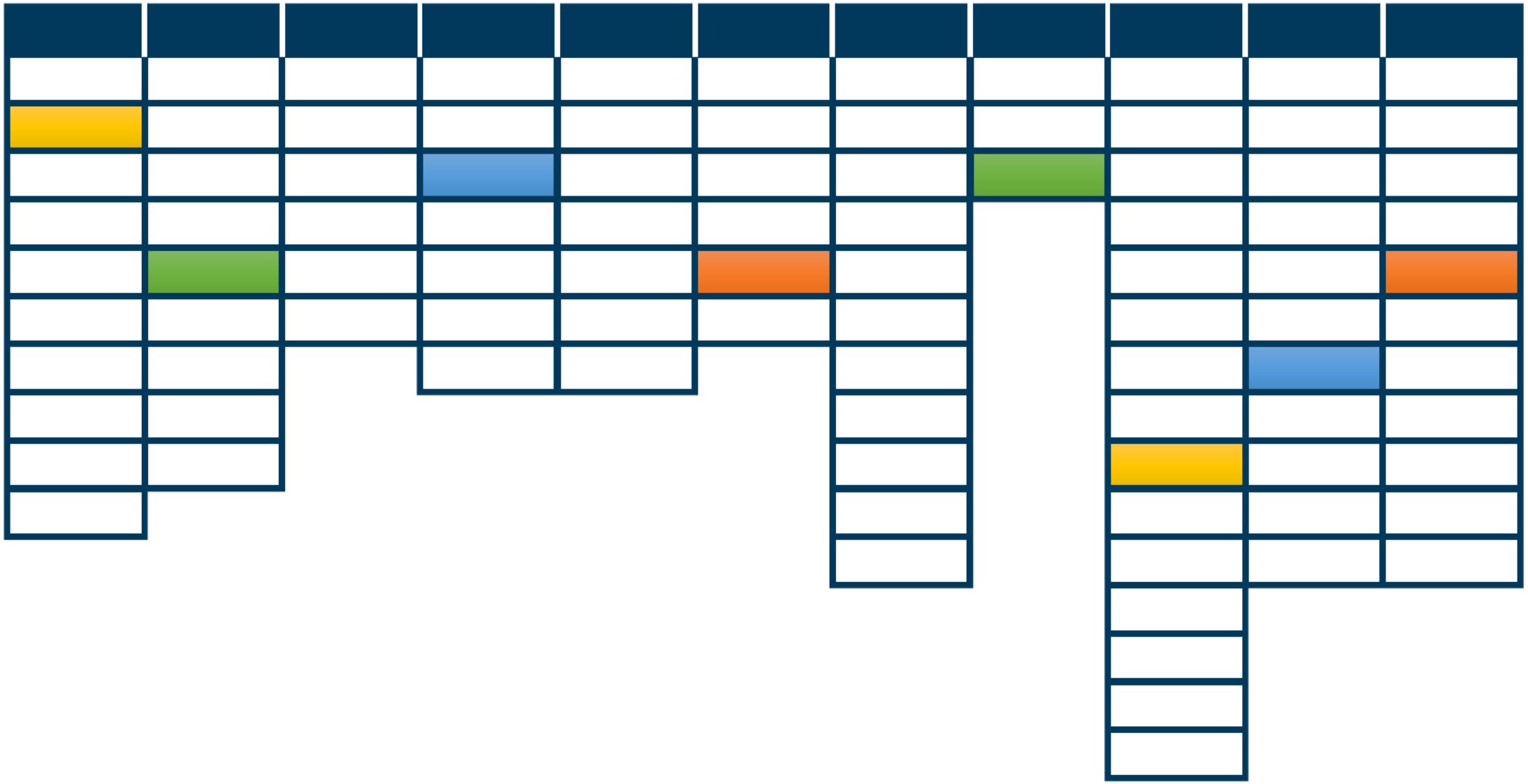

MITRE ATT&CK™
DEFEND
ENGAGE
MITRE ENGENUITY™
SoT
CWE™
CVE®
CAPEC™

MITRE WORLD


ATT&CK®
NAVIGATOR
MITRE
ATT&CK™
CALDERA
PahtFinder
ATLAS
AI
CREF Navigator
MITRE
ENGENUITY™
Attack
FLOW
TRAM
MICRO
Emulation Plans
DeTT&CT
+ableau
ATT&CK®
pyATTACK
OSSEM
3

navigator

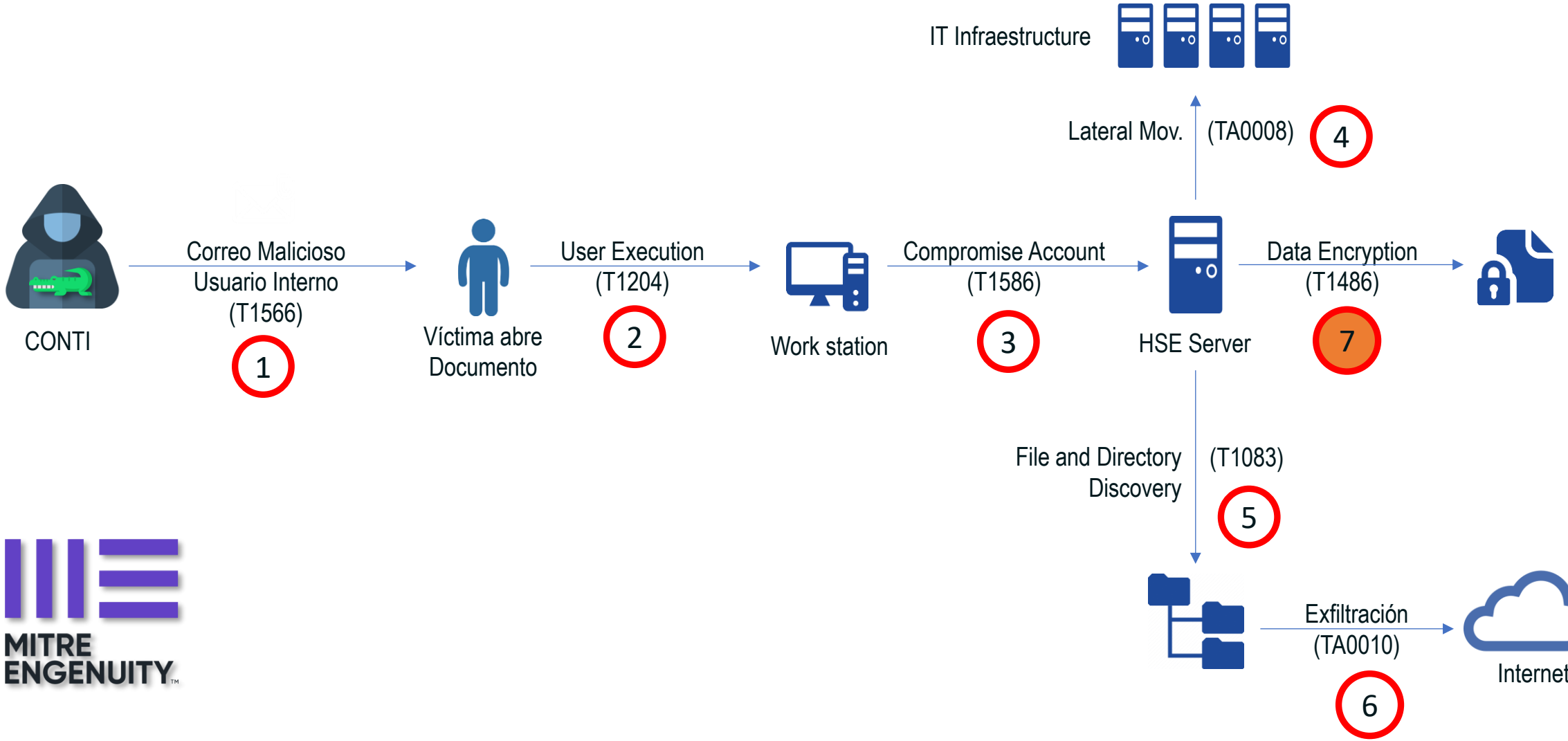
MITRE | ATT&CK®



DeTT&CT

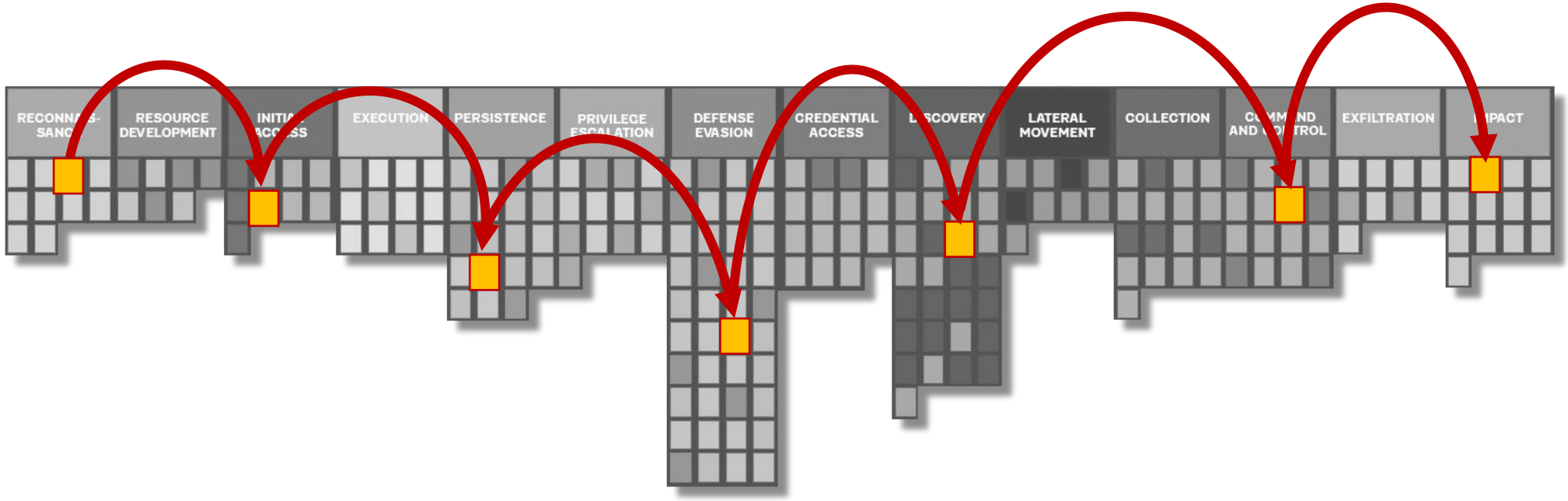
- Visibilidad
- Detección

Attack Flow



https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

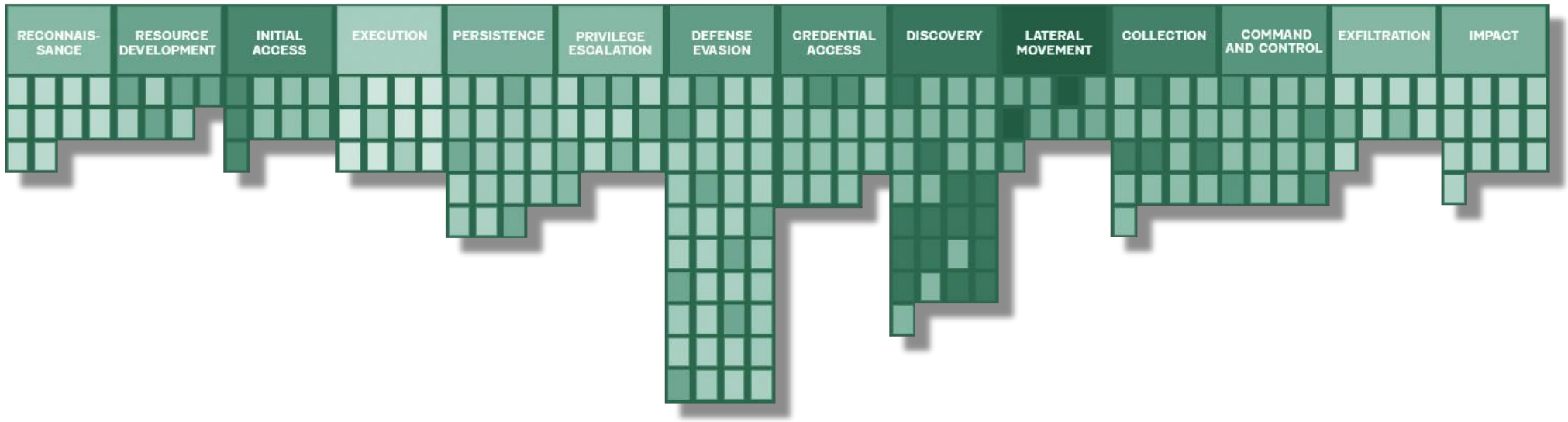
Attack Flow



https://center-for-threat-informed-defense.github.io/attack-flow/developers/

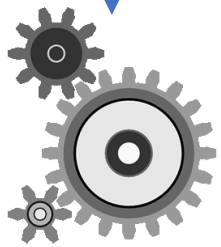
Atlas

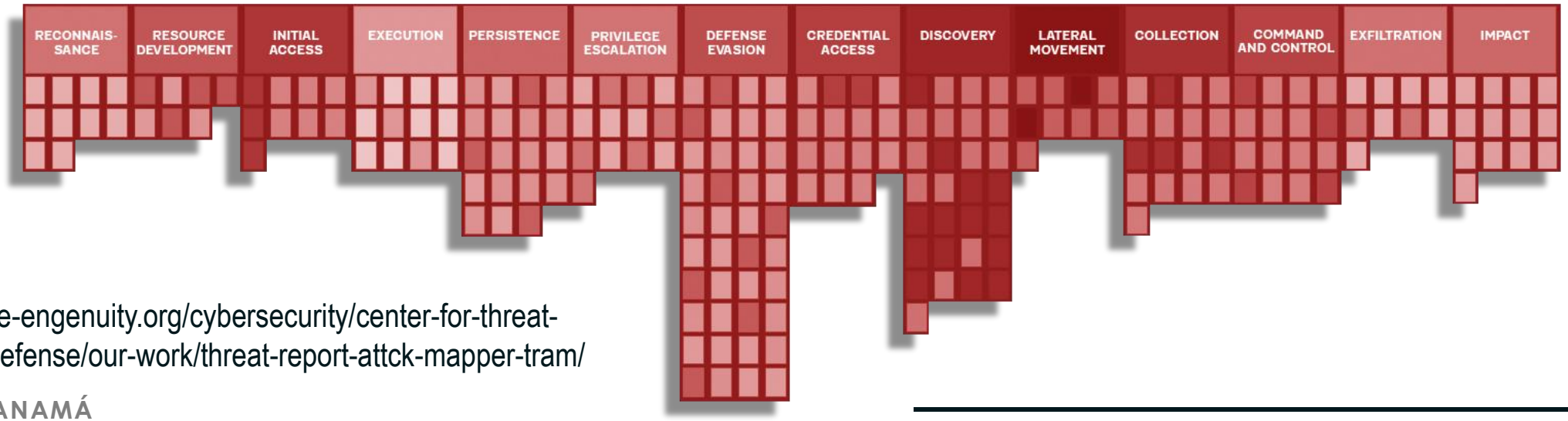
AI mapped to ATT&CK®



https://mitre-atlas.github.io/atlas-navigator/

TRAM: Threat Report Attack Mapping





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

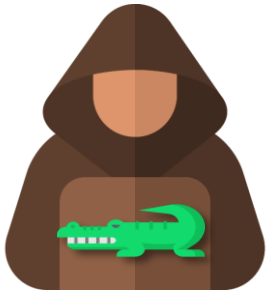
Demo time!!

Resumiendo

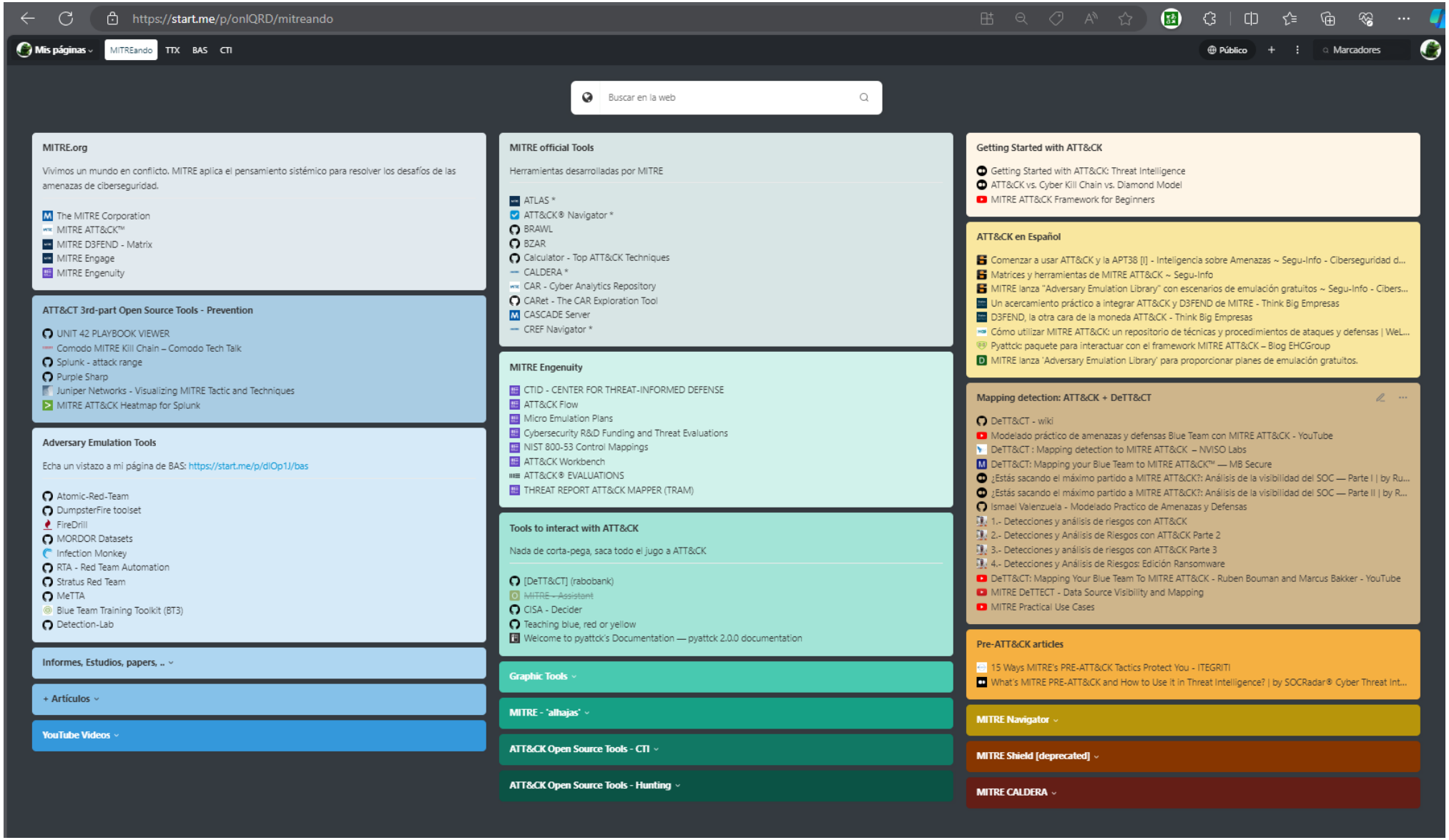
CONTROLES

vs

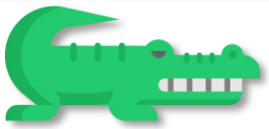
CAPACIDADES



MITRE goodies



- https://start.me/p/onlQRD/mitreando



Emilio Rico

Security Advisor at trc

@Emilio_RR

Emilio Rico Ruiz

https://github.com/3MilioRR

https://start.me/p/onlQRD/mitreando

IV JORNADAS STIC & CONGRESO ROOTED CON

CAPÍTULO **PANAMÁ**

GRACIAS

ORGANIZADORES

APOYO INSTITUCIONAL

COLABORADORES