sepian

Seguridad Digital
de Andalucía

WEBINAR

Protección del punto final con soluciones EDR

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

Contenidos

Qué vamos a tratar

Contenidos

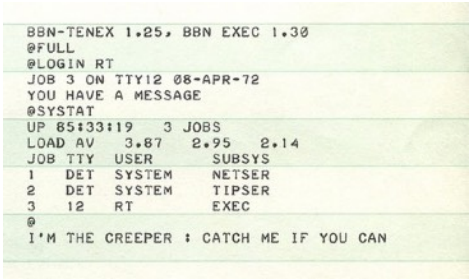
1. Evolución del malware
2. Evolución de soluciones anti-malware
3. Definición de EDR y sus funcionalidades
4. Principales diferencias de EDR frente a otras soluciones antimalware
5. Tipo de despliegue de la solución
6. Estado actual del mercado
7. Posibilidades de ampliación de funcionalidad con otras soluciones
8. Aplicaciones prácticas de EDR

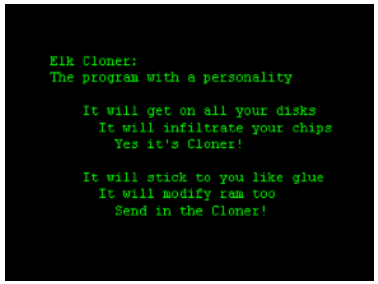
Evolución del malware

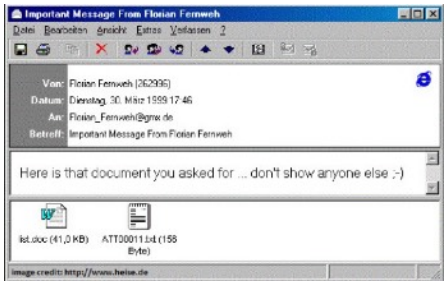
1971 - Creeper

1982 - Elk Cloner

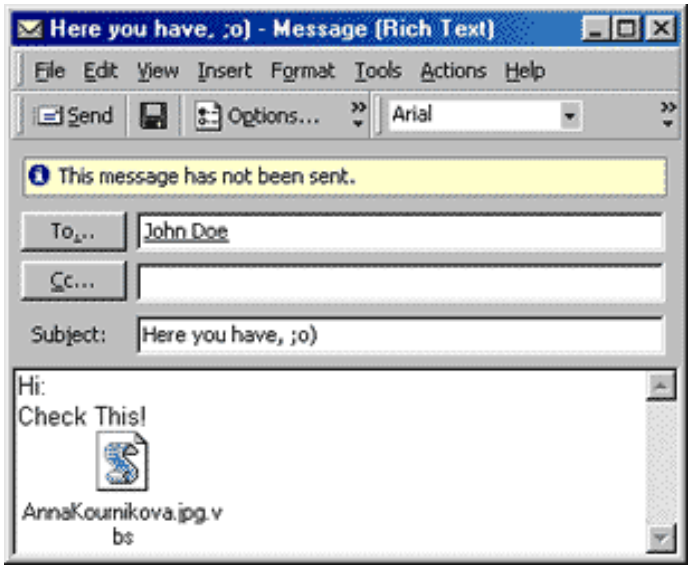
1999 - Melissa Virus



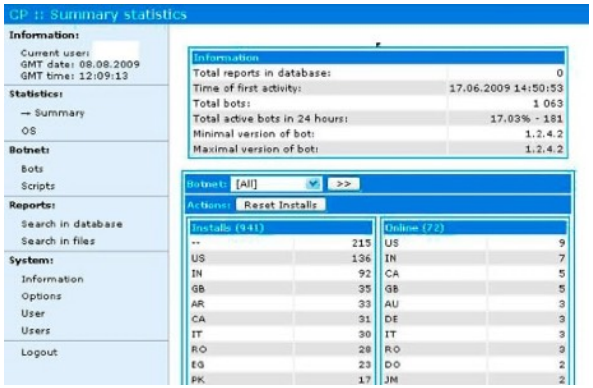




2000 – ILOVEYOU



2001 – Anna Kournikova



2010 - Stuxnet

2011 - Zeus

2017 - WannaCry

2019 - Emotet/Trickbot/Ryuk

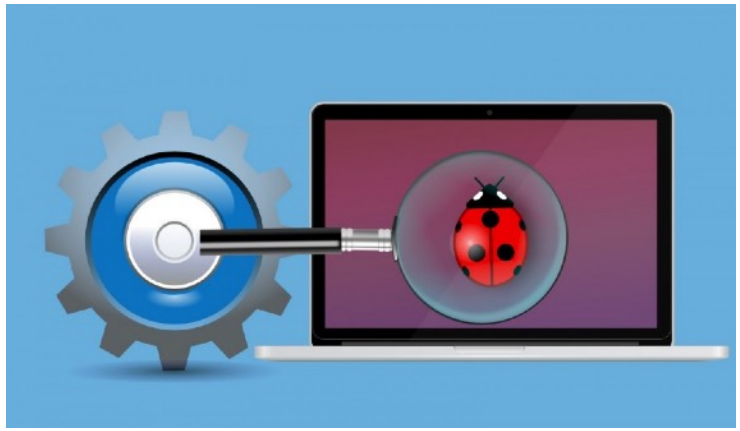
Evolución de soluciones anti-malware

sedian Seguridad Digital de Andalucía

- 1982 – Reaper (para eliminar Creeper)
- 1987 – Bernt Fix (para eliminar Vienna)
- 1987 – G Data Software AG (considerado primer antivirus)
- 1987 – McAfee
- 1987 – NOD32
- 1987 – FlushShot (primeras aproximaciones heurísticas)
- 1987 – Anti4us (primeras aproximaciones heurísticas)

Las primeras soluciones se enfocaban al análisis estático (enfocado a previa ejecución de ficheros):

- Firmas/hashes
- Heurística



Las soluciones van evolucionando hacia un análisis dinámico de comportamiento (no sólo de ejecución de ficheros):

- Sandbox
- Análisis de comportamiento
- Registro de actividades

Definición de EDR y sus funcionalidades

Las soluciones EDR (Endpoint Detection and Response) registran y almacenan comportamientos a nivel de Endpoint, usando técnicas de analítica de datos para detectar comportamientos sospechosos, proporcionando información contextual, bloqueando la actividad maliciosa y proporcionando recomendaciones de remediación para la restauración de los sistemas afectados.

Definición de EDR y sus funcionalidades

Las soluciones EDR se enmarcan dentro de las EPP (Endpoint Protection Platforms) – Definición de Gartner.

Capacidades:

- **Detección** de incidentes de seguridad.
- **Contención** de incidentes desde el endpoint.
- **Investigación** de incidentes de seguridad.
- Proporcionar guías de **remediación.**

Principales diferencias de EDR frente a otras soluciones anti-malware

sedian Seguridad Digital de Andalucía

EDR vs Antivirus

- EDR asume que has sido ciberatacado/Antivirus se centra en la prevención.
- EDR registra los eventos para posterior investigación de incidentes.
- EDR se centra en el comportamiento (dinámico)/Antivirus se centra en el análisis estático (firmas/heurística).

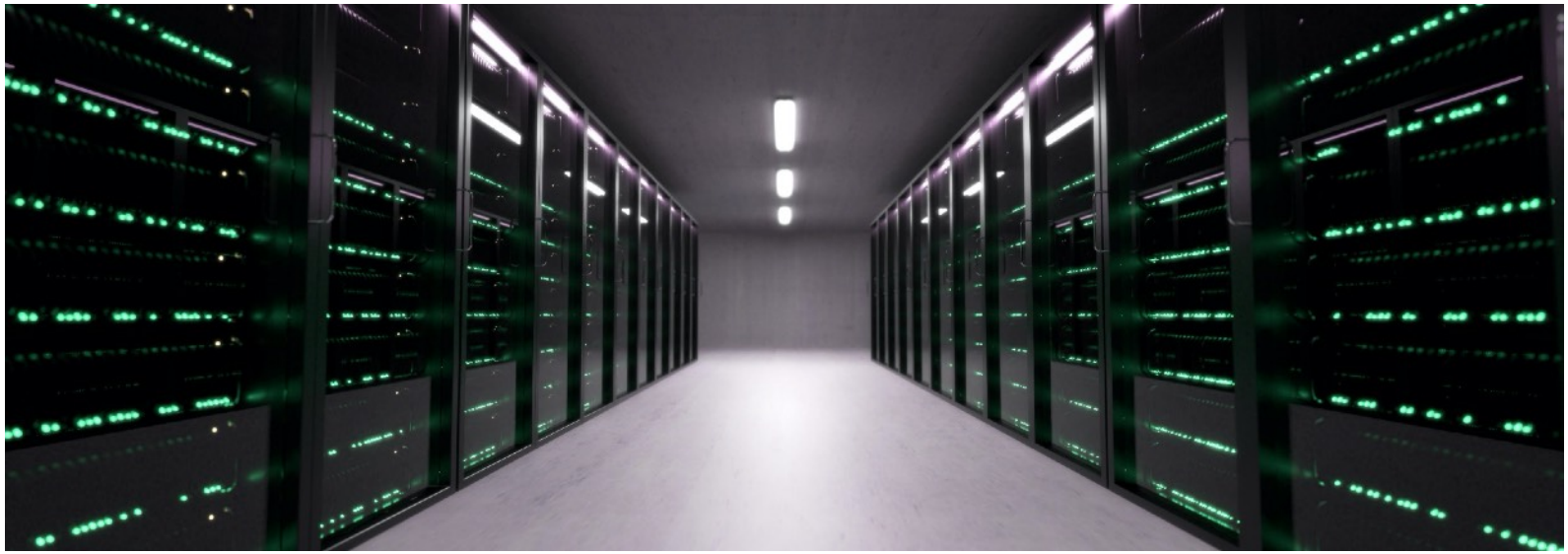
Antivirus vs NGAV (Next Generation Antivirus)

- NGAV es un Antivirus con algunas capacidades extra como detección de exploits o protección de ataques fileless.

Principales diferencias de EDR frente a otras soluciones anti-malware

Tipo de despliegue de la solución

- Instalación de agente con monitorización desde consola.
- Cloud u on-premise.
- Appliance físico/virtual.



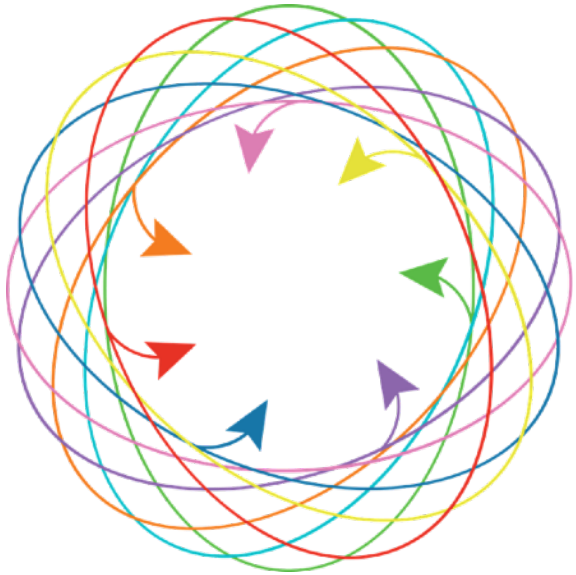
Estado actual del mercado

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

Posibilidades de ampliación de funcionalidad con otras soluciones

- SIEM: Security Information and Event Management.
- IDS/IPS: Intrusion Detection/ Prevention System.
- Threat Intelligence.

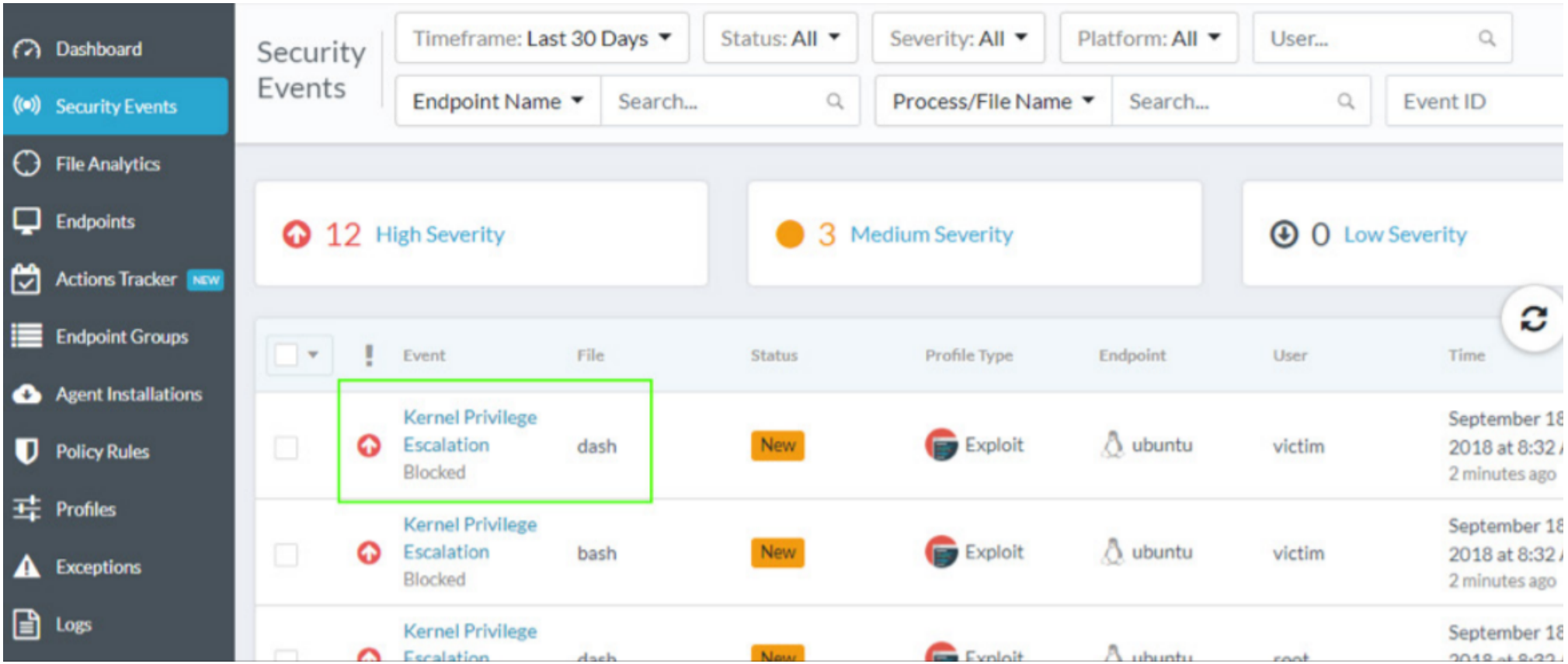


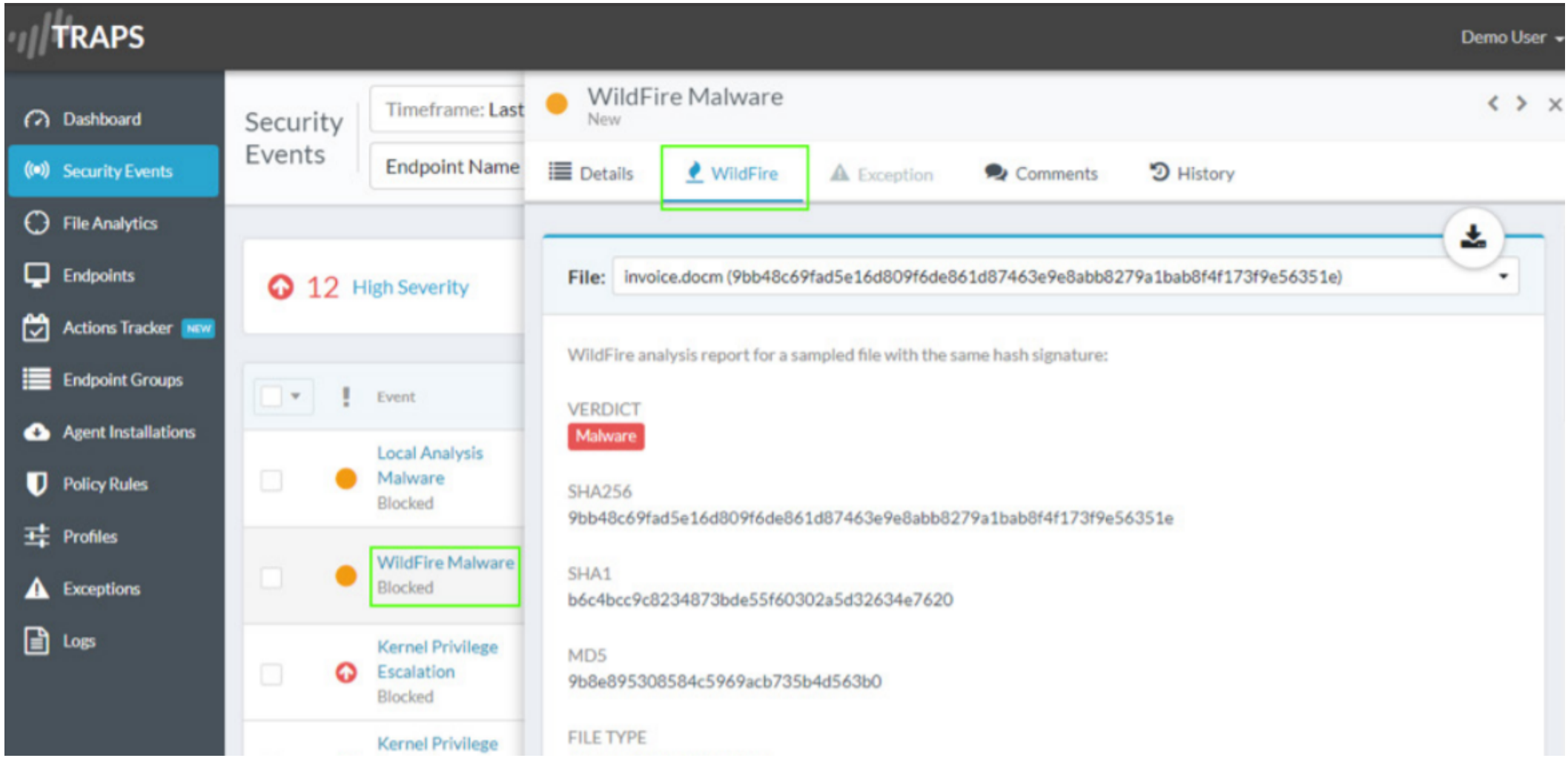
Posibilidad de ampliación de funcionalidad con otras soluciones

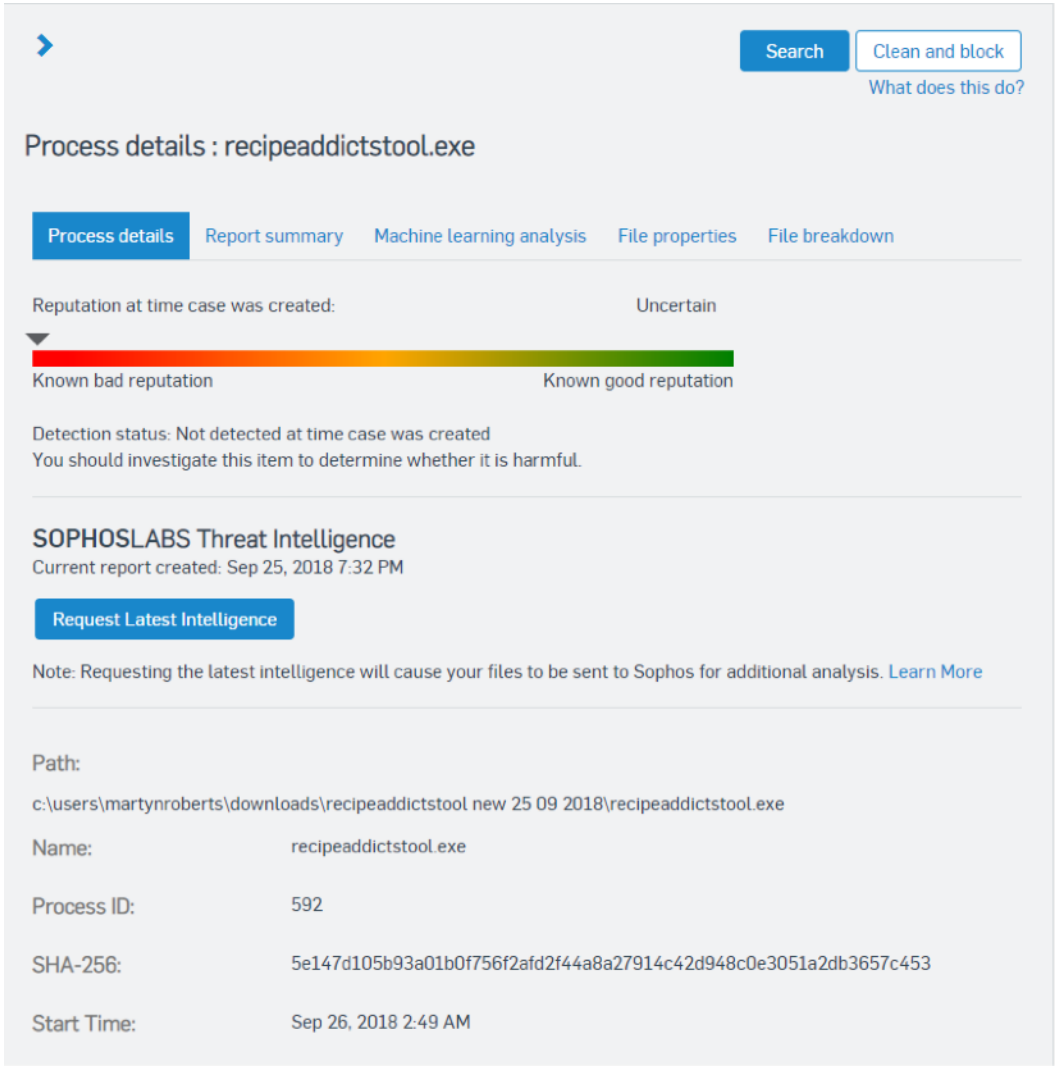
Aplicaciones prácticas de EDR

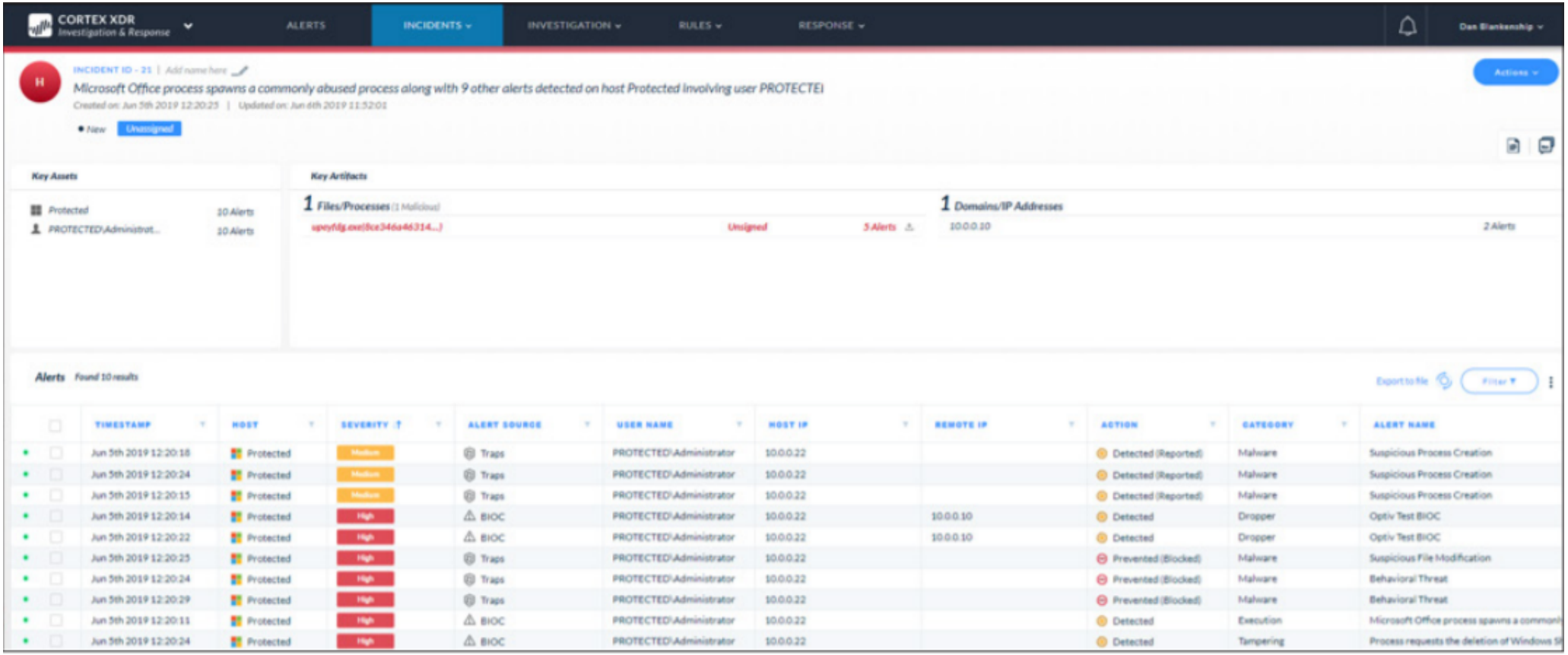
Consejos para seleccionar EDR:

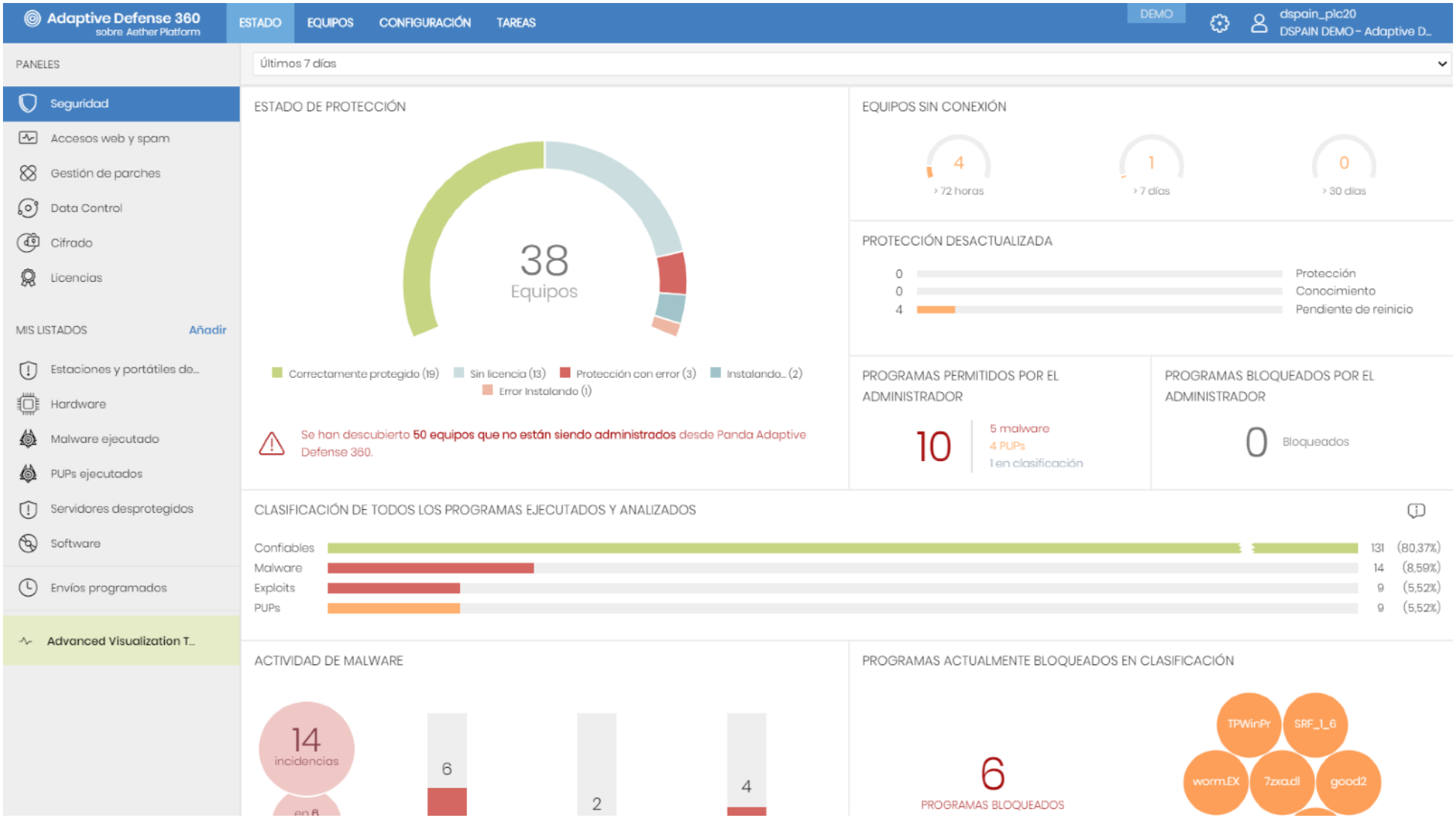
- ¿Puede la solución proteger las vulnerabilidades de los endpoints cuando los sistemas no están parcheados?
- ¿Puede la solución identificar los ficheros maliciosos sin actualizarse diariamente?
- ¿Cómo la solución detecta y protege frente a movimiento lateral?
- ¿Cómo gestiona la solución la remediación tras un incidente?
- ¿Qué tácticas, técnicas y procedimientos utilizan los atacantes y cómo la solución mejora la seguridad de la organización?

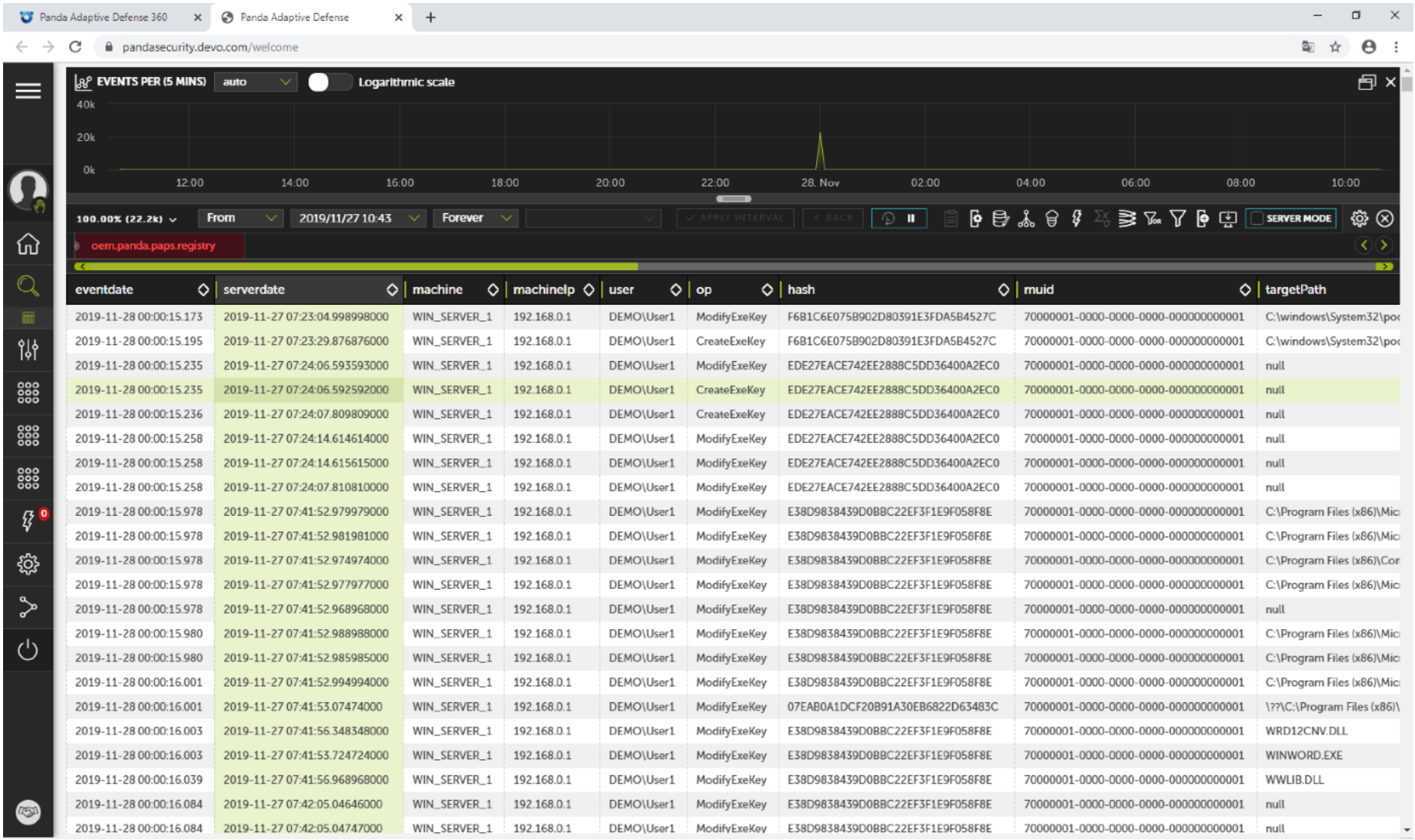

Dashboard
Security Events
File Analytics
Endpoints
Actions Tracker
NEW
Endpoint Groups
Agent Installations
Policy Rules
Profiles
Exceptions
Logs
Security Events
Timeframe: Last 30 Days
Status: All
Severity: All
Platform: All
User...
Endpoint Name
Search...
Process/File Name
Search...
Event ID
12 High Severity
3 Medium Severity
0 Low Severity
Event
File
Status
Profile Type
Endpoint
User
Time
Kernel Privilege Escalation
Blocked
dash
New
Exploit
ubuntu
victim
September 18
2018 at 8:32
2 minutes ago
Kernel Privilege Escalation
Blocked
bash
New
Exploit
ubuntu
victim
September 18
2018 at 8:32
2 minutes ago
Kernel Privilege


TRAPS
Demo User
Dashboard
Security Events
File Analytics
Endpoints
Actions Tracker
NEW
Endpoint Groups
Agent Installations
Policy Rules
Profiles
Exceptions
Logs
Security Events
Timeframe: Last
Endpoint Name
12 High Severity
Event
Local Analysis Malware Blocked
WildFire Malware Blocked
Kernel Privilege Escalation Blocked
Kernel Privilege
WildFire Malware
New
Details
WildFire
Exception
Comments
History
File: invoice.docm (9bb48c69fad5e16d809f6de861d87463e9e8abb8279a1bab8f4f173f9e56351e)
WildFire analysis report for a sampled file with the same hash signature:
VERDICT
Malware
SHA256
9bb48c69fad5e16d809f6de861d87463e9e8abb8279a1bab8f4f173f9e56351e
SHA1
b6c4bcc9c8234873bde55f60302a5d32634e7620
MD5
9b8e895308584c5969acb735b4d563b0
FILE TYPE

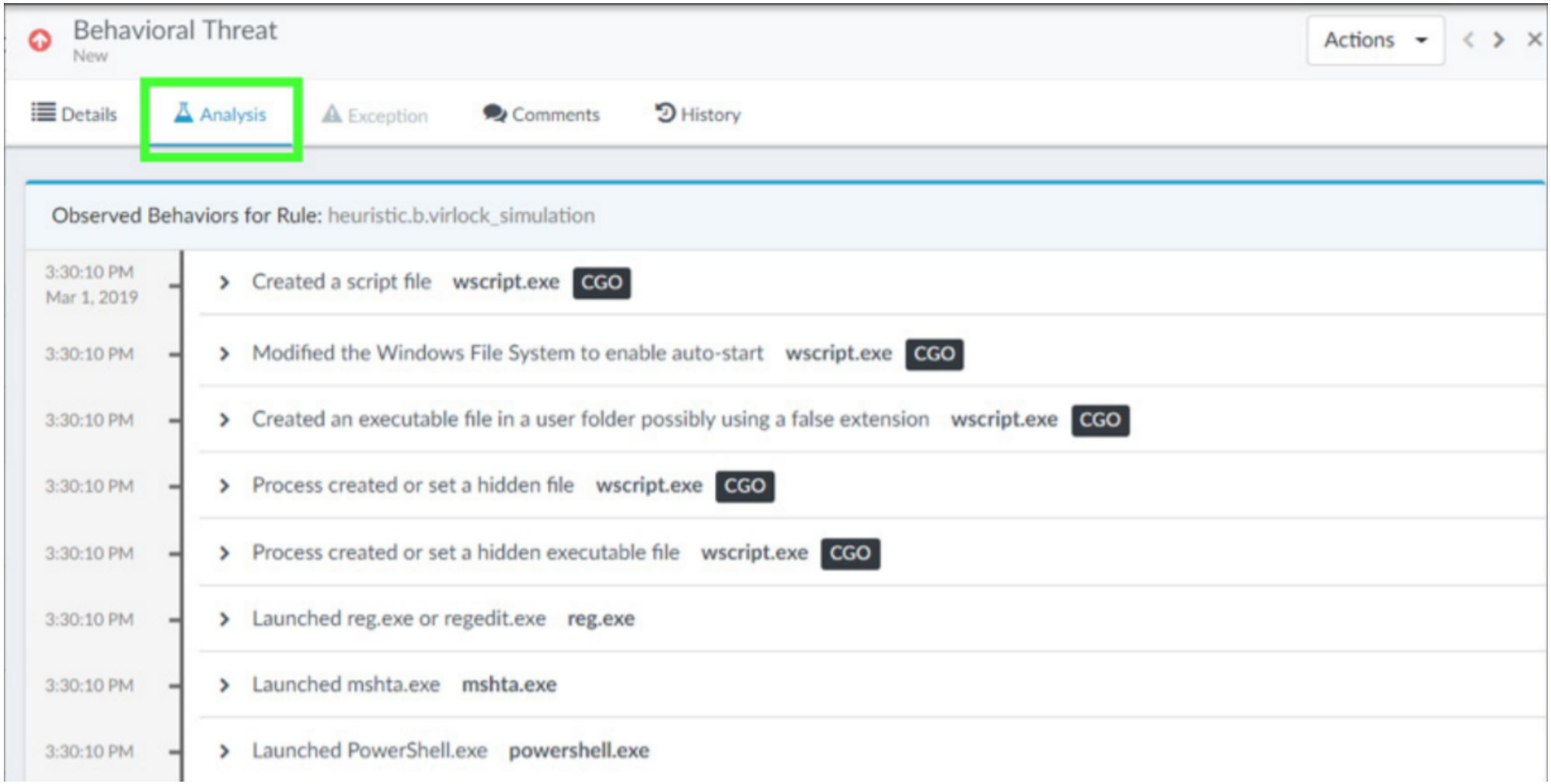

Search
Clean and block
What does this do?
Process details : recipeaddictstool.exe
Process details
Report summary
Machine learning analysis
File properties
File breakdown
Reputation at time case was created:
Uncertain
Known bad reputation
Known good reputation
Detection status: Not detected at time case was created
You should investigate this item to determine whether it is harmful.
SOPHOSLABS Threat Intelligence
Current report created: Sep 25, 2018 7:32 PM
Request Latest Intelligence
Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. Learn More
Path:
c:\users\martynroberts\downloads\recipeaddictstool new 25 09 2018\recipeaddictstool.exe
Name: recipeaddictstool.exe
Process ID: 592
SHA-256: 5e147d105b93a01b0f756f2afd2f44a8a27914c42d948c0e3051a2db3657c453
Start Time: Sep 26, 2018 2:49 AM

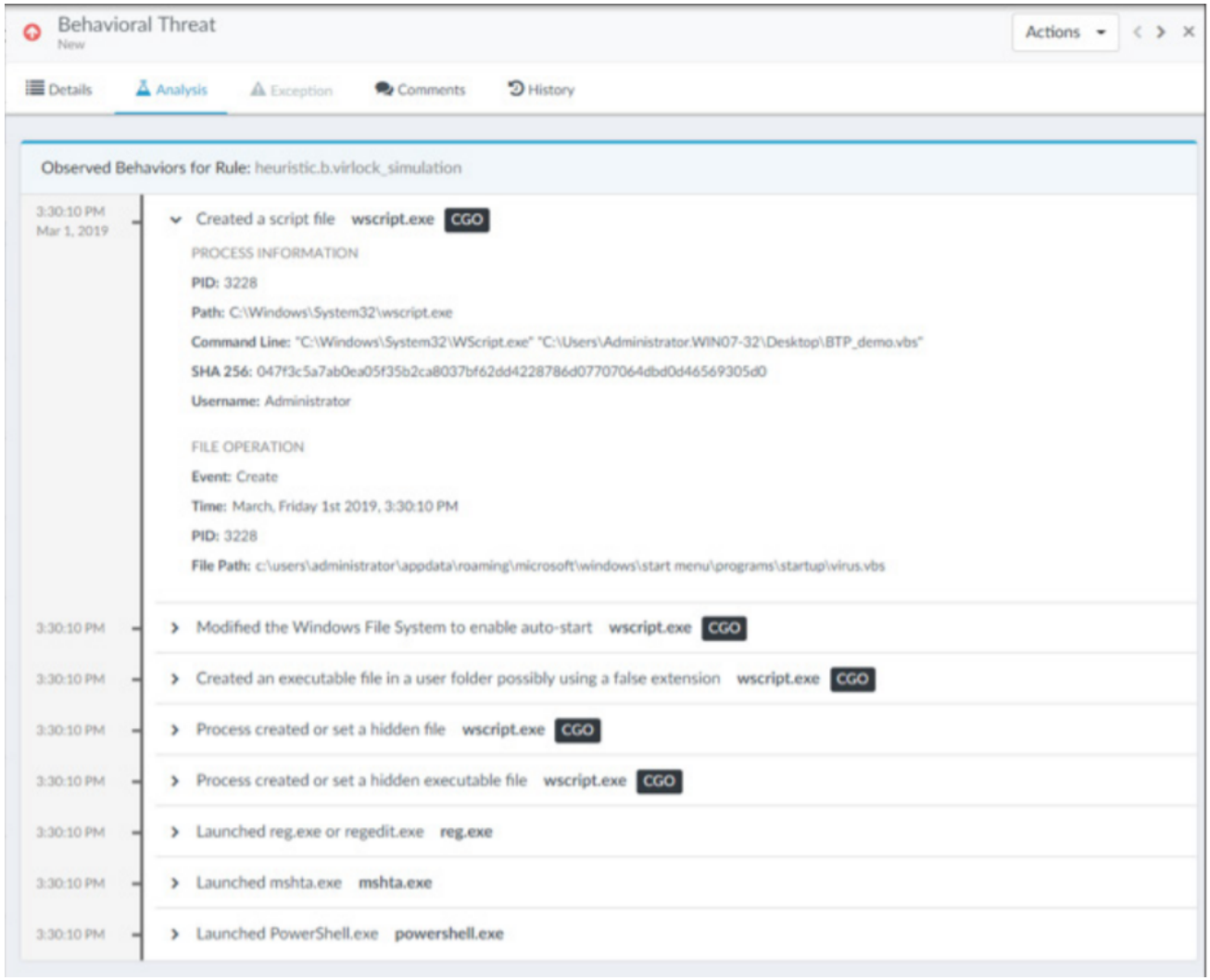

CORTEX XDR
Investigation & Response
ALERTS
INCIDENTS
INVESTIGATION
RULES
RESPONSE
Microsoft Office process spawns a commonly abused process along with 9 other alerts detected on host Protected Involving user PROTECTEI
Key Assets
Protected
10 Alerts
Key Artifacts
1 Files/Processes
1 Domains/IP Addresses
Unsigned
5 Alerts
10.0.0.10
2 Alerts
Alerts
Found 10 results
TIMESTAMP
HOST
SEVERITY
ALERT SOURCE
USER NAME
HOST IP
REMOTE IP
ACTION
CATEGORY
ALERT NAME
Jun 5th 2019 12:20:18 Protected Traps PROTECTED\Administrator 10.0.0.22 Detected (Reported) Malware Suspicious Process Creation
Jun 5th 2019 12:20:24 Protected Traps PROTECTED\Administrator 10.0.0.22 Detected (Reported) Malware Suspicious Process Creation
Jun 5th 2019 12:20:15 Protected Traps PROTECTED\Administrator 10.0.0.22 Detected (Reported) Malware Suspicious Process Creation
Jun 5th 2019 12:20:14 Protected BIOC PROTECTED\Administrator 10.0.0.22 10.0.0.10 Detected Dropper Optiv Test BIOC
Jun 5th 2019 12:20:22 Protected BIOC PROTECTED\Administrator 10.0.0.22 10.0.0.10 Detected Dropper Optiv Test BIOC
Jun 5th 2019 12:20:25 Protected Traps PROTECTED\Administrator 10.0.0.22 Prevented (Blocked) Malware Suspicious File Modification
Jun 5th 2019 12:20:24 Protected Traps PROTECTED\Administrator 10.0.0.22 Prevented (Blocked) Malware Behavioral Threat
Jun 5th 2019 12:20:29 Protected Traps PROTECTED\Administrator 10.0.0.22 Prevented (Blocked) Malware Behavioral Threat
Jun 5th 2019 12:20:11 Protected BIOC PROTECTED\Administrator 10.0.0.22 Detected Execution
Jun 5th 2019 12:20:24 Protected BIOC PROTECTED\Administrator 10.0.0.22 Detected Tampering

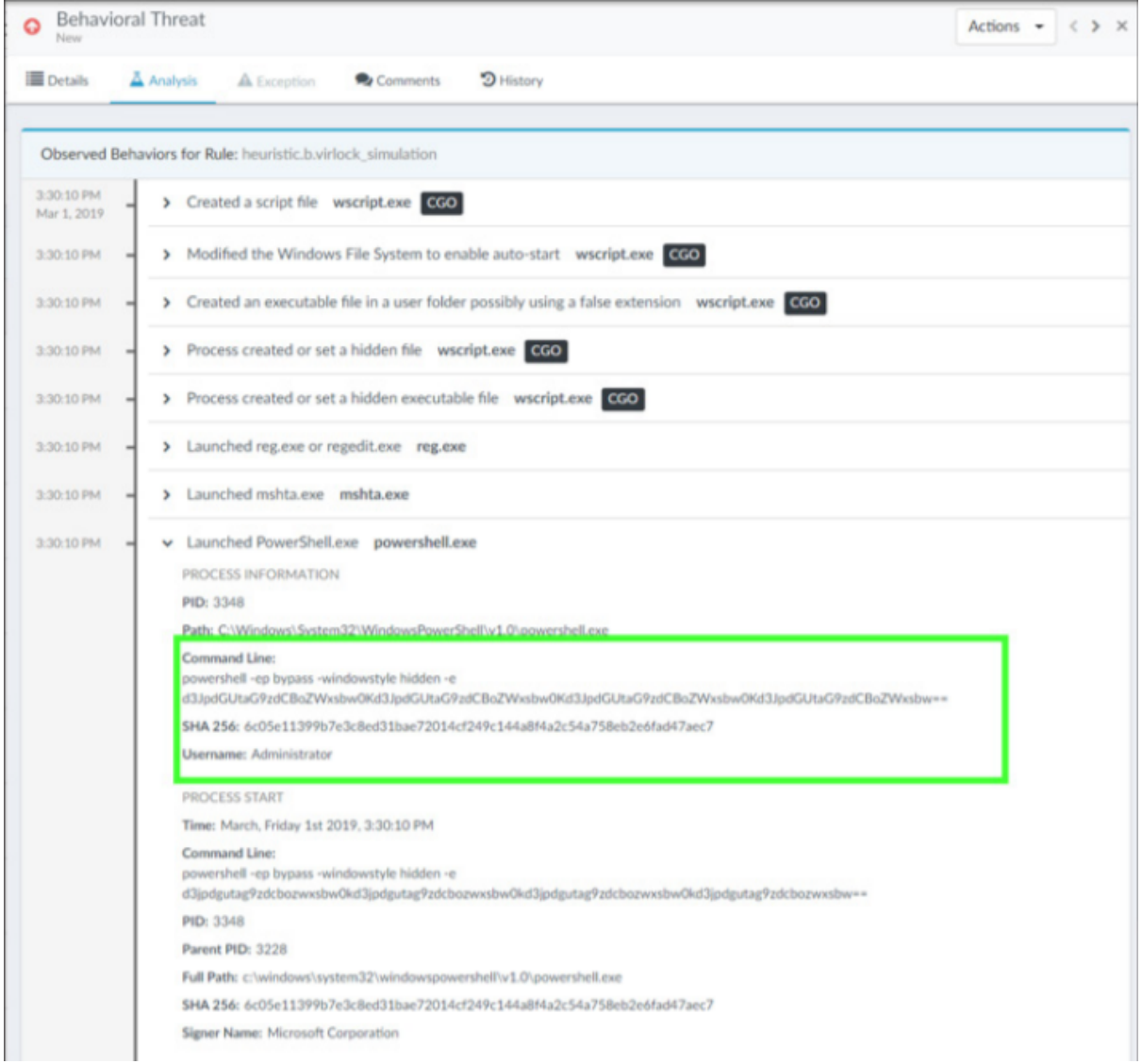

Adaptive Defense 360
sobre Aether Platform
ESTADO
EQUIPOS
CONFIGURACIÓN
TAREAS
DEMO
dspain_plc20
DSPAIN DEMO - Adaptive D...
PANELES
Últimos 7 días
Seguridad
Accesos web y spam
Gestión de parches
Data Control
Cifrado
Licencias
MIS LISTADOS
Añadir
Estaciones y portátiles de...
Hardware
Malware ejecutado
PUPs ejecutados
Servidores desprotegidos
Software
Envíos programados
Advanced Visualization T...
ESTADO DE PROTECCIÓN
38
Equipos
Correctamente protegido (19)
Sin licencia (13)
Protección con error (3)
Instalando... (2)
Error instalando (1)
Se han descubierto 50 equipos que no están siendo administrados desde Panda Adaptive Defense 360.
EQUIPOS SIN CONEXIÓN
4
> 72 horas
1
> 7 días
0
> 30 días
PROTECCIÓN DESACTUALIZADA
0 Protección
0 Conocimiento
4 Pendiente de reinicio
PROGRAMAS PERMITIDOS POR EL ADMINISTRADOR
10
5 malware
4 PUPs
1 en clasificación
PROGRAMAS BLOQUEADOS POR EL ADMINISTRADOR
0
Bloqueados
CLASIFICACIÓN DE TODOS LOS PROGRAMAS EJECUTADOS Y ANALIZADOS
Confiables 131 (80,37%)
Malware 14 (8,59%)
Exploits 9 (5,52%)
PUPs 9 (5,52%)
ACTIVIDAD DE MALWARE
14
incidencias
6
2
4
PROGRAMAS ACTUALMENTE BLOQUEADOS EN CLASIFICACIÓN
6
PROGRAMAS BLOQUEADOS
TPWinPr
SRF_1_6
worm.EX
7zxa.dl
good2

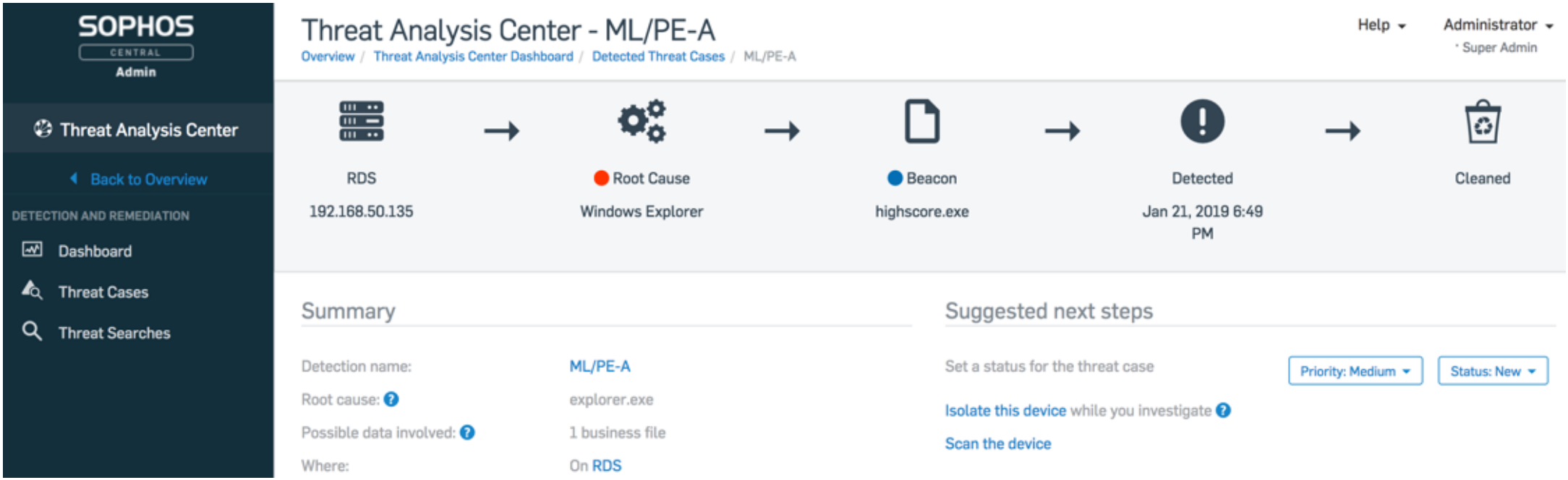


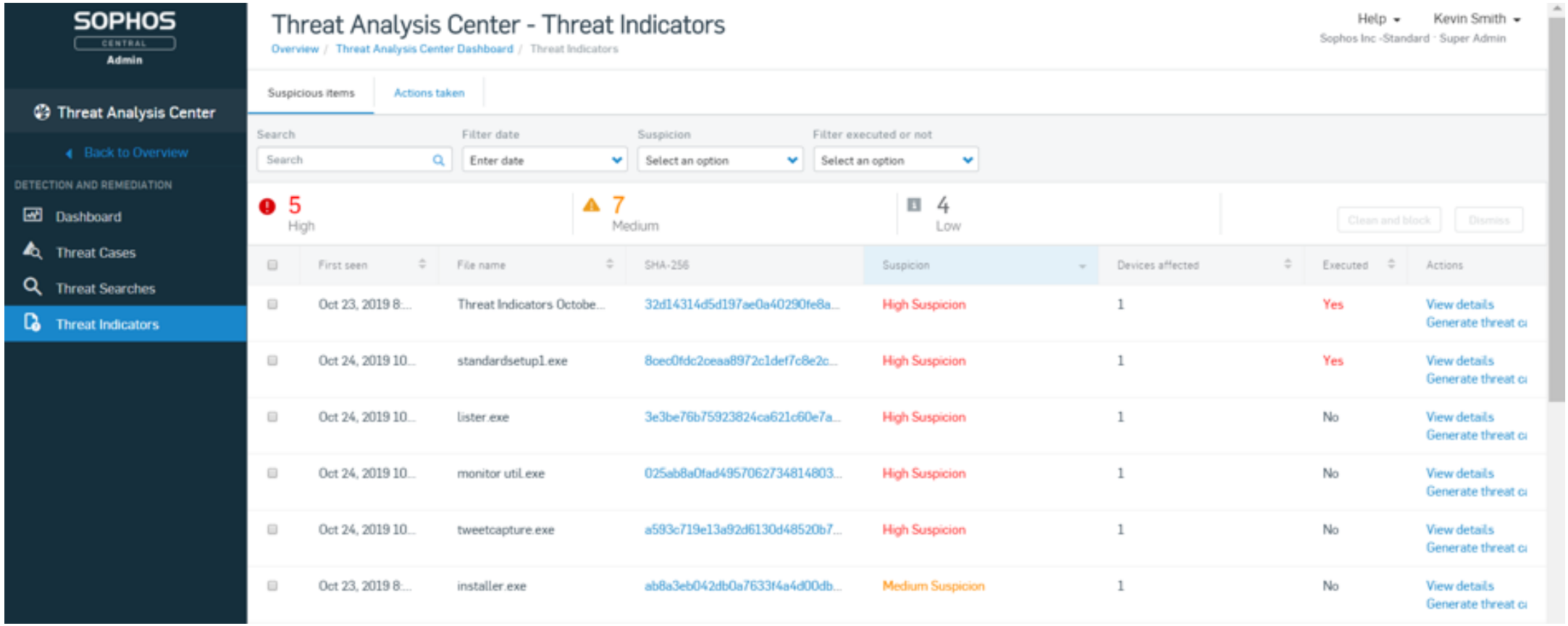
eventdate	serverdate	machine	machineIp	user	op	hash	muid	targetPath
2019-11-28 00:00:15.173	2019-11-27 07:23:04.998998000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	F6B1C6E075B902D80391E3FDA5B4527C	70000001-0000-0000-0000-000000000001	C:\windows\System32\poc
2019-11-28 00:00:15.195	2019-11-27 07:23:29.876876000	WIN_SERVER_1	192.168.0.1	DEMO\User1	CreateExeKey	F6B1C6E075B902D80391E3FDA5B4527C	70000001-0000-0000-0000-000000000001	C:\windows\System32\poc
2019-11-28 00:00:15.235	2019-11-27 07:24:06.593593000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	EDE27EACE742EE2888C5DD36400A2EC0	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:15.235	2019-11-27 07:24:06.592592000	WIN_SERVER_1	192.168.0.1	DEMO\User1	CreateExeKey	EDE27EACE742EE2888C5DD36400A2EC0	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:15.236	2019-11-27 07:24:07.809809000	WIN_SERVER_1	192.168.0.1	DEMO\User1	CreateExeKey	EDE27EACE742EE2888C5DD36400A2EC0	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:15.258	2019-11-27 07:24:14.614614000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	EDE27EACE742EE2888C5DD36400A2EC0	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:15.258	2019-11-27 07:24:14.615615000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	EDE27EACE742EE2888C5DD36400A2EC0	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:15.258	2019-11-27 07:24:07.810810000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	EDE27EACE742EE2888C5DD36400A2EC0	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:15.978	2019-11-27 07:41:52.979979000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	C:\Program Files (x86)\Mic
2019-11-28 00:00:15.978	2019-11-27 07:41:52.981981000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	C:\Program Files (x86)\Mic
2019-11-28 00:00:15.978	2019-11-27 07:41:52.974974000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	C:\Program Files (x86)\Cor
2019-11-28 00:00:15.978	2019-11-27 07:41:52.977977000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	C:\Program Files (x86)\Mic
2019-11-28 00:00:15.978	2019-11-27 07:41:52.968968000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:15.980	2019-11-27 07:41:52.988988000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	C:\Program Files (x86)\Mic
2019-11-28 00:00:15.980	2019-11-27 07:41:52.985985000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	C:\Program Files (x86)\Mic
2019-11-28 00:00:16.001	2019-11-27 07:41:52.994994000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	C:\Program Files (x86)\Mic
2019-11-28 00:00:16.001	2019-11-27 07:41:53.07474000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	07EAB0A1DCF20B91A30EB6822D63483C	70000001-0000-0000-0000-000000000001	\??\C:\Program Files (x86)\
2019-11-28 00:00:16.003	2019-11-27 07:41:56.348348000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	WRD12CNV.DLL
2019-11-28 00:00:16.003	2019-11-27 07:41:53.724724000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	WINWORD.EXE
2019-11-28 00:00:16.039	2019-11-27 07:41:56.968968000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	WWLIB.DLL
2019-11-28 00:00:16.084	2019-11-27 07:42:05.04646000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	null
2019-11-28 00:00:16.084	2019-11-27 07:42:05.04747000	WIN_SERVER_1	192.168.0.1	DEMO\User1	ModifyExeKey	E38D9838439D0BBC22EF3F1E9F058F8E	70000001-0000-0000-0000-000000000001	null


Behavioral Threat
New
Actions
Details
Analysis
Exception
Comments
History
Observed Behaviors for Rule: heuristic.b.virlock_simulation
3:30:10 PM Mar 1, 2019
Created a script file wscript.exe CGO
3:30:10 PM
Modified the Windows File System to enable auto-start wscript.exe CGO
3:30:10 PM
Created an executable file in a user folder possibly using a false extension wscript.exe CGO
3:30:10 PM
Process created or set a hidden file wscript.exe CGO
3:30:10 PM
Process created or set a hidden executable file wscript.exe CGO
3:30:10 PM
Launched reg.exe or regedit.exe reg.exe
3:30:10 PM
Launched mshta.exe mshta.exe
3:30:10 PM
Launched PowerShell.exe powershell.exe


Behavioral Threat
New
Actions
Details
Analysis
Exception
Comments
History
Observed Behaviors for Rule: heuristic.b.virlock_simulation
3:30:10 PM
Mar 1, 2019
Created a script file wscript.exe CGO
PROCESS INFORMATION
PID: 3228
Path: C:\Windows\System32\wscript.exe
Command Line: "C:\Windows\System32\WScript.exe" "C:\Users\Administrator.WIN07-32\Desktop\BTP_demo.vbs"
SHA 256: 047f3c5a7ab0ea05f35b2ca8037bf62dd4228786d07707064dbd0d46569305d0
Username: Administrator
FILE OPERATION
Event: Create
Time: March, Friday 1st 2019, 3:30:10 PM
PID: 3228
File Path: c:\users\administrator\appdata\roaming\microsoft\windows\start menu\programs\startup\virus.vbs
3:30:10 PM
Modified the Windows File System to enable auto-start wscript.exe CGO
3:30:10 PM
Created an executable file in a user folder possibly using a false extension wscript.exe CGO
3:30:10 PM
Process created or set a hidden file wscript.exe CGO
3:30:10 PM
Process created or set a hidden executable file wscript.exe CGO
3:30:10 PM
Launched reg.exe or regedit.exe reg.exe
3:30:10 PM
Launched mshta.exe mshta.exe
3:30:10 PM
Launched PowerShell.exe powershell.exe

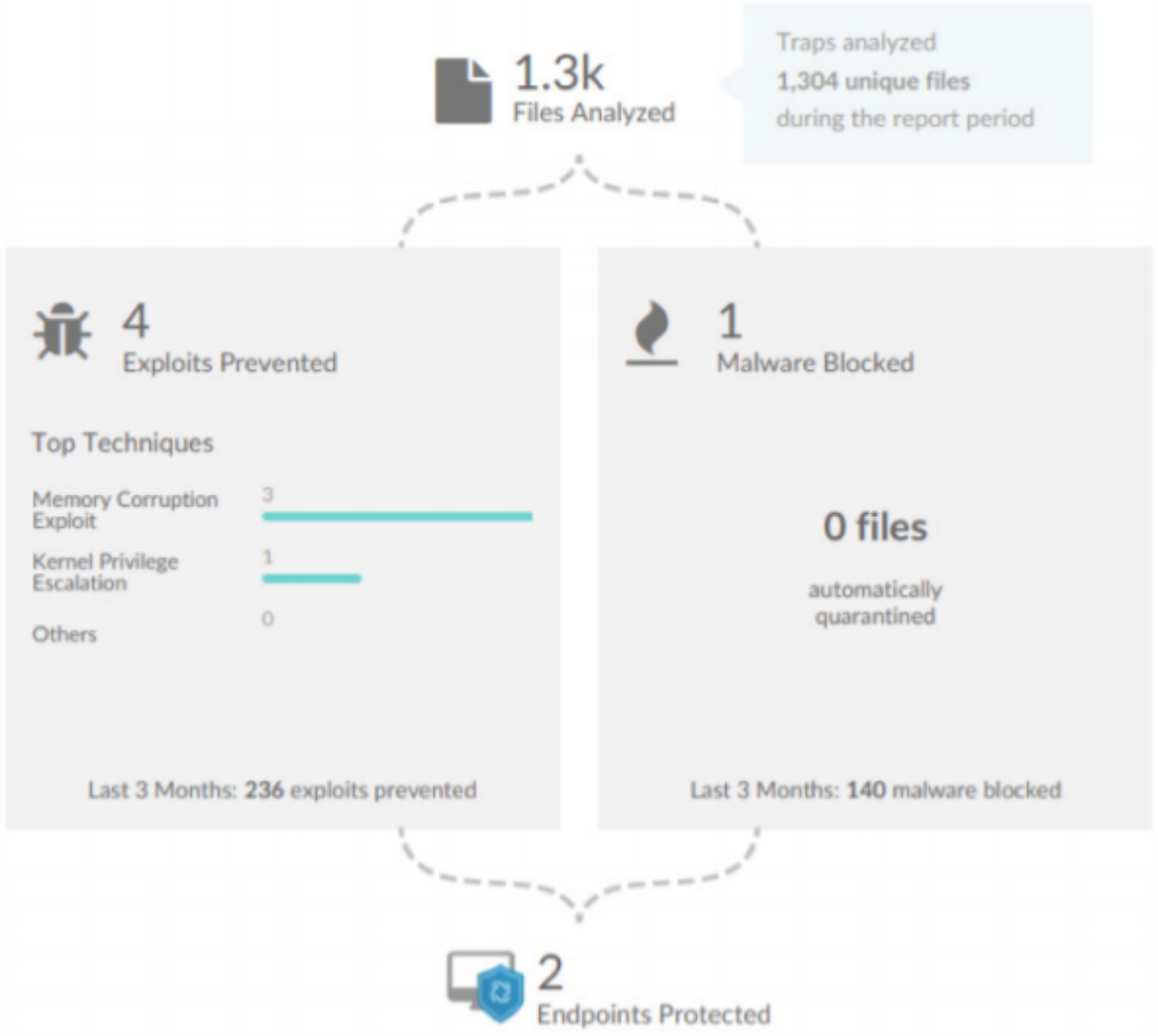

Behavioral Threat
New
Actions
Details
Analysis
Exception
Comments
History
Observed Behaviors for Rule: heuristic.b.virlock_simulation
3:30:10 PM Mar 1, 2019
Created a script file wscript.exe CGO
3:30:10 PM
Modified the Windows File System to enable auto-start wscript.exe CGO
3:30:10 PM
Created an executable file in a user folder possibly using a false extension wscript.exe CGO
3:30:10 PM
Process created or set a hidden file wscript.exe CGO
3:30:10 PM
Process created or set a hidden executable file wscript.exe CGO
3:30:10 PM
Launched reg.exe or regedit.exe reg.exe
3:30:10 PM
Launched mshta.exe mshta.exe
3:30:10 PM
Launched PowerShell.exe powershell.exe
PROCESS INFORMATION
PID: 3348
Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command Line:
powershell -ep bypass -windowstyle hidden -e
d3JpdGUtaG9zdCBoZWxsbw0Kd3JpdGUtaG9zdCBoZWxsbw0Kd3JpdGUtaG9zdCBoZWxsbw0Kd3JpdGUtaG9zdCBoZWxsbw==
SHA 256: 6c05e11399b7e3c8ed31bae72014cf249c144a8f4a2c54a758eb2e6fad47aec7
Username: Administrator
PROCESS START
Time: March, Friday 1st 2019, 3:30:10 PM
Command Line:
powershell -ep bypass -windowstyle hidden -e
d3jpdgutag9zdcbozwxsbw0kd3jpdgutag9zdcbozwxsbw0kd3jpdgutag9zdcbozwxsbw0kd3jpdgutag9zdcbozwxsbw==
PID: 3348
Parent PID: 3228
Full Path: c:\windows\system32\windowspowershell\v1.0\powershell.exe
SHA 256: 6c05e11399b7e3c8ed31bae72014cf249c144a8f4a2c54a758eb2e6fad47aec7
Signer Name: Microsoft Corporation


SOPHOS
CENTRAL
Admin
Threat Analysis Center
Back to Overview
DETECTION AND REMEDIATION
Dashboard
Threat Cases
Threat Searches
Threat Analysis Center - ML/PE-A
Overview / Threat Analysis Center Dashboard / Detected Threat Cases / ML/PE-A
Help
Administrator
Super Admin
RDS
192.168.50.135
Root Cause
Windows Explorer
Beacon
highscore.exe
Detected
Jan 21, 2019 6:49 PM
Cleaned
Summary
Detection name: ML/PE-A
Root cause: explorer.exe
Possible data involved: 1 business file
Where: On RDS
Suggested next steps
Set a status for the threat case
Priority: Medium
Status: New
Isolate this device while you investigate
Scan the device



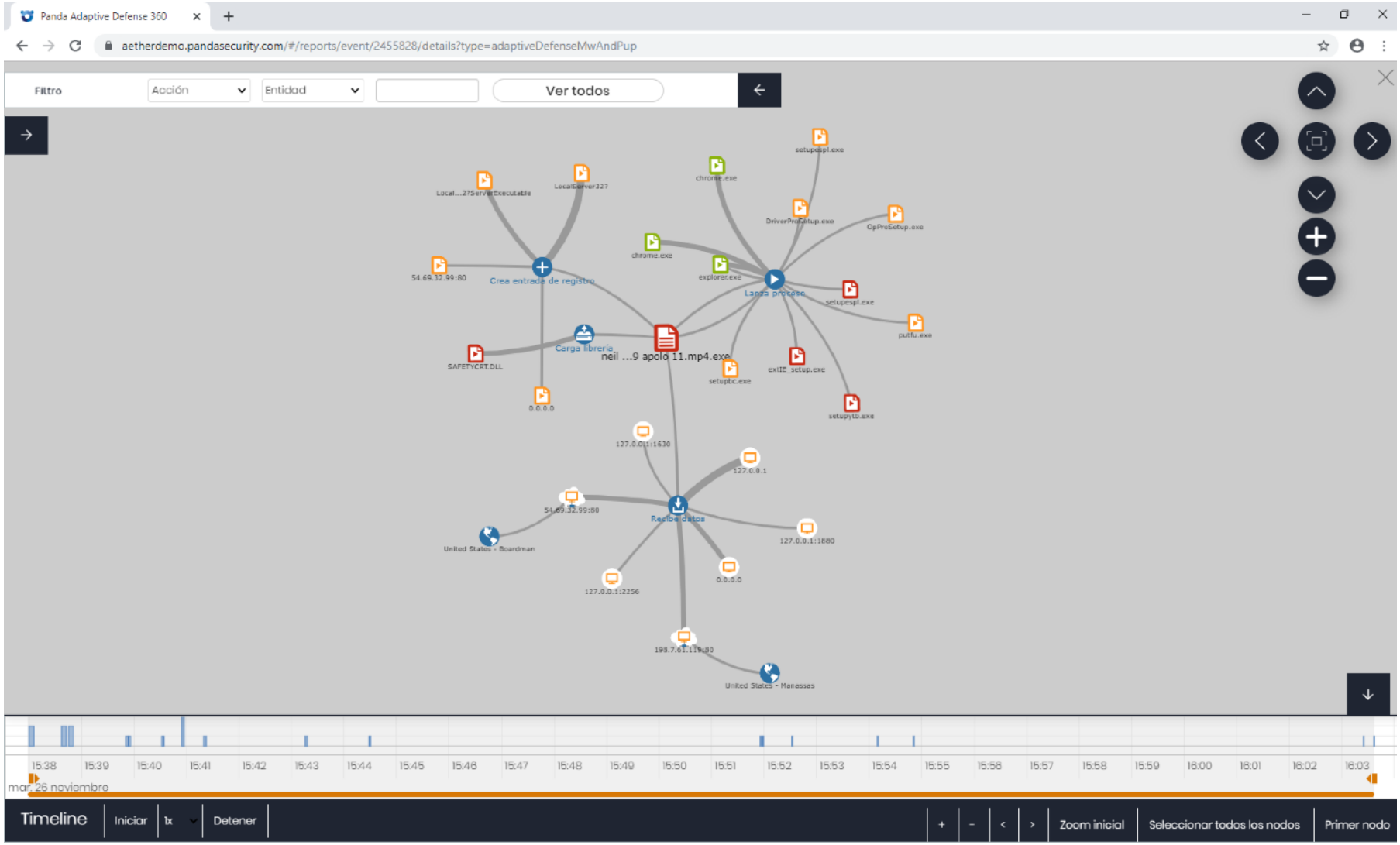
sedian Seguridad Digital de Andalucía

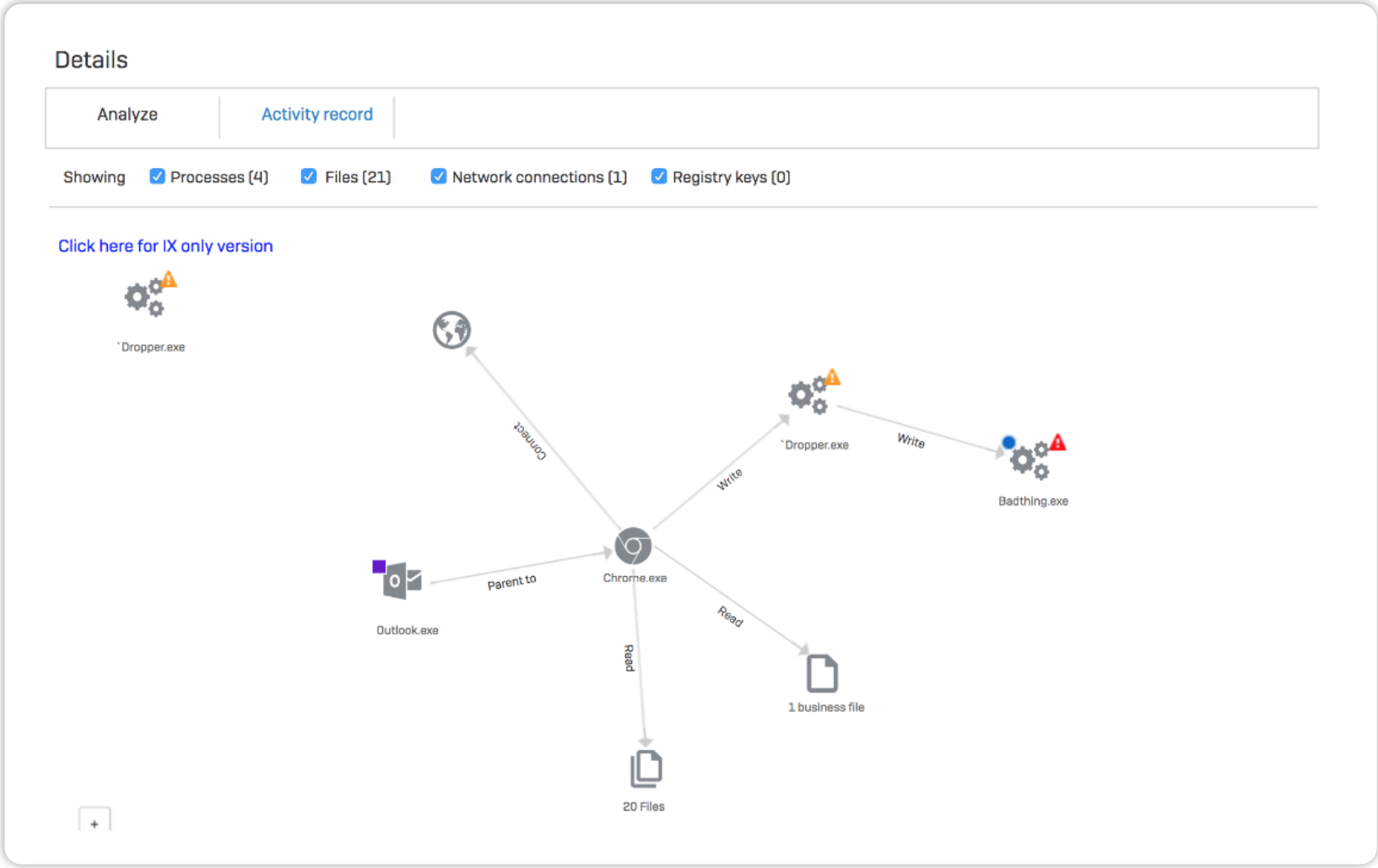
Aplicaciones prácticas de EDR


1.3k
Files Analyzed
Traps analyzed
1,304 unique files
during the report period
4
Exploits Prevented
Top Techniques
Memory Corruption Exploit
3
Kernel Privilege Escalation
1
Others
0
Last 3 Months: 236 exploits prevented
1
Malware Blocked
0 files
automatically quarantined
Last 3 Months: 140 malware blocked
2
Endpoints Protected

sedian Seguridad Digital de Andalucía

Aplicaciones prácticas de EDR


Panda Adaptive Defense 360
aetherdemo.pandasecurity.com/#/reports/event/2455828/details?type=adaptiveDefenseMwAndPup
Filtro
Acción
Entidad
Ver todos
Crea entrada de registro
Carga librería
neil ...9 apolo 11.mp4.exe
Lanza proceso
Recibe datos
SAFETYCRT.DLL
United States - Boardman
United States - Manassas
15:38
15:39
15:40
15:41
15:42
15:43
15:44
15:45
15:46
15:47
15:48
15:49
15:50
15:51
15:52
15:53
15:54
15:55
15:56
15:57
15:58
15:59
16:00
16:01
16:02
16:03
mar 26 noviembre
Timeline
Iniciar
1x
Detener
Zoom inicial
Seleccionar todos los nodos
Primer nodo


Details
Analyze
Activity record
Showing
Processes (4)
Files (21)
Network connections (1)
Registry keys (0)
Click here for IX only version
`Dropper.exe
Connect
Write
`Dropper.exe
Write
Badthing.exe
Outlook.exe
Parent to
Chrome.exe
Read
Read
1 business file
20 Files

sedian Seguridad Digital de Andalucía