



&

/Rooted[®] CON
ENTERTAINMENT

PRESENTAN



ESCUUELA DE CALOR



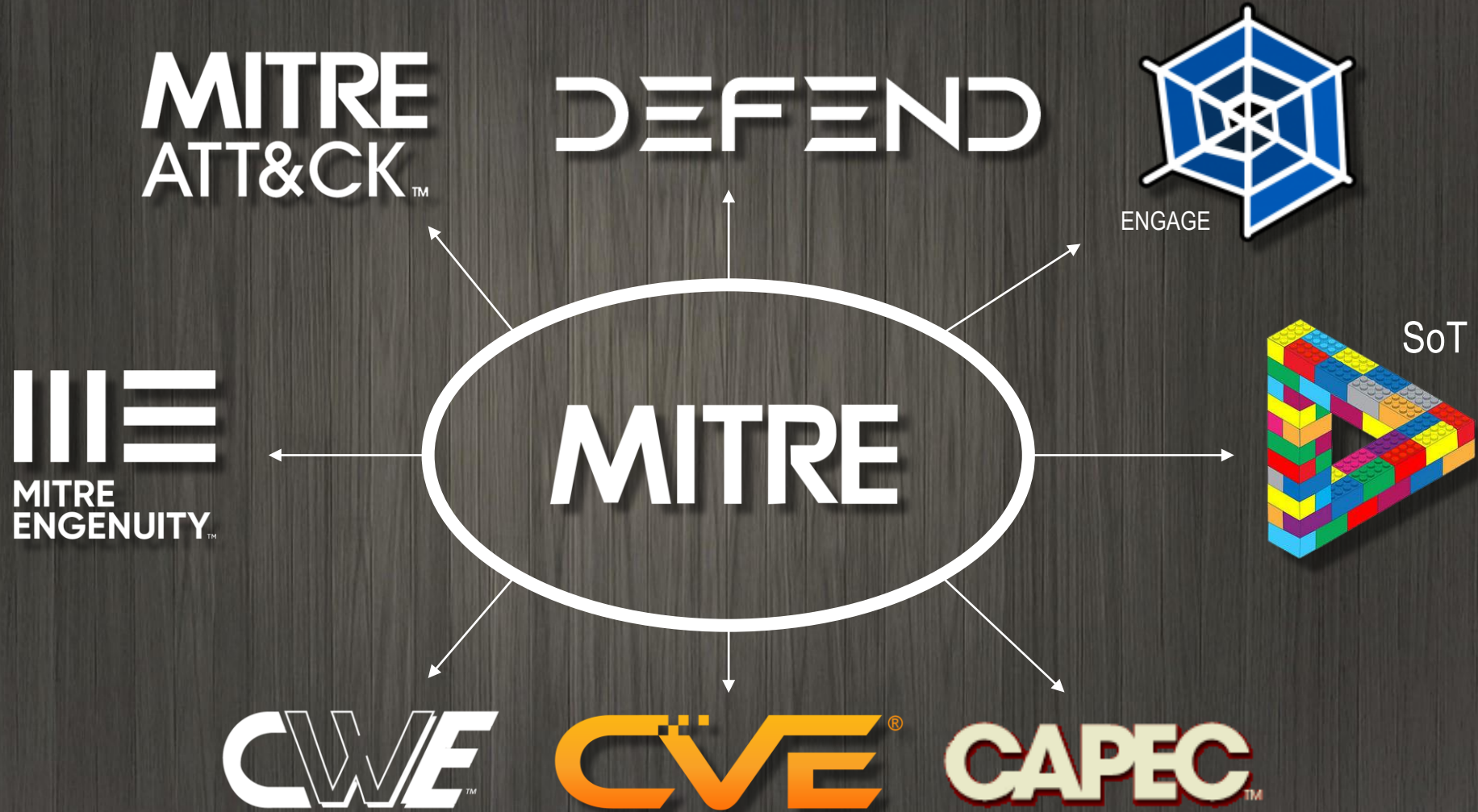


10 años

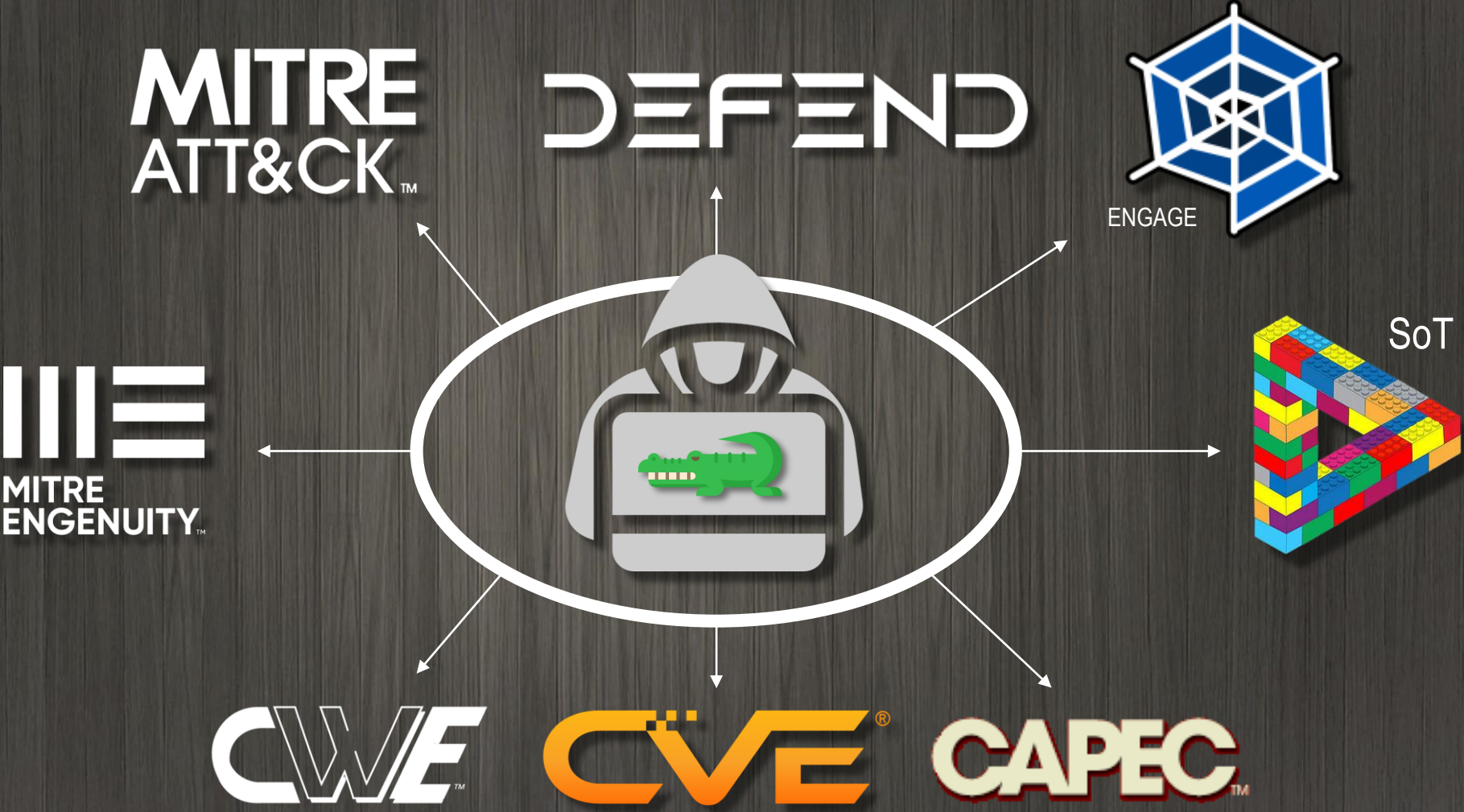
MITRE
ATT&CK™

2013 – 2023

MITRE WORLD



MITRE WORLD





MITRE
ATT&CK™

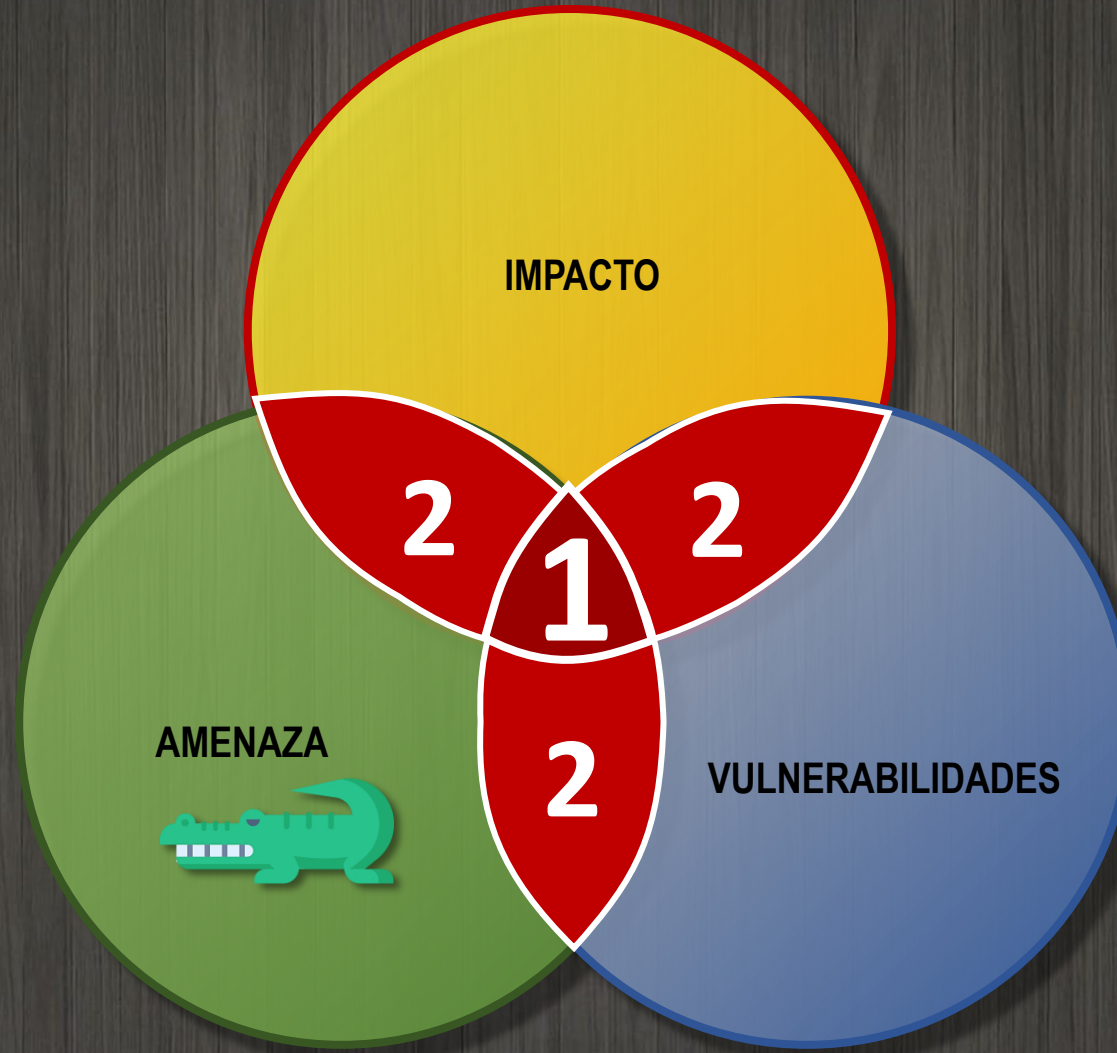


ATLAS

CREF Navigator

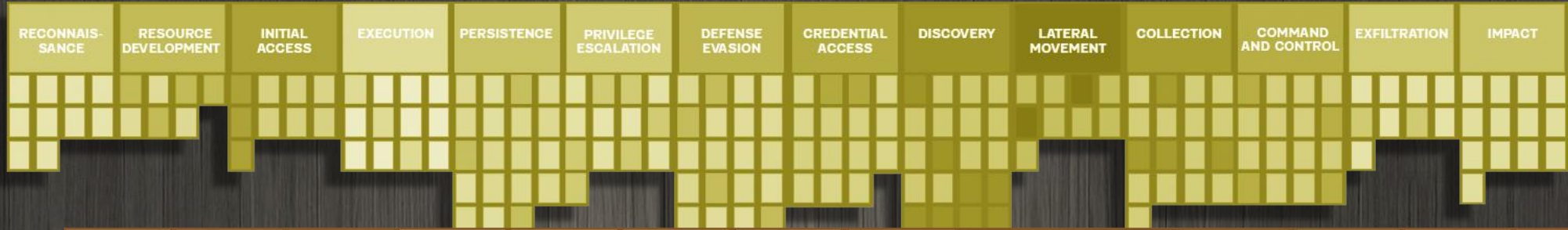


RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



Mapping THREATS | ATT&CK®

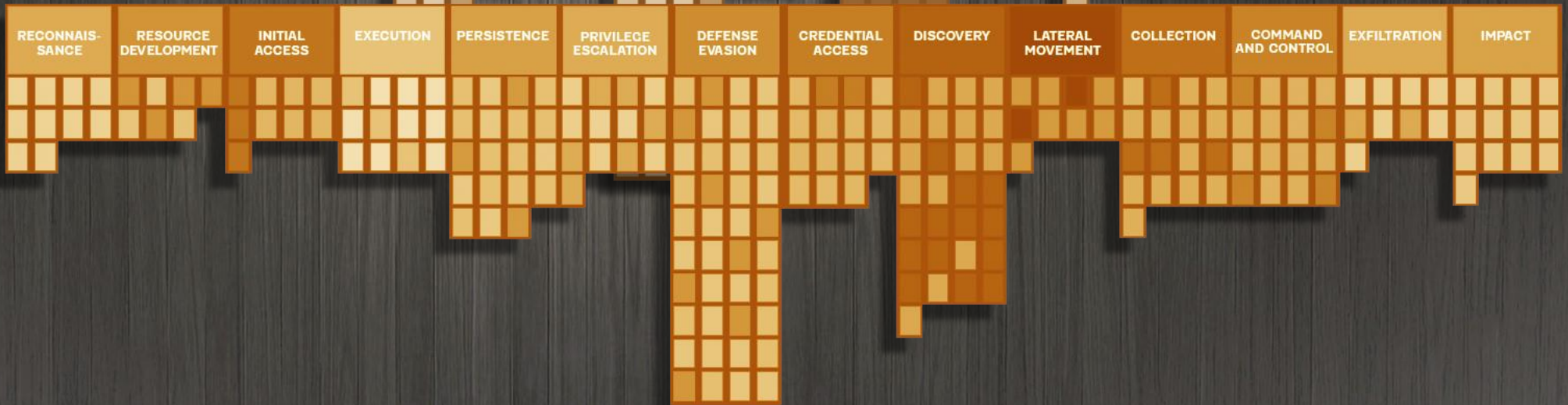
APT-B



APT-A

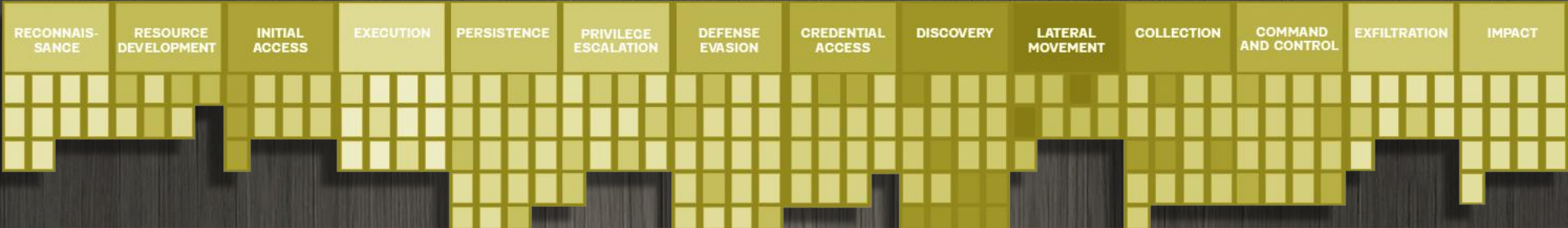


APT-C



Mapping THREATS | ATT&CK®

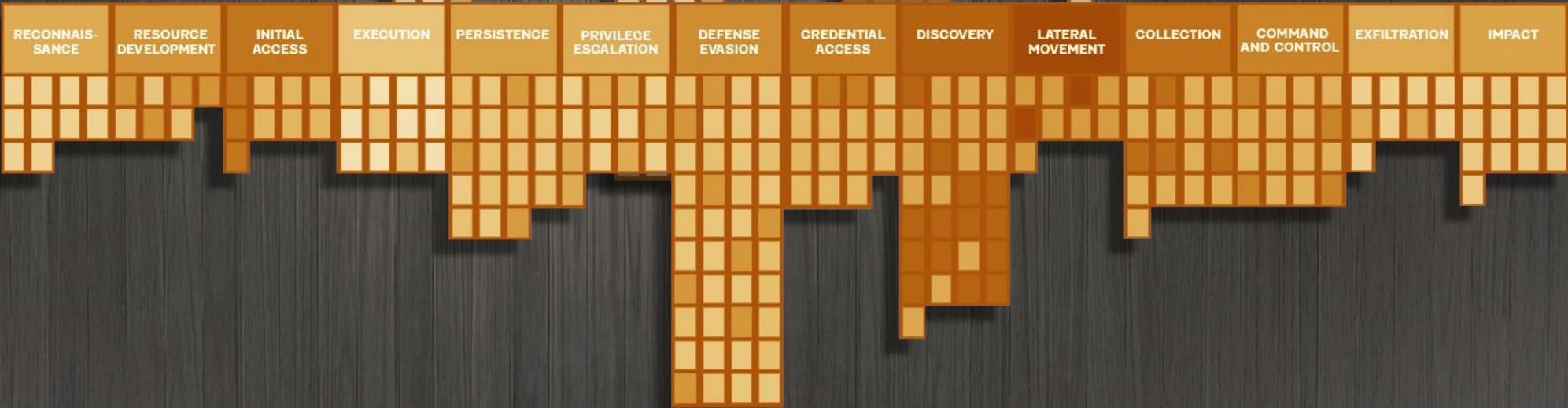
APT-B



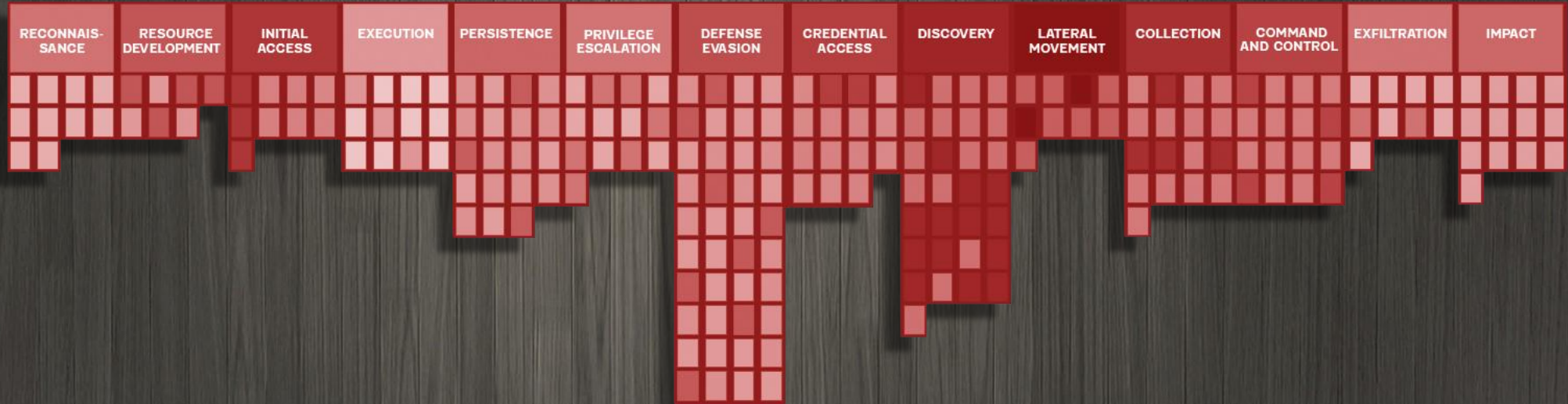
APT-A



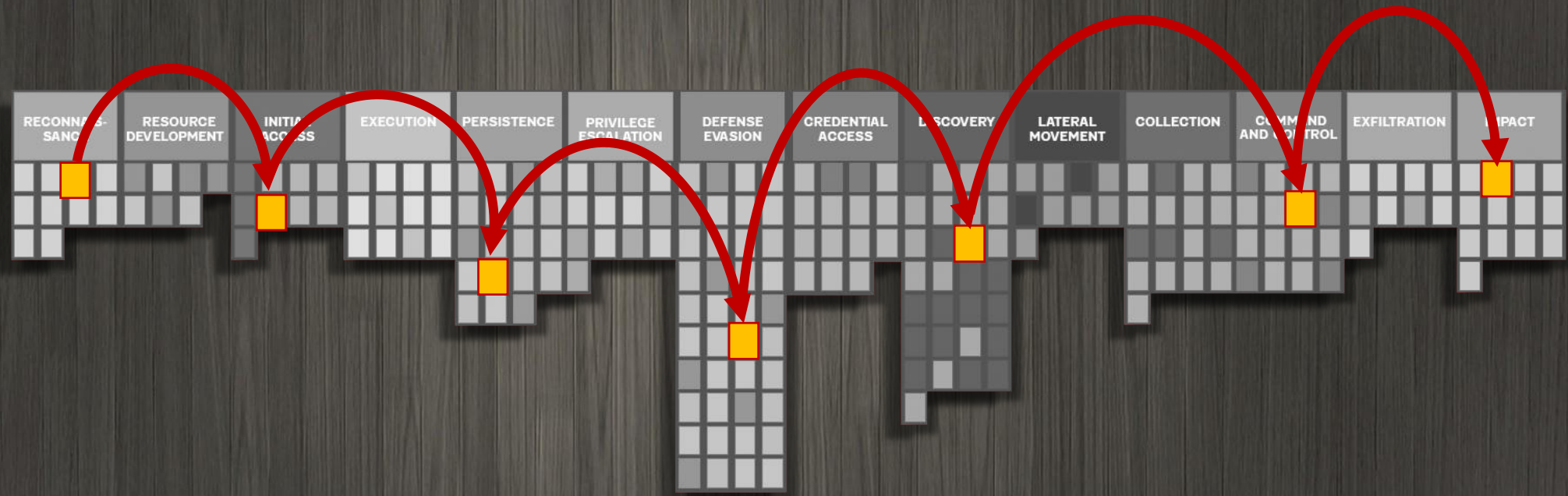
APT-C



Threats



Attack Flow |



Attack Flow



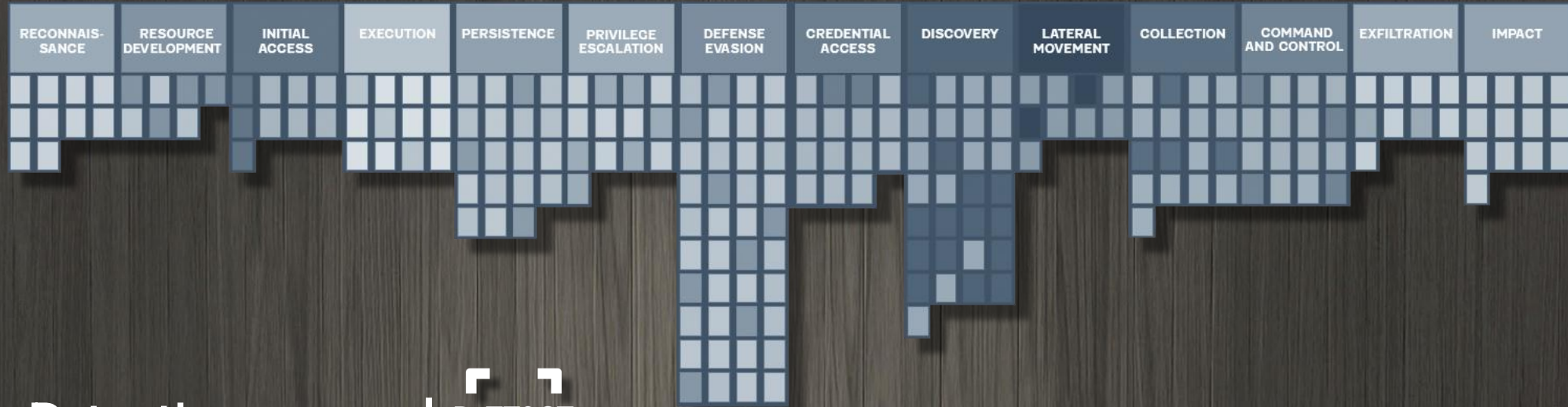
<https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>



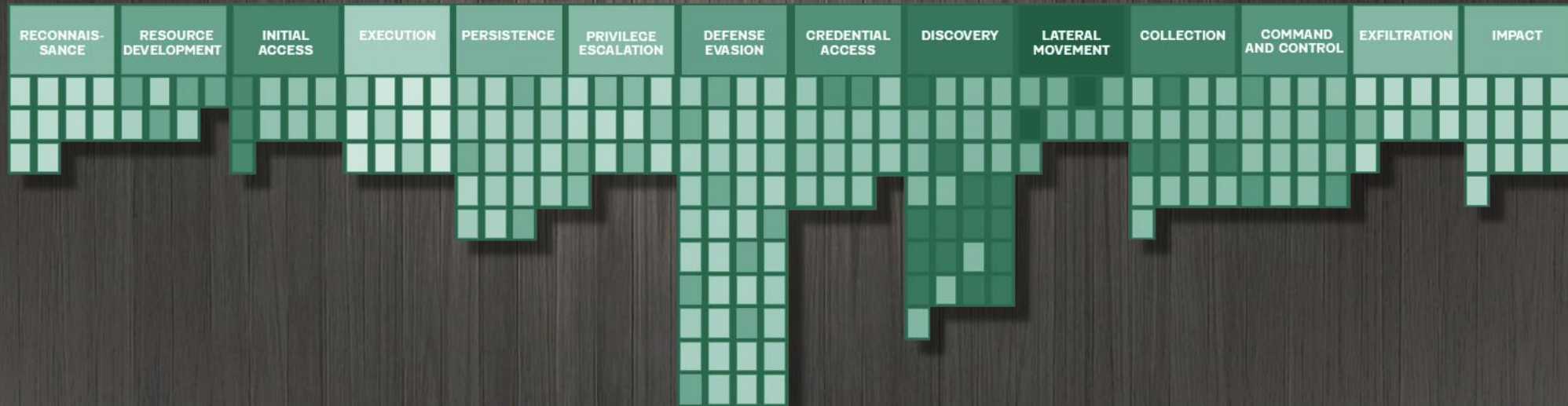
DeTT&CT

- Visibilidad
- Detección

Visibility scores |





















Detection scores |



Micro Emulación



Atomic Testing	Micro Emulation	Full Emulation
Emulate single technique	Emulate compound behaviors across 2–3 techniques	Emulate adversary operation
 Executable in seconds	 Executable in seconds	 Executable in hours
<i>E.g., Atomic Red test for T1003.001 - LSASS Memory</i>	<i>E.g., Fork & Run Process Injection</i>	<i>E.g., FIN6 adversary emulation plan</i>
 Easy to automate	 Easy to automate	 Easy to automate
 Validate atomic analytics	 Validate atomic analytics	 Validate atomic analytics
 Validate chain analytics	 Validate chain analytics	 Validate chain analytics
 Evaluate SOC against a specific set of TTPs	 Evaluate SOC against a specific set of TTPs	 Evaluate SOC against a specific set of TTPs
 Evaluate SOC holistically against specific groups	 Evaluate SOC holistically against specific groups	 Evaluate SOC holistically against specific groups



Demo time !!



ATT&CK  @MITREattack · 1d

Let's continue our ATT&CK misunderstandings series & discuss procedures.

People sometimes assume ATT&CK is trying to cover every possible way a (sub-)technique can be done, but our procedures only cover what we've seen in public reporting tied to Groups, Software, or Campaigns.



 10

 71

 141

 58,4K



“Hay APTs ocultas cerca del río
Esperando que caiga la noche”





MitreGator goodies



- Pass: 4randril@



- <https://www.grupotrc.com/.../escuela-de-calor>
- <https://github.com/3MlioRR/MTREando>
- <https://start.me/p/onlQRD/escuela-de-calor>



THE END

ESQUELA DE CALOR

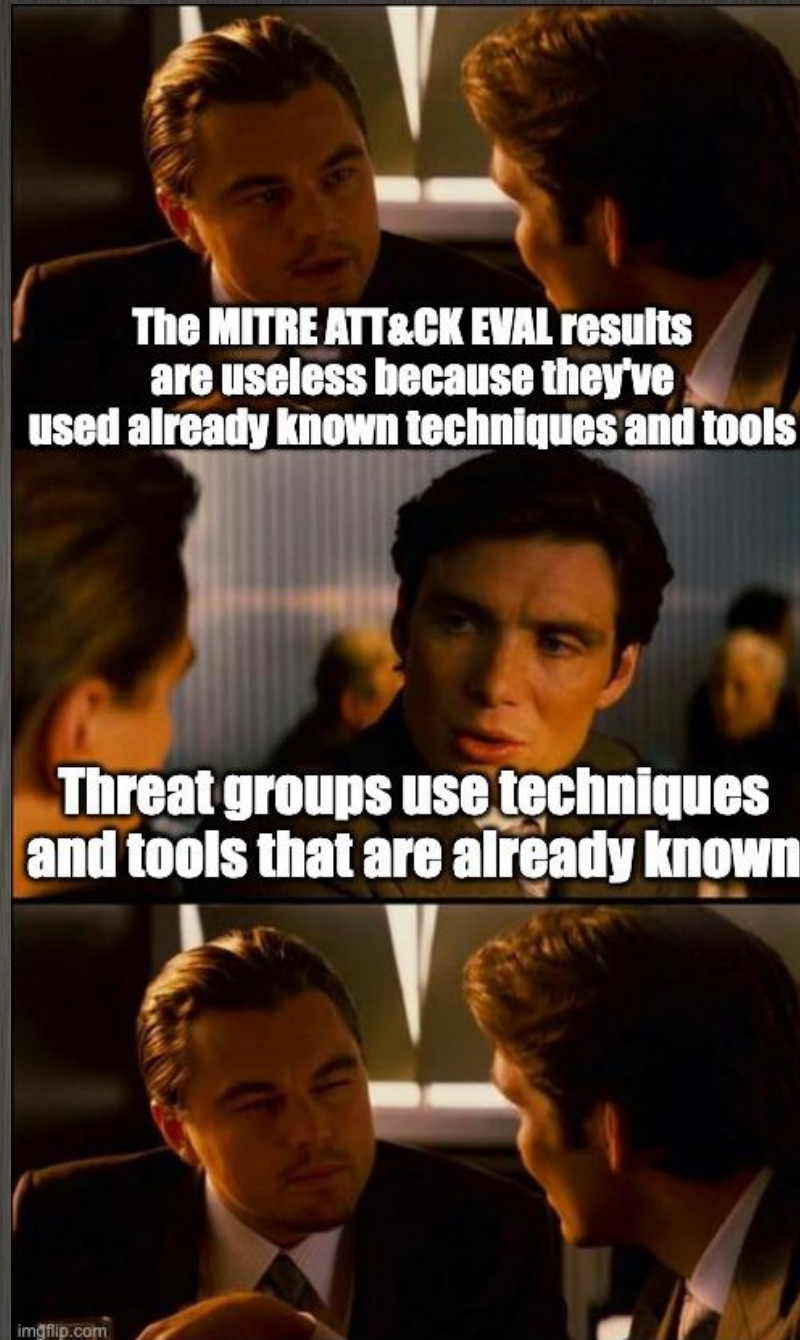


Muchas gracias !!



I go through life assuming everyone
gets **MITRE**
ATT&CK™ references.
And when people don't,
I'm like:







BEFORE MITRE ATT&CK



AFTER MITRE ATT&CK