Token Ops

Dr. Victor Pasknel
Yuri Maia

RED WOLVES

whoami

Victor Pasknel

- Doutor em Informática Aplicada (UNIFOR)
- Pentester / Red Team (~14 anos)
- VP @ RedWolves

Yuri Maia

- OSEP, CRTO e CRTL
- Pentester / Red Team (~7 anos)
- Consultor @ RedWolves

Agenda

01

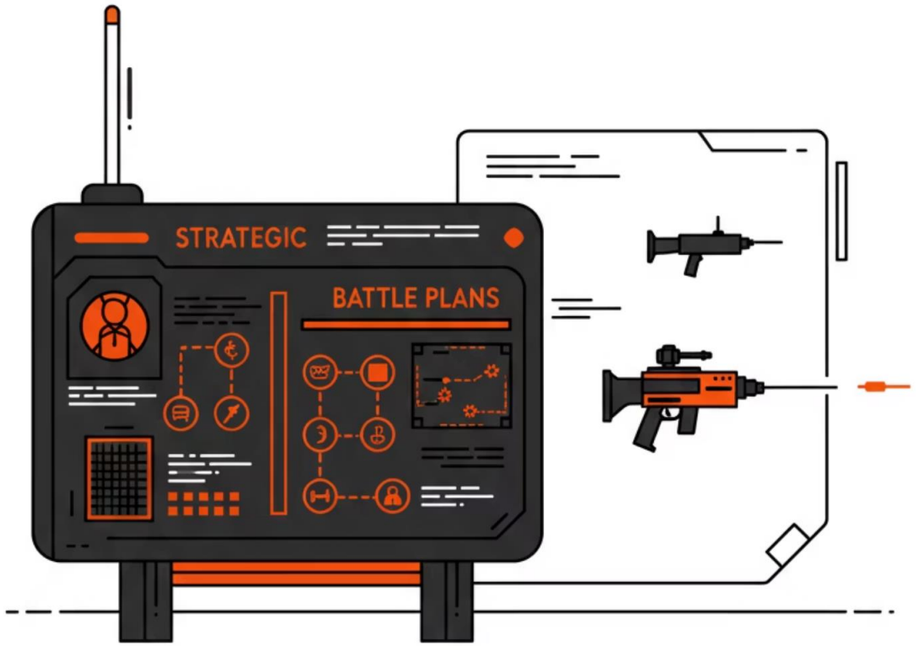
Motivação

02

Token Ops: Microsoft

03

Token Ops: DevOps



Motivação

https://x.com/cyb3rops/status/1892833225526989121

Motivação

Motivação

Uso crescente de tokens ao longo dos anos

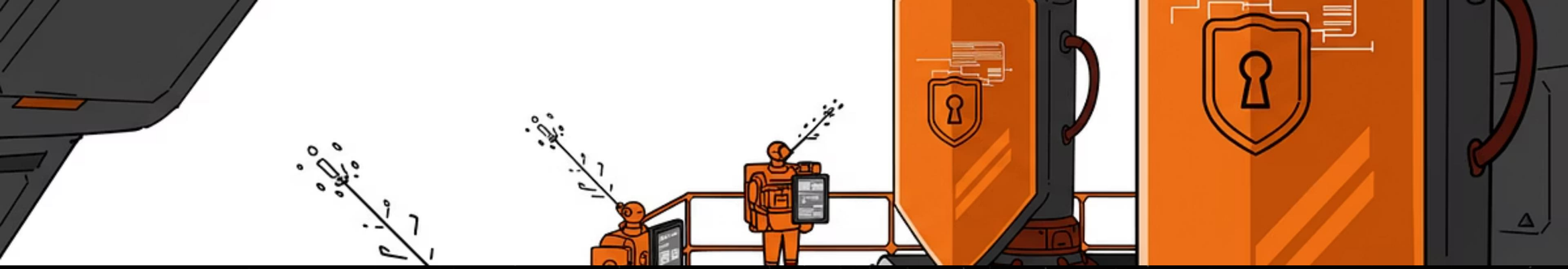
APIs em todos os lugares !

Movimentação da industria para *passwordless*

Vantages de tokens:

- Tokens vazados em diversas fontes
- Não precisa realizar bypass de MFA
- Oportunidades de movimentação lateral

Token Ops: Microsoft



Token Ops: Microsoft

EDRs

Sistemas de detecção e resposta em endpoints

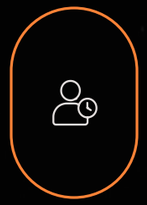
PPL / Credential Guard

Habilitado por padrão no Win11

AD Honeypots (decoys)

Ambientes sofisticados com armadilhas

Token Ops: Microsoft – Tipos de Tokens



Primary Refresh Token (14 dias)

Family of Refresh Tokens (90 dias)

Refresh Token (90 dias)

Access Token (60 min)

Token Ops: Microsoft – Dump!?

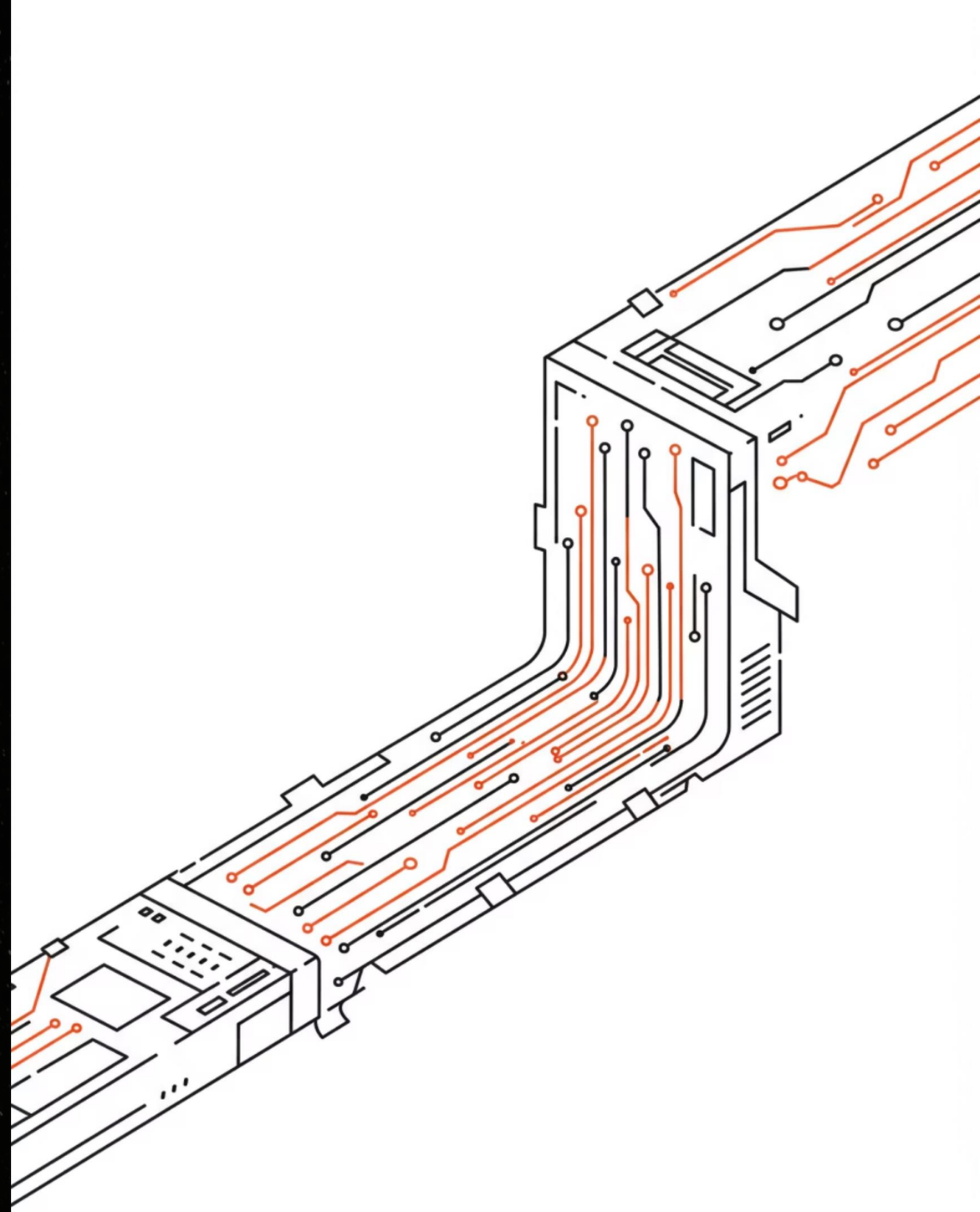
Dump de memória dos processos M365

Win11 (notepad e paint)

Arquivos de cache TBRES

`%LOCALAPPDATA%\Microsoft\TokenBroker\Cache`

Não precisa ser administrador local!!



https://github.com/g0ttfrid/Steal365

Token Ops: Microsoft

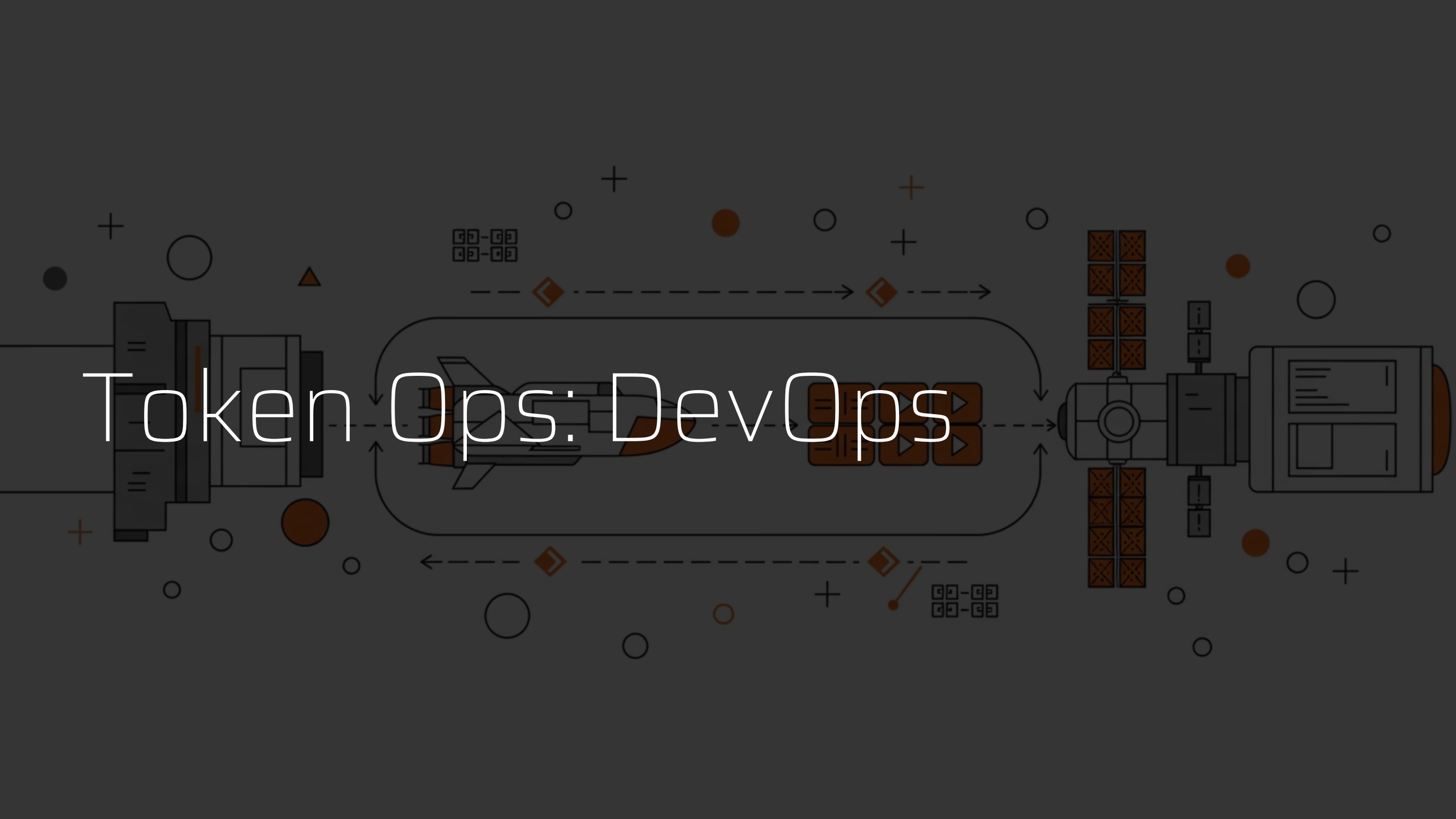
Demonstrações

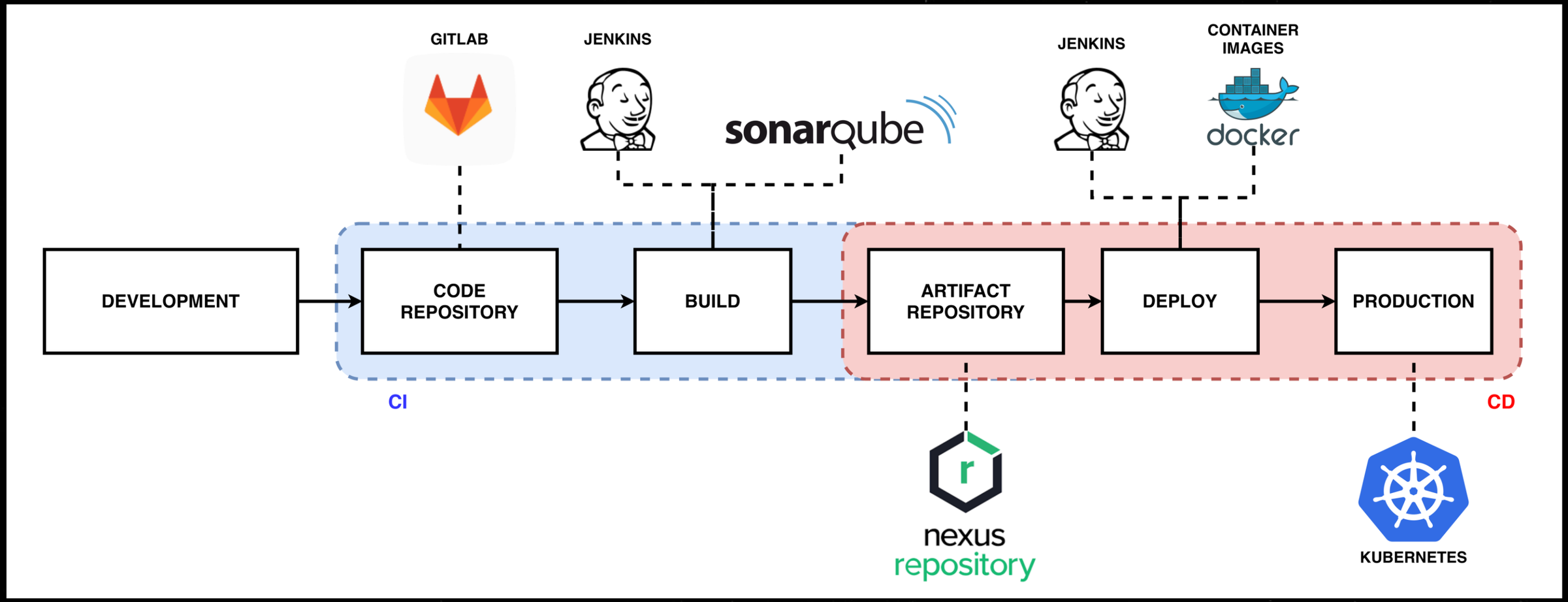
Obtendo Tokens

- Dump de memória M365 (Steal365.cs)
- Arquivos de cache TBRES (Invoke-TBRESDecryptor.ps1)

Utilizando os Tokens

- Graph API
- Token no Teams (OfficeLeak.ps1)


Token Ops: DevOps



Token Ops: DevOps

Token Ops: DevOps

Múltiplos alvos

- Múltiplos alvos dentro do ecosistema de DevOps
- Uso extenso de APIs em esteiras de CI/CD

Acesso a MUITA informação

- Código fonte de projetos
- Imagens de containers
- Credenciais (Banco de dados & AD)
- Tokens para outras ferramentas de DevOps
- Cloud (AWS/Azure/GCP)

Token Ops: DevOps

Epyon

- Canivete suiço para pentest em ambientes DevOps
- Implementado em Golang
- Diversos módulos disponíveis
- Integração com outras tools
- Github
  - https://github.com/pasknel/epyon

> *Talk Epyon*
> (Cloud Village - DEFCON 32)

Token Ops: DevOps

Demonstrações

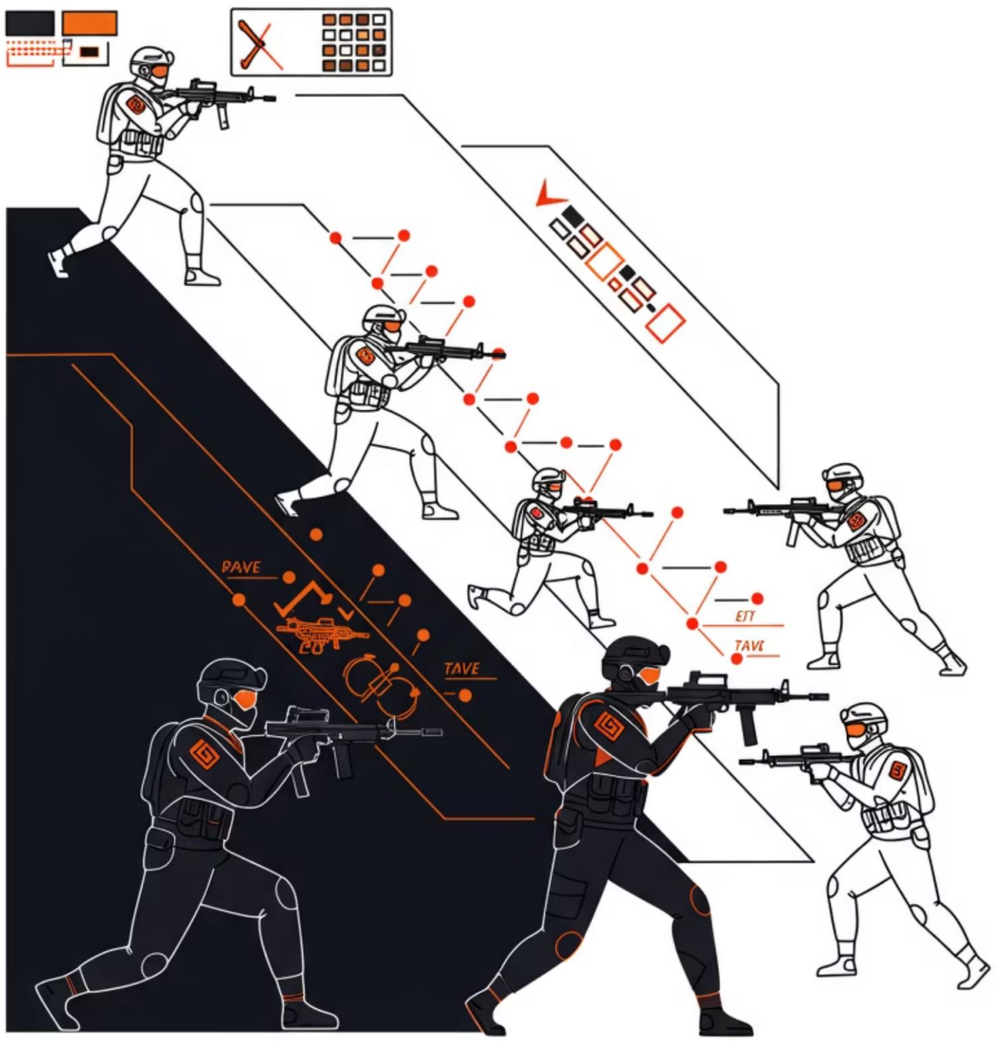
Baseado em projetos da vida real

Dividido em 3 partes

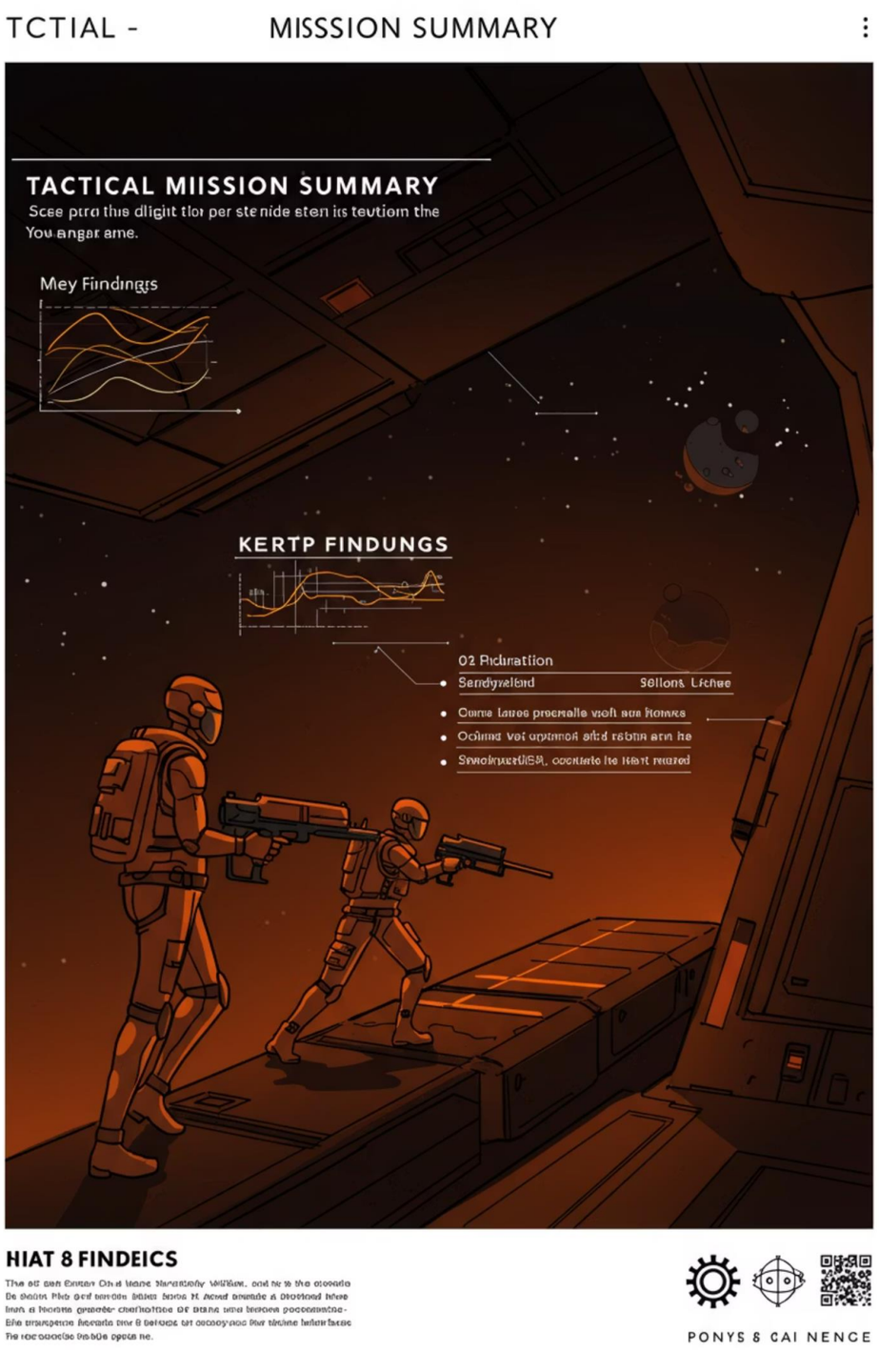
Parte 01: Acesso Inicial

Parte 02: Escalação de privilégios

Parte 03: Movimentação lateral



Conclusões



Conclusões

- Tokens são o novo OURO para red teams
- Omnipresença de APIs em ambientes corporativos
- Diversas oportunidades de abusos de APIs

Obrigado!

Dúvidas ?