



Tempest

ACADEMY

Conference  
2023

# A Guerra do Kernel

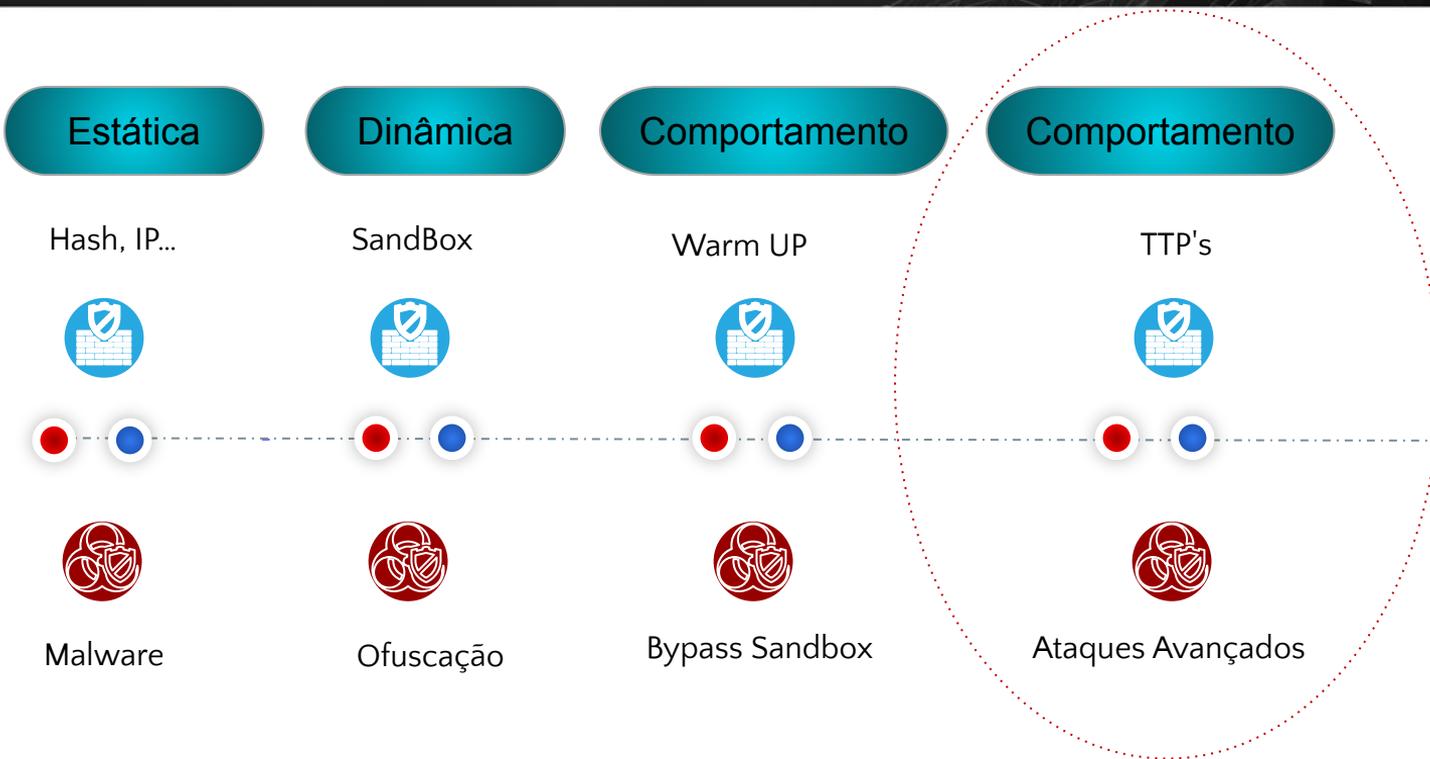
(Endpoint Attacks)

---

Rivaldo Oliveira



# Defense Evasion - Timeline



# Endpoint Attacks - Overview

## ACESSO

### Escalção de Privilégio

### Credencial de Acesso

- Exploit
- CVE
- UAC
- Process Injection
- Hacker Tools

- PwShell
- Scripts
- Process Injection
- Dump Tools
- PsExec

Execução

Execução

Discovery

- Quem eu Sou?
- Onde eu Estou?
- O que eu preciso?

FootHold

Fast Discovery

Execução

Execução

- Disable Sec Tools
- Regsrv32
- Scripts
- Disable Event Logs

- SchTasks
- Reg.exe
- RegSrv32
- WMI
- Rundll32

Evasão de Defesa

Persistência

## SUPORTE

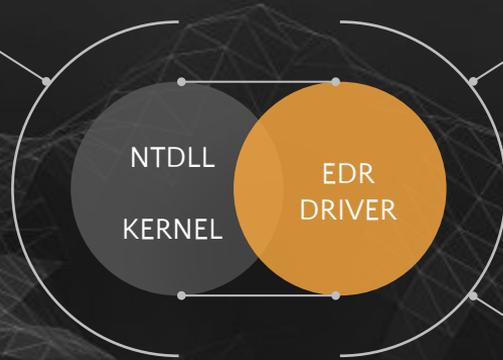
- NetGroups
- NetUsers
- AD Info
- Servers
- Data Info

- Admin
- GROUPS
- Privileges
- Polices
- ACLS

# Defense Evasion - EDR Timeline



Criação de Processo no Sistema

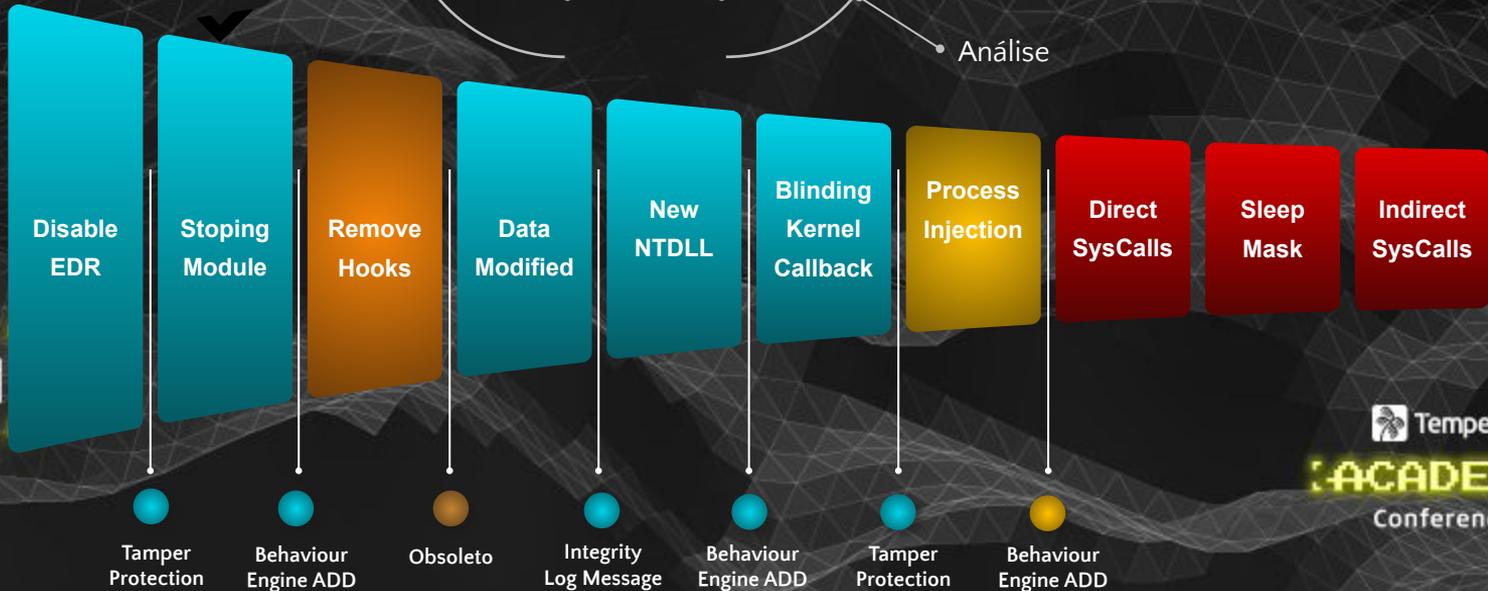


Monitoramento de chamadas ao Kernel



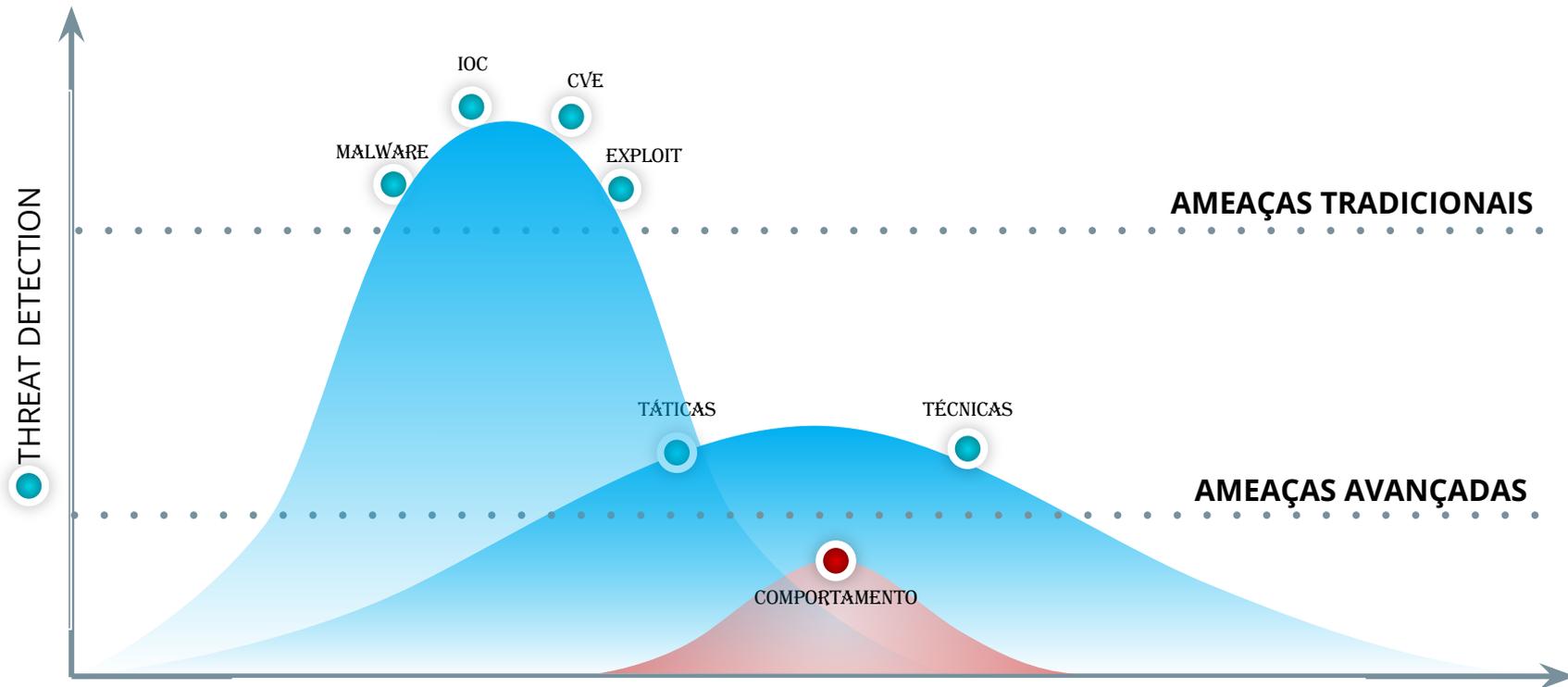
HOOKING

Análise



Tempest  
[ACADEMY]  
Conference

# Threat Detection



# ENDPOINT

# PROTECTION

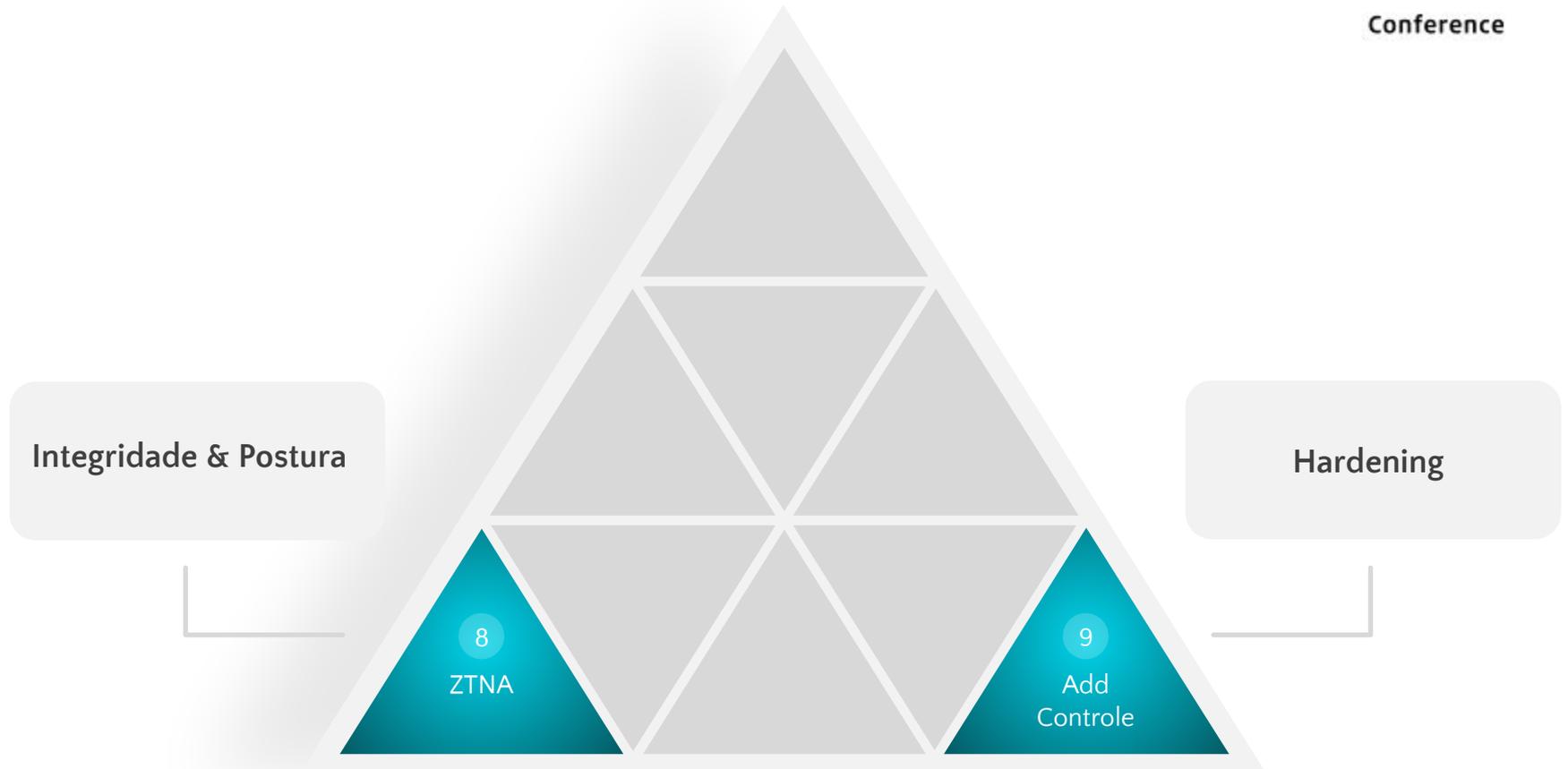
- **POSTURA & INTEGRIDADE**
- **WARMUP & SIMULATION**
- **NUKES (THREAT HUNTING)**

 Tempest

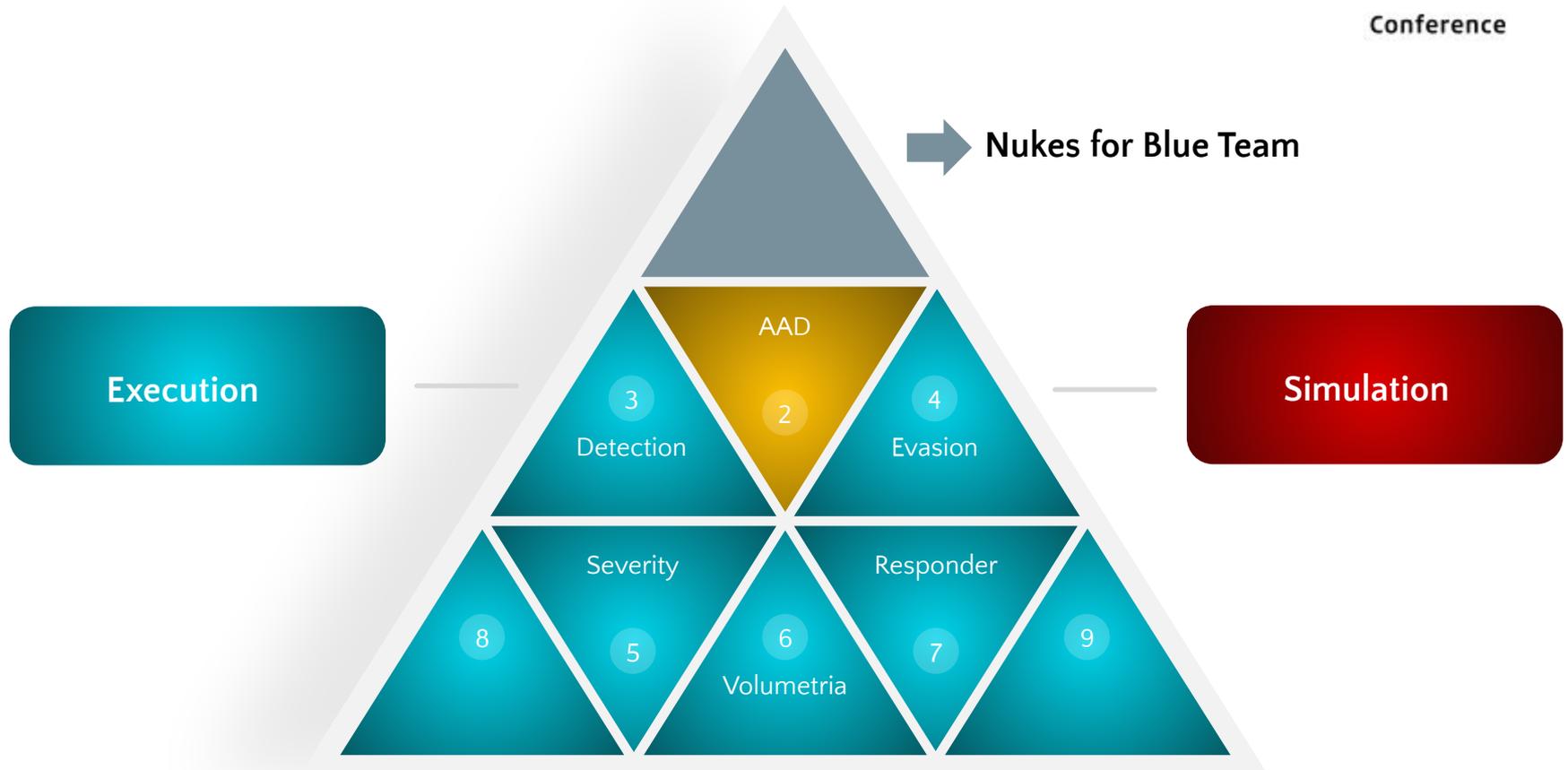
**ACADEMY**

Conference

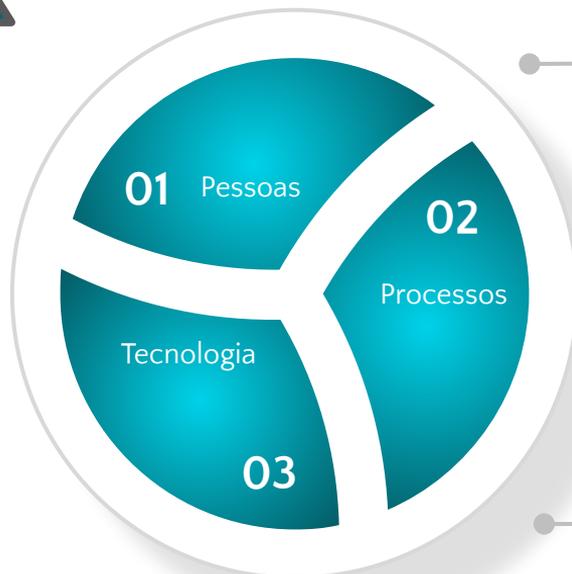
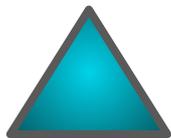
# BASE - ENDPOINT PROTECTION



# WARMUP - ENDPOINT PROTECTION



# NUKES - Threat Hunting



SKILL TÉCNICO

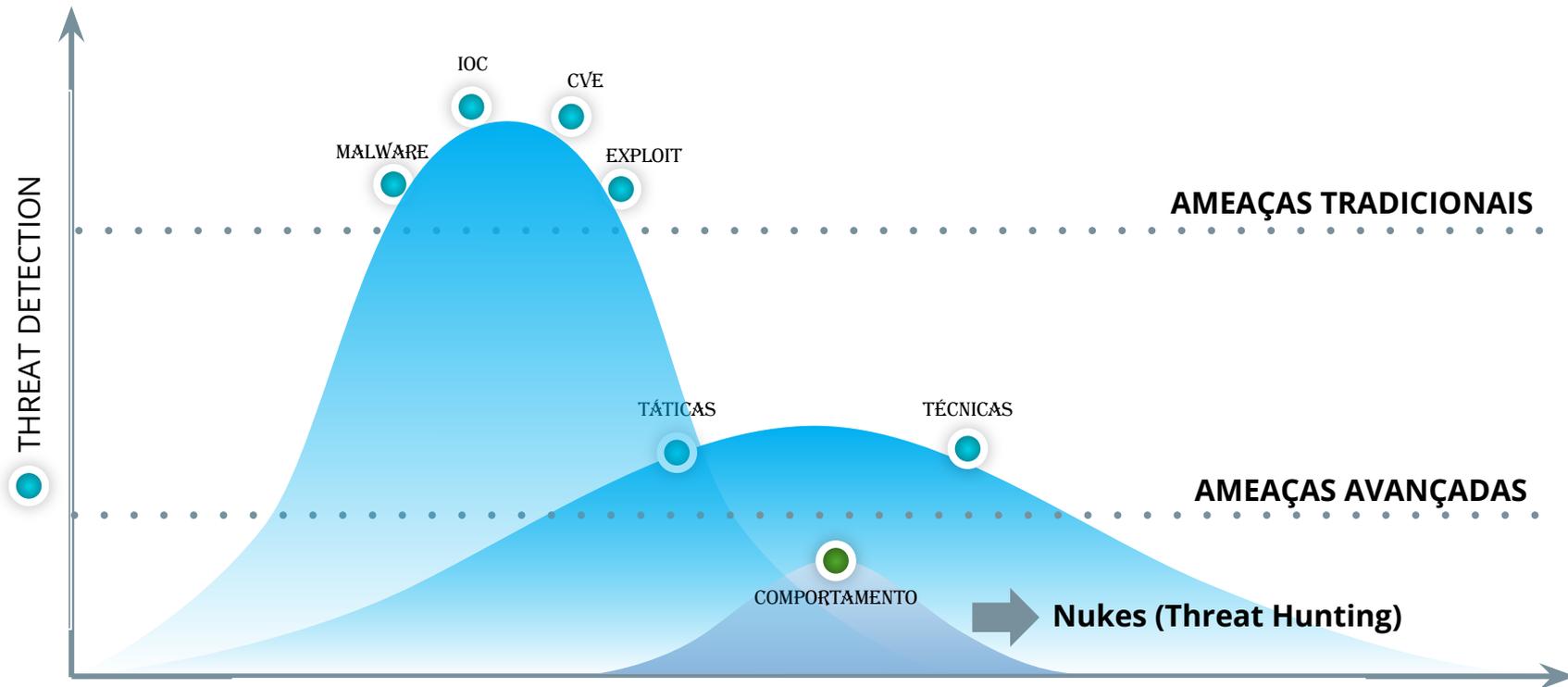


HIPÓTESES  
FORMATO  
ESCOPO  
FLUXO  
WARROM



Telemetria  
Searchs/Volumetria

# Threat Response





Tempest

# Obrigado!

## ACADEMY

Conference

2023

Rivaldo Oliveira

<https://www.linkedin.com/in/rivaldocoliveira/>

