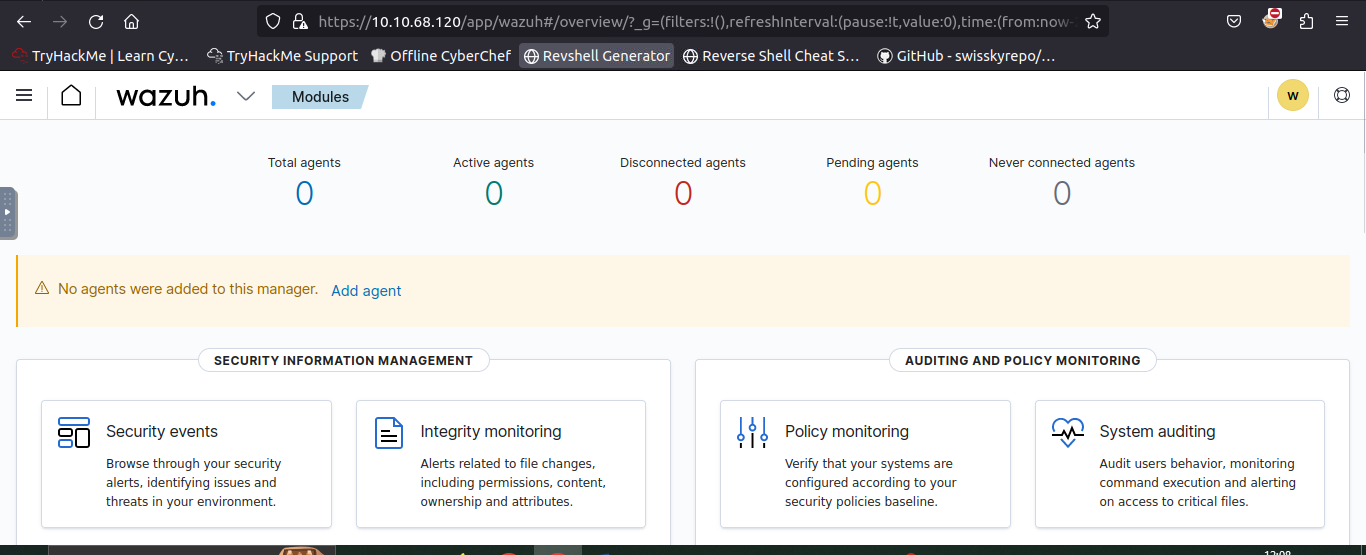
Wazuh

Dashboard



Sysmon log file for the rule set

\*\*Phase 1: Completed pre-decoding.

full event: Mar 29 13:36:36 WinEvtLog: Microsoft-Windows-Sysmon/Operational: INFORMATION(1): Microsoft-Windows-Sysmon: SYSTEM: NT AUTHORITY: WIN-P57C9KN929H: Process Create: UtcTime: 2017-03-29 11:36:36.964 ProcessGuid: {DB577E3B-9C44-58DB-0000-0010B0983A00} ProcessId: 3784 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-file" "C:\Users\Alberto\Desktop\test.ps1" CurrentDirectory: C:\Users\Alberto\Desktop\ User: WIN-P57C9KN929H\Alberto LogonGuid: {DB577E3B-89E5-58DB-0000-0020CB290500} LogonId: 0x529cb TerminalSessionId: 1 IntegrityLevel: Medium Hashes: MD5=92F44E405DB16AC55D97E3BFE3B132FA,SHA256=6C05E11399B7E3C8ED31BAE72014CF249C144A8F4A2C54A758EB2E6FAD47AEC7 ParentProcessGuid: {DB577E3B-89E6-58DB-0000-0010FA3B0500} ParentProcessId: 2308 ParentImage: C:\Windows\explorer.exe ParentCommandLine: C:\Windows\Explorer.EXE

timestamp: Mar 29 13:36:36

hostname: WinEvtLog:

program\_name: WinEvtLog

\*\*Phase 2: Completed decoding.

name: windows

parent: windows

data: {

"srcuser": "WIN-P57C9KN929H\\Alberto",

"id": "1",

"sysmon": {

"processGuid": "{DB577E3B-9C44-58DB-0000-0010B0983A00 }",

"processId": "3784",

"image": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",

"commandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \"-file\" \"C:\\Users\\Alberto\\Desktop\\test.ps1\"",

"currentDirectory": "C:\\Users\\Alberto\\Desktop\\",

"logonGuid": "{DB577E3B-89E5-58DB-0000-0020CB290500}",

"logonId": "0x529cb",

"terminalSessionId": "1",

"integrityLevel": "Medium",

"hashes": "92F44E405DB16AC55D97E3BFE3B132FA,SHA256=6C05E11399B7E3C8ED31BAE72014CF249C144A8F4A2C54A758EB2E6FAD47AEC7",

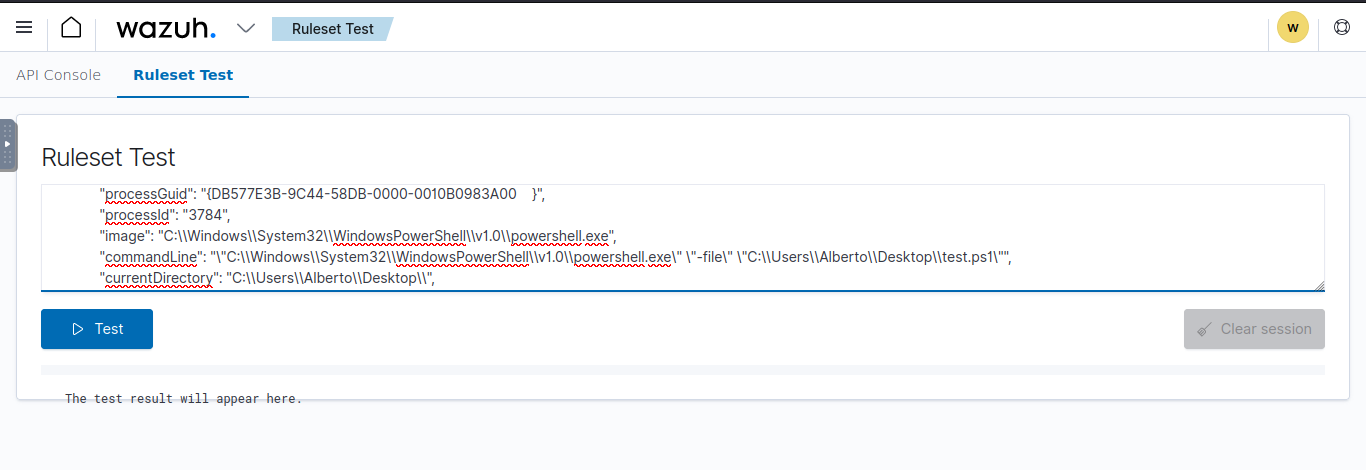
"parentProcessGuid": "{DB577E3B-89E6-58DB-0000-0010FA3B0500}",

"parentProcessId": "2308",

"parentImage": "C:\\Windows\\explorer.exe"

}

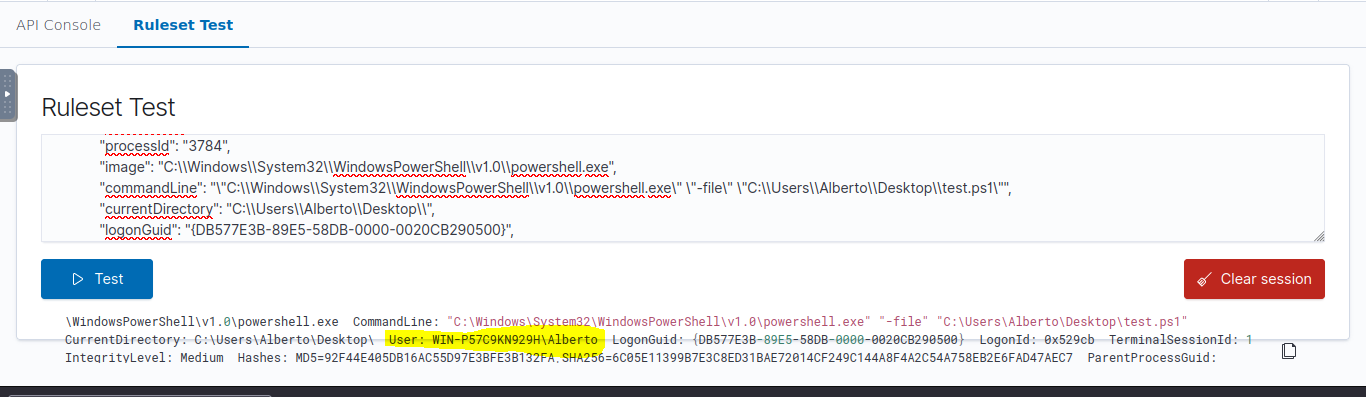
}



Phase 1 is the pre-decoding phase. The event log is parsed, and the header details like timestamp, hostname, and program\_name are retrieved. This is done automatically on the backend by Wazuh.

Phase 2 is the decoding phase, where the decoders do their magic. When done, all the extracted data from the declared decoder blocks are displayed here. For example, we can see in the results that the "id" field has been assigned the value of 1, which shows that the decoder works.

User details



Phase 3 shows what information an alert would contain when a rule is triggered, like "id", "level", "description", etc.

**\*\*Phase 3: Completed filtering (rules). id: 184665 level: - description: Sysmon - Event 1 groups: ["sysmon","sysmon\_event1"] firedtimes: 1 gdpr: "-" gpg13: "-" hipaa: "-" mail: "-" mitre.id: "-" mitre.technique: "-" nist\_800\_53: "-" pci\_dss: "-" tsc: "-"**

Output

\*\*Phase 1: Completed pre-decoding.

full event: '\*\*Phase 1: Completed pre-decoding. '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' full event: Mar 29 13:36:36 WinEvtLog: Microsoft-Windows-Sysmon/Operational: INFORMATION(1): Microsoft-Windows-Sysmon: SYSTEM: NT AUTHORITY: WIN-P57C9KN929H: Process Create: UtcTime: 2017-03-29 11:36:36.964 ProcessGuid: {DB577E3B-9C44-58DB-0000-0010B0983A00} ProcessId: 3784 Image: C:\Windows\System32\svchost.exe v1.0\powershell.exe CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-file" "C:\Users\Alberto\Desktop\test.ps1" CurrentDirectory: C:\Users\Alberto\Desktop\ User: WIN-P57C9KN929H\Alberto LogonGuid: {DB577E3B-89E5-58DB-0000-0020CB290500} LogonId: 0x529cb TerminalSessionId: 1 IntegrityLevel: Medium Hashes: MD5=92F44E405DB16AC55D97E3BFE3B132FA,SHA256=6C05E11399B7E3C8ED31BAE72014CF249C144A8F4A2C54A758EB2E6FAD47AEC7 ParentProcessGuid: {DB577E3B-89E6-58DB-0000-0010FA3B0500} ParentProcessId: 2308 ParentImage: C:\Windows\explorer.exe ParentCommandLine: C:\Windows\Explorer.EXE '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' timestamp: Mar 29 13:36:36 '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' hostname: WinEvtLog: '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' program\_name: WinEvtLog '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: '\*\*Phase 2: Completed decoding. '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' name: windows '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' parent: windows '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' data: {'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "srcuser": "WIN-P57C9KN929H\\Alberto",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "id": "1",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "sysmon": {'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "processGuid": "{DB577E3B-9C44-58DB-0000-0010B0983A00 }",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "processId": "3784",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "image": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "commandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \"-file\" \"C:\\Users\\Alberto\\Desktop\\test.ps1\"",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "currentDirectory": "C:\\Users\\Alberto\\Desktop\\",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "logonGuid": "{DB577E3B-89E5-58DB-0000-0020CB290500}",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "logonId": "0x529cb",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "terminalSessionId": "1",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "integrityLevel": "Medium",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "hashes": "92F44E405DB16AC55D97E3BFE3B132FA,SHA256=6C05E11399B7E3C8ED31BAE72014CF249C144A8F4A2C54A758EB2E6FAD47AEC7",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "parentProcessGuid": "{DB577E3B-89E6-58DB-0000-0010FA3B0500}",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "parentProcessId": "2308",'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' "parentImage": "C:\\Windows\\explorer.exe"'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' }'

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: '} '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: '\*\*Phase 3: Completed filtering (rules). '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' id: 184665 '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' level: - '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' description: Sysmon - Event 1 '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' groups: ["sysmon","sysmon\_event1"] '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' firedtimes: 1 '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' gdpr: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' gpg13: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' hipaa: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' mail: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' mitre.id: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' mitre.technique: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' nist\_800\_53: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' pci\_dss: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.

\*\*Phase 1: Completed pre-decoding.

full event: ' tsc: "-" '

\*\*Phase 2: Completed decoding.

No decoder matched.