ANALISANDO A FORMAÇÃO DO PONTO DE APOIO (FOOTHOLD) PARA A MOVIMENTAÇÃO LATERAL

RIVALDO OLIVEIRA

OVERVIEW

Tempest

ACESSO INICIAL

ESTABLISHED FOOTHOLD

Initial Discovery

Evasão de Defesa

Escalação de Privilégios

Persistência

Credencial De Acesso

Discovery

Evasão de Defesa

Persistência

LATERAL MOVEMENT

Credencial De Acesso

Collection

Collection

C&C

Collection

C&C

OBJECTIVE

EXFILTRAÇÃO

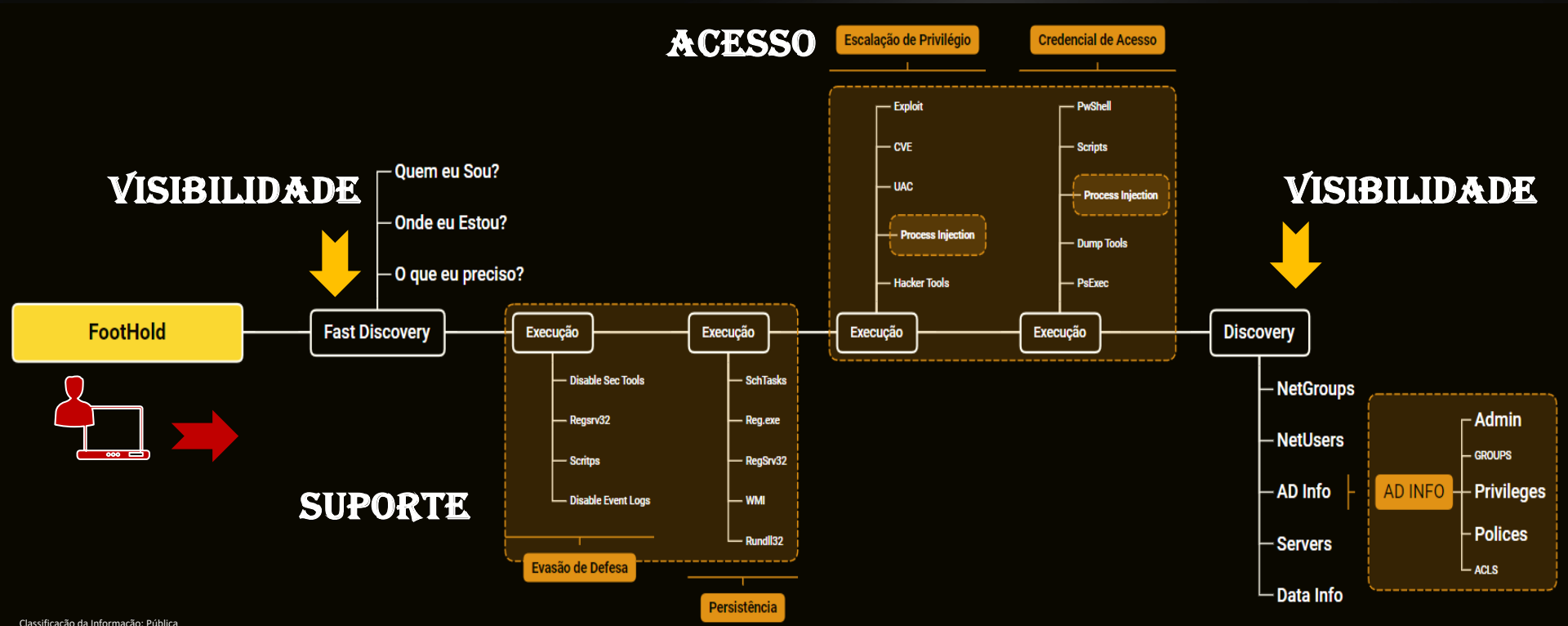
AD COMPROMISSE

EXFILTRAÇÃO

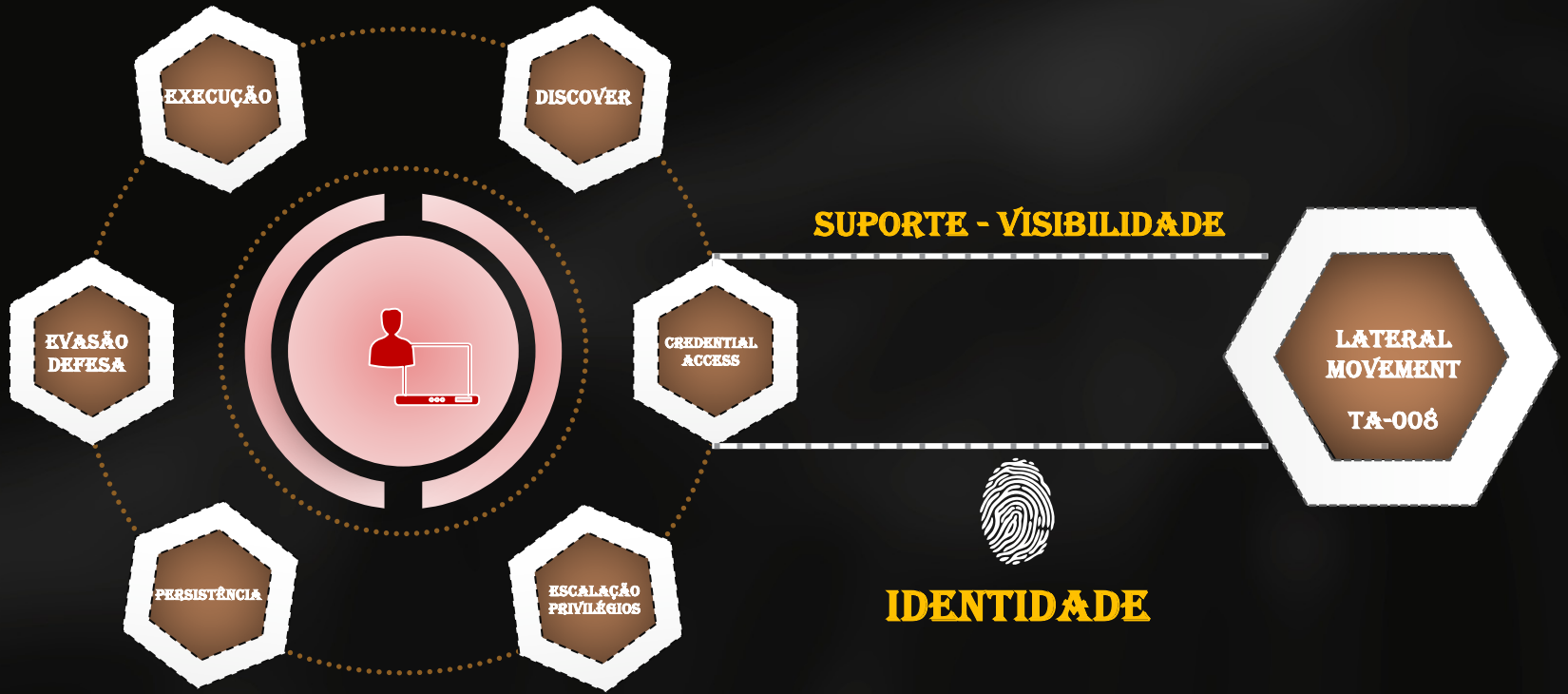
AD COMPROMISSE

ESTABLISHED FOOTHOLD

Tempest



ESTABLISHED FOOTHOLD



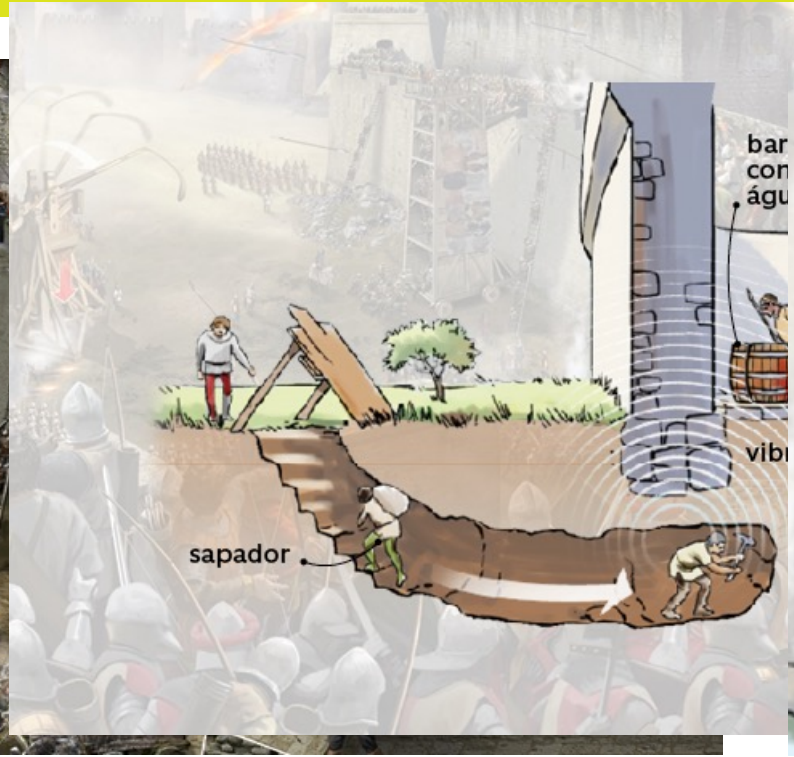
Tempest

ENDPOINT PROTECTION

☑ TERRENO ELEVADO (HIGH GROUND)

"EM UMA BATALHA, AQUELE EXERCITO QUE ESTIVER EM POSIÇÃO MAIS ELEVADA, TERÁ VANTAGEM SOBRE SEU ADVERSÁRIO"

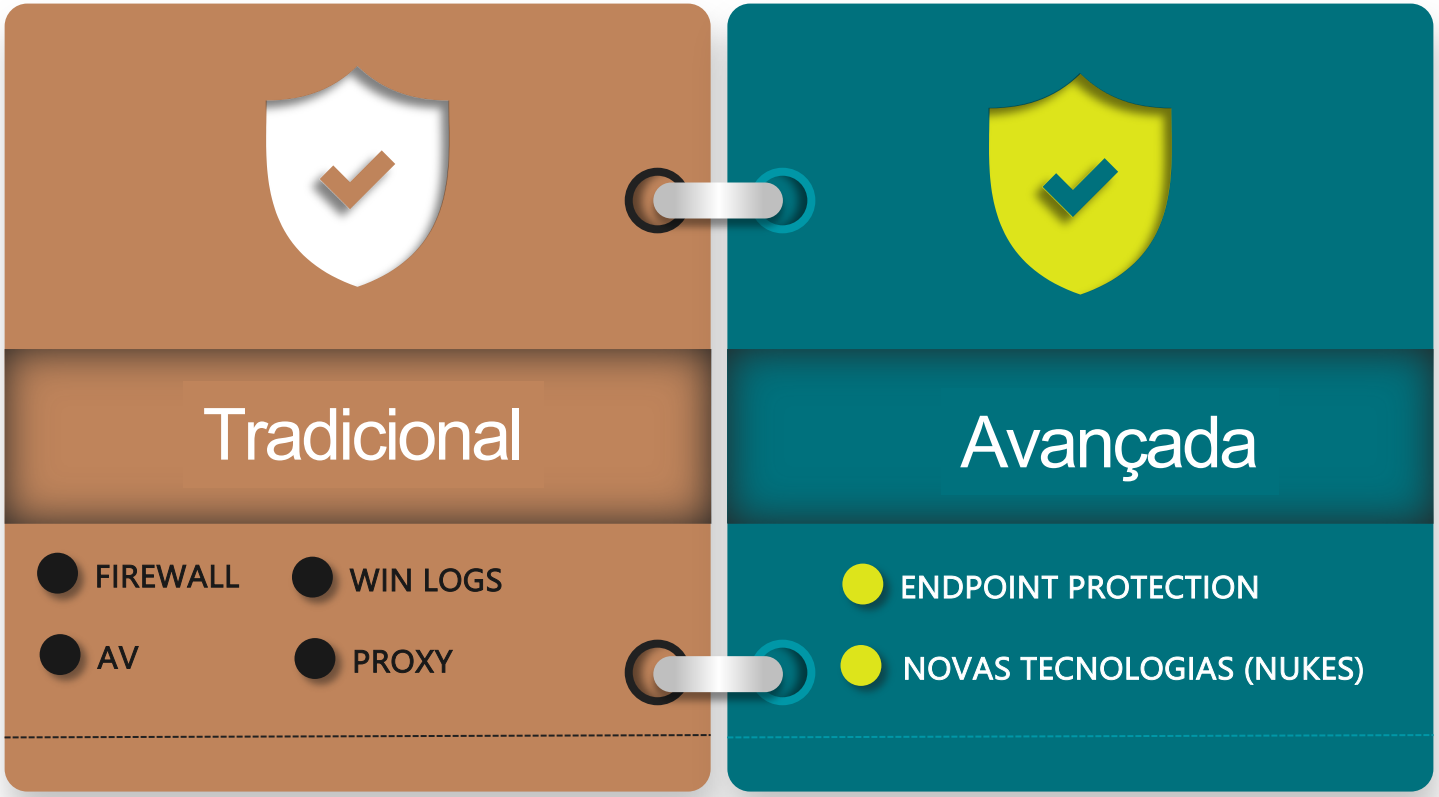
TERRENO ELEVADO



Fonte: https://super.abril.com.br/mundo-estranho/como-eram-as-guerras-na-idade-media/

TERRENO ELEVADO

Tempest



TERRENO ELEVADO

Tempest

EDR – ENDPOINT DETECTION & RESPONSE

- COMPORTAMENTO
- IOA

- TELEMETRIA

Telemetry Feature Category	Sub-Category					
Process Activity	Process Creation	🟩	🟩	🟩	🟩	🟩
****	Process Termination	🟧	🟩	🟩	🟩	🟩
****	Process Access	🟩	🟩	🟩	🟧	🟩
****	Image/Library Loaded	🟩	🟩	🟩	🟩	🟩
****	Remote Thread Creation	🟩	🟩	🟩	🟩	🟩
****	Process Tampering Activity	🟧	🟩	❓	🟥	🟩
File Manipulation	File Creation	🟩	🟩	🟩	🟧	🟩
****	File Opened	🟩	🟧	🟥	🟥	🟩
****	File Deletion	🟩	🟩	🟩	🟩	🟩
****	File Modification	🟩	🟩	🟥	🟥	🟩
****	File Renaming	🟩	🟩	🟩	🟩	🟩
User Account Activity	Local Account Creation	🟥	🟩	🟥	🟩	🟥
****	Local Account Modification	🟥	🟧	🟥	🟩	🟥
****	Local Account Deletion	🟥	🟩	🟥	🟩	🟥
****	Account Login	▯	🟩	🟩	🟩	🟩
****	Account Logoff	▯	🟩	🟩	🟩	🟩

https://github.com/tsale/EDR-Telemetry

TERRENO ELEVADO

Tempest

EDR BYPASS

CROWDSTRIKE
Microsoft
SentinelOne
SOPHOS
Bitdefender
Trellix
TREND MICRO

1 sem •

Silly question, is it possible that some EDRs are now able to hide their hooks when a debugger is used? I am pretty sure that the respective #EDR hooks NtAllocateVirtualMemory, NtWriteVirtualMemory, NtProtectVirtualMemory, also Telemetry Sourcerer show me that these APIs are hooked. But when I try to identify the hook with Windbg, I am not able to see the hook. Could remember that this was different in the past with the same EDR.

#redteam #itsec #reversing

https://lnkd.in/eqzK6MRe
Video demonstrating the use of my project FilelessPeLoader:
https://lnkd.in/eszK4QhF... ...ver ma

Bypass Windows Defender with FilelessPELoader - Mimikatz and Meterpreter
youtube.com

2 sem •

With my new blogpost "Meterpreter vs Modern EDR(s)" I want to show, that the shellcode of well-known C2 frameworks like Metasploit is not always a limiting factor. No new insights, but I would like to share them with the commu ...ver mais

Meterpreter vs Modern EDR(s) - RedOps
redops.at • 1 min de leitura

1 m •

📢 New EDR/AV evasion technique added to the #UnprotectProject by Alex J.: "Unloading Module Using FreeLibrary." This technique involves unloading a spe ...ver mais

3 sem •

The Prelude talk recording is now available to watch on YouTube for those who are interested:
... ...ver mais

AV/EDR Evasion: Packer Style
youtube.com

TERRENO ELEVADO

Tempest

I - ENDPOINT PROTECTION

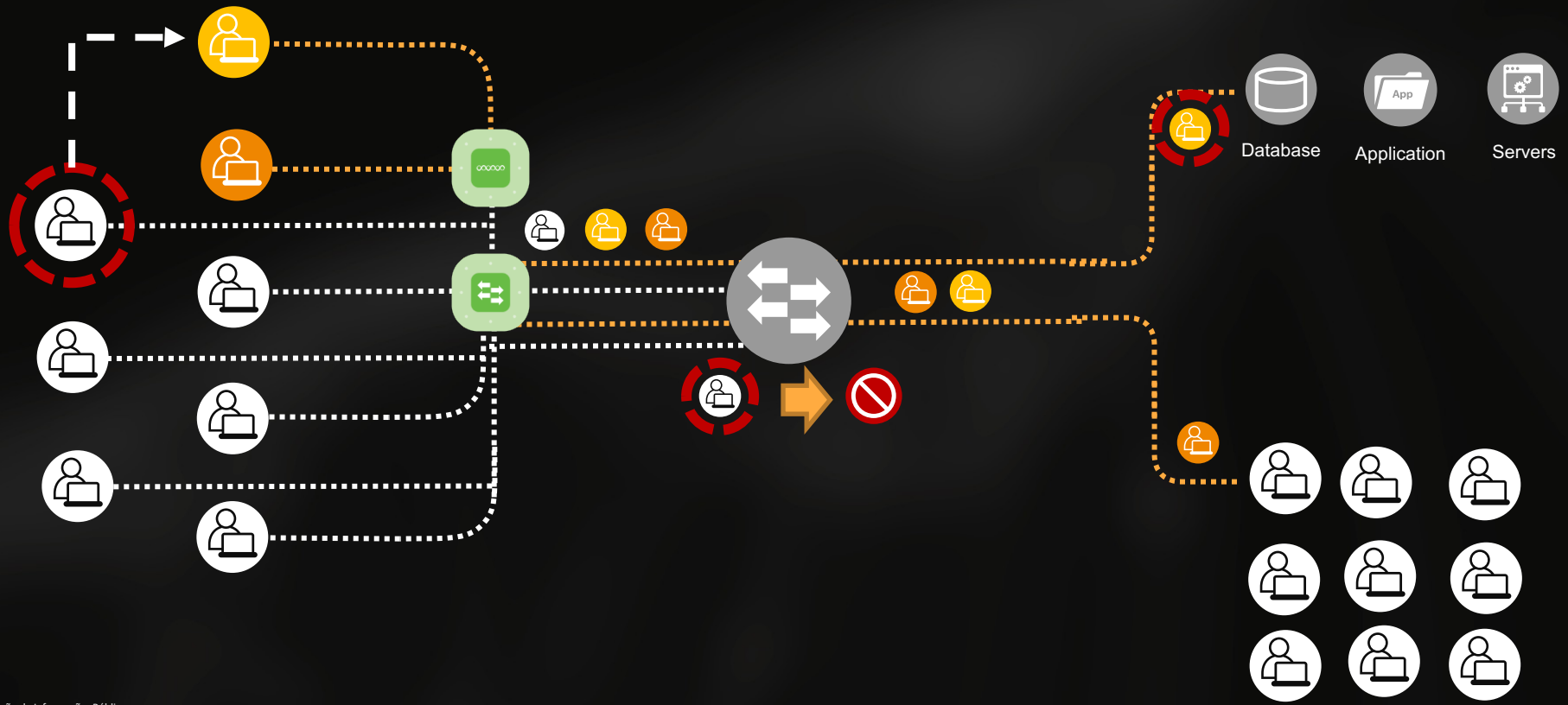
- POSTURA & INTEGRIDADE
- SIMULATION (RED TEAM)
- HARDENING (TERRA ARRASSADA)

II - NUKES

- THREAT HUNTING
- NOVAS TECNOLOGIAS
- ***IDENTIDADE

LATERAL MOVEMENT

Tempest



IDENTIDADE

DETECTAR

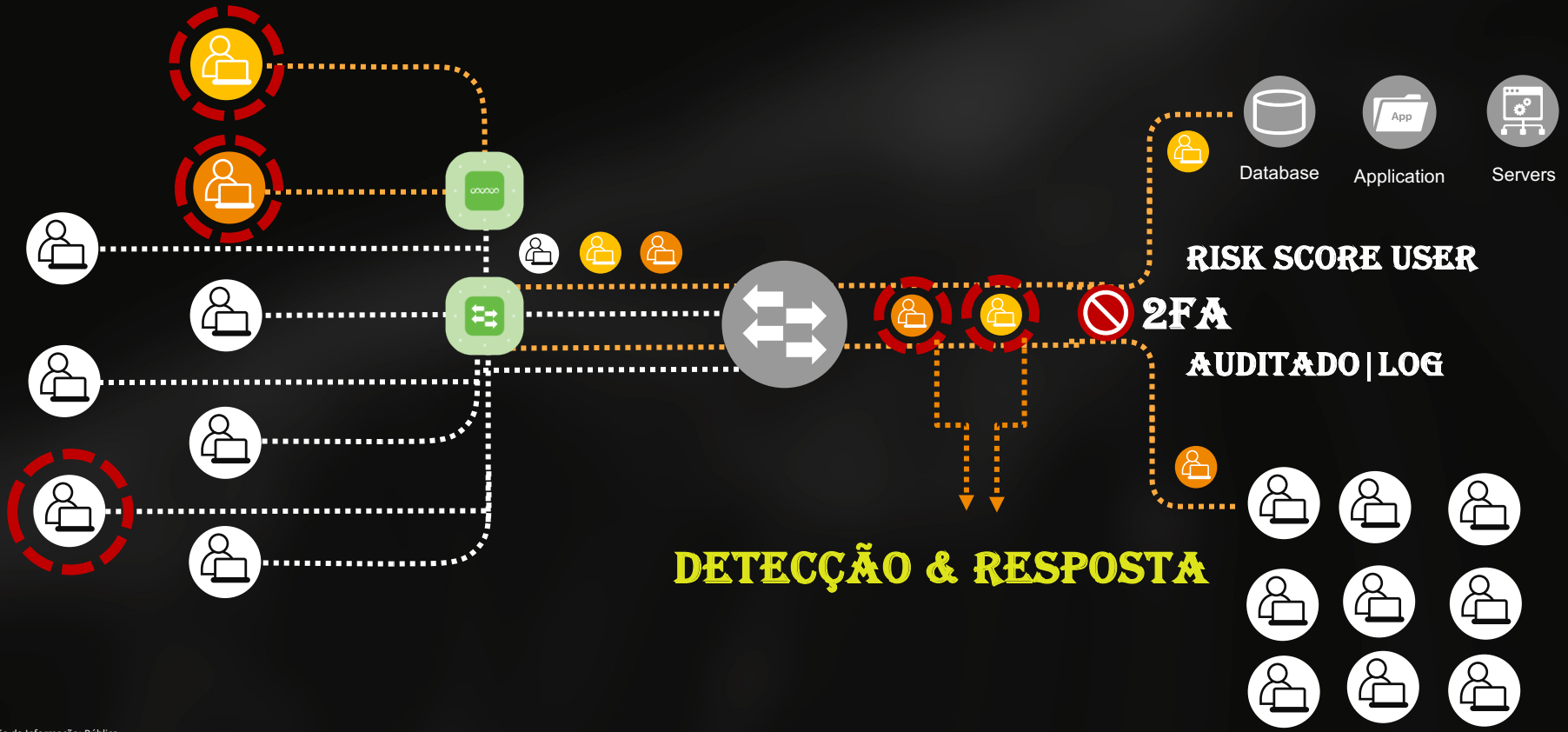
RESPONDER

TIME RESPONDER

CONTER

ITDR

Tempest



Tempest

OBRIGADO!

RIVALDO OLIVEIRA

WWW.LINKEDIN.COM/IN/RIVALDOCOLIVEIRA/