2024-01-25 05:40:00.456 172.16.21.47
{"true":1706161198.55231,"timestamp":"2024-01-25T07:39:58.162+0200","rule":{"level"
:3,"description":"Software protection service scheduled
successfully.","id":"60642","firedtimes":2,"mail":true,"groups":["windows","windows
_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager"
:{"name":"wazuh"},"id":"1706161198.176054","decoder":{"name":"windows_eventchannel"
},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","provide
rGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software
Protection Platform
Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywo
rds":"0x80000000000000","systemTime":"2024-01-25T05:39:56.4838180Z","eventRecordID"
:"1533","processID":"4344","threadID":"0","channel":"Application","computer":"test-
pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software
Protection service for re-start at 2024-01-25T09:25:56Z. Reason:
RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:56Z,
RulesEngine"}}},"location":"EventChannel"}
2024-01-25 05:39:00.456 172.16.21.47
{"true":1706161136.546787,"timestamp":"2024-01-25T07:38:56.522+0200","rule":{"level
":3,"description":"Software protection service scheduled
successfully.","id":"60642","firedtimes":1,"mail":true,"groups":["windows","windows
_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager"
:{"name":"wazuh"},"id":"1706161136.174463","decoder":{"name":"windows_eventchannel"
},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","provide
rGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software
Protection Platform
Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywo
rds":"0x80000000000000","systemTime":"2024-01-25T05:38:54.8443373Z","eventRecordID"
:"1531","processID":"3048","threadID":"0","channel":"Application","computer":"test-
pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software
Protection service for re-start at 2024-01-25T09:25:54Z. Reason:
RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:54Z,
RulesEngine"}}},"location":"EventChannel"}
2024-01-25 05:38:30.458 172.16.21.47
{"true":1706161107.544337,"timestamp":"2024-01-25T07:38:27.448+0200","rule":{"level
":3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":1,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706161107.167117","decoder":{"name":"windows_eventchannel"},"data":{"wi
n":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"
{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0",
"task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-2
5T05:38:24.7547881Z","eventRecordID":"18079","processID":"1224","threadID":"7080","
channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":
"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon

Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 05:18:50.456 172.16.21.47 {"true":1706159928.44431,"timestamp":"2024-01-25T07:18:47.640+0200","rule":{"level":7,"description":"CVE-2023-40551 affects shim-signed","id":"23504","firedtimes":12,"mail":true,"groups":["vulnerability-detector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id":"1706159927.165959","decoder":{"name":"json"},"data":{"vulnerability":{"package":{"name":"shim-signed","source":"shim-signed","version":"1.51.3","architecture":"amd64","condition":"Package unfixed"},"cve":"CVE-2023-40551","title":"CVE-2023-40551 affects shim-signed","severity":"Medium","published":"2024-01-23","status":"Active","type":"PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40

551"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159928.444298,"timestamp":"2024-01-25T07:18:47.594+0200","rule":{"level
":7,"description":"CVE-2023-40551 affects
secureboot-db","id":"23504","firedtimes":11,"mail":true,"groups":["vulnerability-de
tector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]
},"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"
id":"1706159927.164850","decoder":{"name":"json"},"data":{"vulnerability":{"package
":{"name":"secureboot-db","version":"1.8","architecture":"amd64","condition":"Packa
ge unfixed"},"cve":"CVE-2023-40551","title":"CVE-2023-40551 affects
secureboot-db","severity":"Medium","published":"2024-01-23","status":"Active","type
":"PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-
40551"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159928.444284,"timestamp":"2024-01-25T07:18:47.549+0200","rule":{"level
":7,"description":"CVE-2023-40550 affects
shim-signed","id":"23504","firedtimes":10,"mail":true,"groups":["vulnerability-dete
ctor"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},
"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id
":"1706159927.163692","decoder":{"name":"json"},"data":{"vulnerability":{"package":
{"name":"shim-signed","source":"shim-signed","version":"1.51.3","architecture":"amd
64","condition":"Package unfixed"},"cve":"CVE-2023-40550","title":"CVE-2023-40550
affects
shim-signed","severity":"Medium","published":"2024-01-23","status":"Active","type":
"PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40
550"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159928.444259,"timestamp":"2024-01-25T07:18:47.503+0200","rule":{"level
":7,"description":"CVE-2023-40550 affects
secureboot-db","id":"23504","firedtimes":9,"mail":true,"groups":["vulnerability-det
ector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]}
,"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"i
d":"1706159927.162583","decoder":{"name":"json"},"data":{"vulnerability":{"package"
:{"name":"secureboot-db","version":"1.8","architecture":"amd64","condition":"Packag
e unfixed"},"cve":"CVE-2023-40550","title":"CVE-2023-40550 affects
secureboot-db","severity":"Medium","published":"2024-01-23","status":"Active","type
":"PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-
40550"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.444095,"timestamp":"2024-01-25T07:18:46.264+0200","rule":{"level
":7,"description":"CVE-2023-40549 affects
shim-signed","id":"23504","firedtimes":8,"mail":true,"groups":["vulnerability-detec
tor"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"
agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id"
:"1706159926.159805","decoder":{"name":"json"},"data":{"vulnerability":{"package":{
"name":"shim-signed","source":"shim-signed","version":"1.51.3","architecture":"amd6
4","condition":"Package unfixed"},"cve":"CVE-2023-40549","title":"CVE-2023-40549
affects shim-signed","rationale":"[Authenticode: verify that the signature header
is in bounds.In the validation logic in verify_buffer_authenticode(), there is
yetanother case where we need to guarantee an object is in the binary butwe're only

validating the pointer to it. In this case, we're validatingthat the actual signature data is in the binary, but unfortunately wefailed to validate that the header describing it is, so a malformedbinary can cause us to take an out-of-bounds read (probably but notnecessarily on the same page) past the end of the buffer.This patch adds a bounds check to verify that the signature isactually within the bounds.It seems unlikely this can be used for more than a denial of service,and if you can get shim to try to verify a malformed binary, you'veeffectively already accomplished a
DoS.]","severity":"Medium","published":"2024-01-23","status":"Active","type":"PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40549"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.444076,"timestamp":"2024-01-25T07:18:46.220+0200","rule":{"level":7,"description":"CVE-2023-40549 affects
secureboot-db","id":"23504","firedtimes":7,"mail":true,"groups":["vulnerability-detector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id":"1706159926.157076","decoder":{"name":"json"},"data":{"vulnerability":{"package":{"name":"secureboot-db","version":"1.8","architecture":"amd64","condition":"Package unfixed"},"cve":"CVE-2023-40549","title":"CVE-2023-40549 affects
secureboot-db","rationale":"[Authenticode: verify that the signature header is in bounds.In the validation logic in verify_buffer_authenticode(), there is yetanother case where we need to guarantee an object is in the binary butwe're only validating the pointer to it. In this case, we're validatingthat the actual signature data is in the binary, but unfortunately wefailed to validate that the header describing it is, so a malformedbinary can cause us to take an out-of-bounds read (probably but notnecessarily on the same page) past the end of the buffer.This patch adds a bounds check to verify that the signature isactually within the bounds.It seems unlikely this can be used for more than a denial of service,and if you can get shim to try to verify a malformed binary, you'veeffectively already accomplished a
DoS.]","severity":"Medium","published":"2024-01-23","status":"Active","type":"PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40549"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.444047,"timestamp":"2024-01-25T07:18:46.173+0200","rule":{"level":7,"description":"CVE-2023-40548 affects
shim-signed","id":"23504","firedtimes":6,"mail":true,"groups":["vulnerability-detector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id":"1706159926.154062","decoder":{"name":"json"},"data":{"vulnerability":{"package":{"name":"shim-signed","source":"shim-signed","version":"1.51.3","architecture":"amd64","condition":"Package unfixed"},"cve":"CVE-2023-40548","title":"CVE-2023-40548 affects shim-signed","rationale":"[Fix integer overflow on SBAT section size on 32-bit systemIn verify_sbat_section(), we do some math on data that comes from thebinary being verified - in this case, we add 1 to the size of the".sbat" section as reported in the section header, which is then used asthe input to the size of an allocation. The original value is then usedfor a size in a memcpy(), which means there's an out-of-bounds write inthe overflow case.Due to the type of the variable being size_t, but the type in thesection header being uint32_t, this is only plausibly accomplished on32-bit systems.This

patch makes the arithmetic use a checked add operation to avoidoverflow.
Additionally, it adds a check in verify_buffer_sbat() toguarantee that the data is
within the binary.It's not currently known if this is actually exploitable on
suchsystems; the memory layout on a particular machine may further mitigatethis
scenario.]","severity":"Medium","published":"2024-01-23","status":"Active","type":"
PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-405
48"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.173729,"timestamp":"2024-01-25T07:18:46.128+0200","rule":{"level
":7,"description":"CVE-2023-40548 affects
secureboot-db","id":"23504","firedtimes":5,"mail":true,"groups":["vulnerability-det
ector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]}
,"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"i
d":"1706159926.151097","decoder":{"name":"json"},"data":{"vulnerability":{"package"
:{"name":"secureboot-db","version":"1.8","architecture":"amd64","condition":"Packag
e unfixed"},"cve":"CVE-2023-40548","title":"CVE-2023-40548 affects
secureboot-db","rationale":"[Fix integer overflow on SBAT section size on 32-bit
systemIn verify_sbat_section(), we do some math on data that comes from thebinary
being verified - in this case, we add 1 to the size of the".sbat" section
as reported in the section header, which is then used asthe input to the size of an
allocation. The original value is then usedfor a size in a memcpy(), which means
there's an out-of-bounds write inthe overflow case.Due to the type of the variable
being size_t, but the type in thesection header being uint32_t, this is only
plausibly accomplished on32-bit systems.This patch makes the arithmetic use a
checked add operation to avoidoverflow. Additionally, it adds a check in
verify_buffer_sbat() toguarantee that the data is within the binary.It's not
currently known if this is actually exploitable on suchsystems; the memory layout
on a particular machine may further mitigatethis
scenario.]","severity":"Medium","published":"2024-01-23","status":"Active","type":"
PACKAGE","references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-405
48"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.1737,"timestamp":"2024-01-25T07:18:46.082+0200","rule":{"level":
7,"description":"CVE-2023-40547 affects
shim-signed","id":"23504","firedtimes":4,"mail":true,"groups":["vulnerability-detec
tor"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"
agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id"
:"1706159926.148596","decoder":{"name":"json"},"data":{"vulnerability":{"package":{
"name":"shim-signed","source":"shim-signed","version":"1.51.3","architecture":"amd6
4","condition":"Package unfixed"},"cve":"CVE-2023-40547","title":"CVE-2023-40547
affects shim-signed","rationale":"[avoid incorrectly trusting HTTP headersWhen
retrieving files via HTTP or related protocols, shim attempts toallocate a buffer
to store the received data. Unfortunately, this meansgetting the size from an HTTP
header, which can be manipulated tospecify a size that's smaller than the received
data. In this case, thecode accidentally uses the header for the allocation but
the protocolmetadata to copy it from the rx buffer, resulting in an
out-of-boundswrite.This patch adds an additional check to test that the rx buffer
is notlarger than the
allocation.]","severity":"Medium","published":"2024-01-23","status":"Active","type"
:"PACKAGE","bugzilla_references":["https://bugs.launchpad.net/ubuntu/+source/shim-s

igned/+bug/2051151"],"references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40547"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.082803,"timestamp":"2024-01-25T07:18:46.037+0200","rule":{"level":7,"description":"CVE-2023-40547 affects secureboot-db","id":"23504","firedtimes":3,"mail":true,"groups":["vulnerability-detector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id":"1706159926.146144","decoder":{"name":"json"},"data":{"vulnerability":{"package":{"name":"secureboot-db","version":"1.8","architecture":"amd64","condition":"Package unfixed"},"cve":"CVE-2023-40547","title":"CVE-2023-40547 affects secureboot-db","rationale":"[avoid incorrectly trusting HTTP headersWhen retrieving files via HTTP or related protocols, shim attempts toallocate a buffer to store the received data. Unfortunately, this meansgetting the size from an HTTP header, which can be manipulated tospecify a size that's smaller than the received data. In this case, thecode accidentally uses the header for the allocation but the protocolmetadata to copy it from the rx buffer, resulting in an out-of-boundswrite.This patch adds an additional check to test that the rx buffer is notlarger than the allocation.]","severity":"Medium","published":"2024-01-23","status":"Active","type":"PACKAGE","bugzilla_references":["https://bugs.launchpad.net/ubuntu/+source/shim-signed/+bug/2051151"],"references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40547"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.082783,"timestamp":"2024-01-25T07:18:45.990+0200","rule":{"level":7,"description":"CVE-2023-40546 affects shim-signed","id":"23504","firedtimes":2,"mail":true,"groups":["vulnerability-detector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id":"1706159925.144225","decoder":{"name":"json"},"data":{"vulnerability":{"package":{"name":"shim-signed","source":"shim-signed","version":"1.51.3","architecture":"amd64","condition":"Package unfixed"},"cve":"CVE-2023-40546","title":"CVE-2023-40546 affects shim-signed","rationale":"[mok: fix LogError() invocationOn some ARM platform, jlinton noticed that when we fail to set avariable (because it isn't supported at all, presumably), our errormessage has an extra argument that doesn't match the format string.This patch removes the extra argument.]","severity":"Medium","published":"2024-01-23","status":"Active","type":"PACKAGE","bugzilla_references":["https://bugs.launchpad.net/ubuntu/+source/shim-signed/+bug/2051151"],"references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40546"]}},"location":"vulnerability-detector"}
2024-01-25 05:18:50.456 172.16.21.47
{"true":1706159926.082757,"timestamp":"2024-01-25T07:18:45.945+0200","rule":{"level":7,"description":"CVE-2023-40546 affects secureboot-db","id":"23504","firedtimes":1,"mail":true,"groups":["vulnerability-detector"],"gdpr":["IV_35.7.d"],"pci_dss":["11.2.1","11.2.3"],"tsc":["CC7.1","CC7.2"]},"agent":{"id":"000","name":"wazuh","ip":"127.0.0.1"},"manager":{"name":"wazuh"},"id":"1706159925.142355","decoder":{"name":"json"},"data":{"vulnerability":{"package":{"name":"secureboot-db","version":"1.8","architecture":"amd64","condition":"Package unfixed"},"cve":"CVE-2023-40546","title":"CVE-2023-40546 affects secureboot-db","rationale":"[mok: fix LogError() invocationOn some ARM platform,

jlinton noticed that when we fail to set avariable (because it isn't supported at all, presumably), our errormessage has an extra argument that doesn't match the format string.This patch removes the extra argument.]","severity":"Medium","published":"2024-01-23","status":"Active","type":"PACKAGE","bugzilla_references":["https://bugs.launchpad.net/ubuntu/+source/shim-signed/+bug/2051151"],"references":["https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40546"]}},"location":"vulnerability-detector"}
2024-01-25 04:30:10.457 172.16.21.47
{"true":1706157009.189836,"timestamp":"2024-01-25T06:30:08.785+0200","rule":{"level":3,"description":"Service startup type was changed","id":"61104","info":"This does not appear to be logged on Windows 2000","firedtimes":2,"mail":true,"groups":["windows","windows_system","policy_changed"],"pci_dss":["10.6"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706157008.140531","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Service Control Manager","providerGuid":"{555908d1-a6d7-4695-8e1e-26931d2012f4}","eventSourceName":"Service Control Manager","eventID":"7040","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x8080000000000000","systemTime":"2024-01-25T04:30:06.1264843Z","eventRecordID":"1556","processID":"1200","threadID":"8940","channel":"System","computer":"test-pc","severityValue":"INFORMATION","message":"\"The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.\""},"eventdata":{"param1":"Background Intelligent Transfer Service","param2":"auto start","param3":"demand start","param4":"BITS"}}},"location":"EventChannel"}
2024-01-25 04:27:45.456 172.16.21.47
{"true":1706156864.177534,"timestamp":"2024-01-25T06:27:44.126+0200","rule":{"level":3,"description":"Service startup type was changed","id":"61104","info":"This does not appear to be logged on Windows 2000","firedtimes":1,"mail":true,"groups":["windows","windows_system","policy_changed"],"pci_dss":["10.6"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706156864.138707","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Service Control Manager","providerGuid":"{555908d1-a6d7-4695-8e1e-26931d2012f4}","eventSourceName":"Service Control Manager","eventID":"7040","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x8080000000000000","systemTime":"2024-01-25T04:27:41.4534002Z","eventRecordID":"1555","processID":"1200","threadID":"8940","channel":"System","computer":"test-pc","severityValue":"INFORMATION","message":"\"The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start.\""},"eventdata":{"param1":"Background Intelligent Transfer Service","param2":"demand start","param3":"auto start","param4":"BITS"}}},"location":"EventChannel"}
2024-01-25 04:27:45.456 172.16.21.47
{"true":1706156864.1775,"timestamp":"2024-01-25T06:27:44.064+0200","rule":{"level":3,"description":"Windows logon

success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":2,"mail":true,"groups":["windows","windows_security","authentication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"],"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706156864.131361","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-25T04:27:41.4143652Z","eventRecordID":"18075","processID":"1224","threadID":"1276","channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000

000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin
kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 04:26:45.456 172.16.21.47
{"true":1706156804.172589,"timestamp":"2024-01-25T06:26:43.431+0200","rule":{"level
":3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":1,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706156803.124015","decoder":{"name":"windows_eventchannel"},"data":{"wi
n":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"
{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0",
"task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-2
5T04:26:40.7764512Z","eventRecordID":"18073","processID":"1224","threadID":"6612","
channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":
"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the

length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 04:02:40.456 172.16.21.47
{"true":1706155356.052987,"timestamp":"2024-01-25T06:02:35.264+0200","rule":{"level":3,"description":"Software protection service scheduled successfully.","id":"60642","firedtimes":1,"mail":true,"groups":["windows","windows_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706155355.122424","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","providerGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software Protection Platform Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x80000000000000","systemTime":"2024-01-25T04:02:33.6188274Z","eventRecordID":"1529","processID":"7828","threadID":"0","channel":"Application","computer":"test-pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software Protection service for re-start at 2024-01-25T09:25:33Z. Reason: RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:33Z, RulesEngine"}}},"location":"EventChannel"}
2024-01-25 03:30:15.456 172.16.21.47
{"true":1706153412.887295,"timestamp":"2024-01-25T05:30:12.146+0200","rule":{"level":3,"description":"Service startup type was changed","id":"61104","info":"This does not appear to be logged on Windows 2000","firedtimes":2,"mail":true,"groups":["windows","windows_system","policy_changed"],"pci_dss":["10.6"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706153412.120600","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Service Control Manager","providerGuid":"{555908d1-a6d7-4695-8e1e-26931d2012f4}","eventSourceName":"Service Control Manager","eventID":"7040","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x8080000000000000","systemTime":"2024-01-25T03:30:09.5099608Z","eventRecordID":"1554","processID":"1200","threadID":"1796","channel":"System","computer":"test-pc","severityValue":"INFORMATION","message":"\"The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.\""},"eventdata":{"param1":"Background Intelligent Transfer Service","param2":"auto start","param3":"demand start","param4":"BITS"}}},"location":"EventChannel"}
2024-01-25 03:27:45.458 172.16.21.47
{"true":1706153263.874898,"timestamp":"2024-01-25T05:27:43.559+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid

Accounts"]},"firedtimes":1,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706153263.113254","decoder":{"name":"windows_eventchannel"},"data":{"wi
n":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"
{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0",
"task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-2
5T03:27:40.9112000Z","eventRecordID":"18067","processID":"1224","threadID":"2352","
channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":
"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the
length of the generated session key. This will be 0 if no session key was
requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$
","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-1
8","targetUserName":"SYSTEM","targetDomainName":"NT
AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","aut
henticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000
000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin

kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 03:27:45.458 172.16.21.47
{"true":1706153262.874763,"timestamp":"2024-01-25T05:27:42.872+0200","rule":{"level
":3,"description":"Service startup type was changed","id":"61104","info":"This does
not appear to be logged on Windows
2000","firedtimes":1,"mail":true,"groups":["windows","windows_system","policy_chang
ed"],"pci_dss":["10.6"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["
AU.6"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc
","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706153262.111430","decoder
":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Service
Control
Manager","providerGuid":"{555908d1-a6d7-4695-8e1e-26931d2012f4}","eventSourceName":
"Service Control
Manager","eventID":"7040","version":"0","level":"4","task":"0","opcode":"0","keywor
ds":"0x8080000000000000","systemTime":"2024-01-25T03:27:41.0648097Z","eventRecordID
":"1553","processID":"1200","threadID":"9232","channel":"System","computer":"test-p
c","severityValue":"INFORMATION","message":"\"The start type of the Background
Intelligent Transfer Service service was changed from demand start to auto
start.\""},"eventdata":{"param1":"Background Intelligent Transfer
Service","param2":"demand start","param3":"auto
start","param4":"BITS"}}},"location":"EventChannel"}
2024-01-25 03:16:45.456 172.16.21.47
{"true":1706152602.818794,"timestamp":"2024-01-25T05:16:42.111+0200","rule":{"level
":3,"description":"Software protection service scheduled
successfully.","id":"60642","firedtimes":1,"mail":true,"groups":["windows","windows
_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager"
:{"name":"wazuh"},"id":"1706152602.109839","decoder":{"name":"windows_eventchannel"
},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","provide
rGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software
Protection Platform
Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywo
rds":"0x80000000000000","systemTime":"2024-01-25T03:16:40.4821591Z","eventRecordID"
:"1527","processID":"7332","threadID":"0","channel":"Application","computer":"test-
pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software
Protection service for re-start at 2024-01-25T09:25:40Z. Reason:
RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:40Z,
RulesEngine"}}},"location":"EventChannel"}
2024-01-25 02:29:35.456 172.16.21.47
{"true":1706149770.586111,"timestamp":"2024-01-25T04:29:29.810+0200","rule":{"level
":3,"description":"Software protection service scheduled
successfully.","id":"60642","firedtimes":2,"mail":true,"groups":["windows","windows
_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager"
:{"name":"wazuh"},"id":"1706149769.108248","decoder":{"name":"windows_eventchannel"
},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","provide
rGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software
Protection Platform
Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywo
rds":"0x80000000000000","systemTime":"2024-01-25T02:29:28.1971210Z","eventRecordID"
:"1525","processID":"5424","threadID":"0","channel":"Application","computer":"test-
pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software

Protection service for re-start at 2024-01-25T09:25:28Z. Reason:
RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:28Z,
RulesEngine"}}},"location":"EventChannel"}
2024-01-25 02:29:05.456 172.16.21.47
{"true":1706149740.583616,"timestamp":"2024-01-25T04:28:59.870+0200","rule":{"level
":3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":3,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706149739.100902","decoder":{"name":"windows_eventchannel"},"data":{"wi
n":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"
{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0",
"task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-2
5T02:28:57.2557921Z","eventRecordID":"18062","processID":"1224","threadID":"8964","
channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":
"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the

length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 02:28:55.456 172.16.21.47
{"true":1706149732.58291,"timestamp":"2024-01-25T04:28:51.730+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":2,"mail":true,"groups":["windows","windows_security","authentication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"],"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706149731.93557","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-25T02:28:49.1152640Z","eventRecordID":"18060","processID":"1224","threadID":"1276","channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process

in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 02:18:20.456 172.16.21.47
{"true":1706149097.530319,"timestamp":"2024-01-25T04:18:17.181+0200","rule":{"level":3,"description":"Software protection service scheduled successfully.","id":"60642","firedtimes":1,"mail":true,"groups":["windows","windows_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706149097.91967","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","providerGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software Protection Platform Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x80000000000000","systemTime":"2024-01-25T02:18:15.5716349Z","eventRecordID":"1523","processID":"8680","threadID":"0","channel":"Application","computer":"test-pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software Protection service for re-start at 2024-01-25T09:26:15Z. Reason: RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:26:15Z, RulesEngine"}}},"location":"EventChannel"}
2024-01-25 02:18:00.456 172.16.21.47
{"true":1706149079.528725,"timestamp":"2024-01-25T04:17:58.556+0200","rule":{"level":3,"description":"PAM: Login session opened.","id":"5501","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":1,"mail":true,"groups":["pam","syslog","authentication_success"],"pci_dss":["10.2.5"],"gpg13":["7.8","7.9"],"gdpr":["IV_32.2"],"hipaa":["164.312.b"],"nist_800_53":["AU.14","AC.7"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1706149078.91532","full_log":"Jan 25 04:17:57 wazuh pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by (uid=1000)","predecoder":{"program_name":"pkexec","timestamp":"Jan 25 04:17:57","hostname":"wazuh"},"decoder":{"parent":"pam","name":"pam"},"data":{"dstuser":"root(uid=0)","uid":"1000"},"location":"/var/log/auth.log"}
2024-01-25 02:17:55.457 172.16.21.47
{"true":1706149070.527989,"timestamp":"2024-01-25T04:17:49.729+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid

Accounts"]},"firedtimes":1,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706149069.84187","decoder":{"name":"windows_eventchannel"},"data":{"win
":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{
54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","
task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-25
T02:17:47.1184917Z","eventRecordID":"18053","processID":"1224","threadID":"1276","c
hannel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"
\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the
length of the generated session key. This will be 0 if no session key was
requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$
","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-1
8","targetUserName":"SYSTEM","targetDomainName":"NT
AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","aut
henticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000
000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin

kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 01:47:40.456 172.16.21.47
{"true":1706147260.379982,"timestamp":"2024-01-25T03:47:40.325+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":1,"mail":true,"groups":["windows","windows_security","authentication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"],"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706147260.76842","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-25T01:47:37.7131933Z","eventRecordID":"18051","processID":"1224","threadID":"1276","channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$

","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-1
8","targetUserName":"SYSTEM","targetDomainName":"NT
AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","aut
henticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000
000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin
kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-25 01:05:00.457 172.16.21.47
{"true":1706144697.16812,"timestamp":"2024-01-25T03:04:56.767+0200","rule":{"level"
:3,"description":"Software protection service scheduled
successfully.","id":"60642","firedtimes":1,"mail":true,"groups":["windows","windows
_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager"
:{"name":"wazuh"},"id":"1706144696.75254","decoder":{"name":"windows_eventchannel"}
,"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","provider
Guid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software
Protection Platform
Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywo
rds":"0x80000000000000","systemTime":"2024-01-25T01:04:55.1833700Z","eventRecordID"
:"1521","processID":"320","threadID":"0","channel":"Application","computer":"test-p
c","severityValue":"INFORMATION","message":"\"Successfully scheduled Software
Protection service for re-start at 2024-01-25T09:25:55Z. Reason:
RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:55Z,
RulesEngine"}}},"location":"EventChannel"}
2024-01-24 23:46:50.456 172.16.21.47
{"true":1706140008.775091,"timestamp":"2024-01-25T01:46:47.875+0200","rule":{"level
":3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":7,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706140007.67909","decoder":{"name":"windows_eventchannel"},"data":{"win
":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{
54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","
task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24
T23:46:45.3295639Z","eventRecordID":"18049","processID":"1224","threadID":"1276","c
hannel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"
\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork

Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 23:46:50.456 172.16.21.47
{"true":1706140006.774812,"timestamp":"2024-01-25T01:46:46.123+0200","rule":{"level":3,"description":"Software protection service scheduled successfully.","id":"60642","firedtimes":3,"mail":true,"groups":["windows","windows_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706140006.66319","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","providerGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software Protection Platform Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x80000000000000","systemTime":"2024-01-24T23:46:44.5632186Z","eventRecordID":"1519","processID":"1304","threadID":"0","channel":"Application","computer":"test-pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software Protection service for re-start at 2024-01-25T09:25:44Z. Reason: RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:44Z, RulesEngine"}}},"location":"EventChannel"}
2024-01-24 23:46:25.456 172.16.21.47
{"true":1706139980.772391,"timestamp":"2024-01-25T01:46:19.791+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid

Accounts"]},"firedtimes":6,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706139979.58974","decoder":{"name":"windows_eventchannel"},"data":{"win
":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{
54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","
task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24
T23:46:17.2144634Z","eventRecordID":"18047","processID":"1224","threadID":"1276","c
hannel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"
\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the
length of the generated session key. This will be 0 if no session key was
requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$
","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-1
8","targetUserName":"SYSTEM","targetDomainName":"NT
AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","aut
henticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000
000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin

kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 23:46:15.456 172.16.21.47
{"true":1706139973.771706,"timestamp":"2024-01-25T01:46:12.848+0200","rule":{"level
":3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":5,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706139972.51629","decoder":{"name":"windows_eventchannel"},"data":{"win
":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{
54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","
task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24
T23:46:10.2810740Z","eventRecordID":"18030","processID":"1224","threadID":"9524","c
hannel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"
\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the
length of the generated session key. This will be 0 if no session key was
requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$

","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-1
8","targetUserName":"SYSTEM","targetDomainName":"NT
AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","aut
henticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000
000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin
kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 23:46:10.457 172.16.21.47
{"true":1706139965.771099,"timestamp":"2024-01-25T01:46:05.424+0200","rule":{"level
":3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":4,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706139965.44284","decoder":{"name":"windows_eventchannel"},"data":{"win
":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{
54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","
task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24
T23:46:02.8692378Z","eventRecordID":"18026","processID":"1224","threadID":"1276","c
hannel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"
\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID

is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 23:26:10.456 172.16.21.47
{"true":1706138769.672134,"timestamp":"2024-01-25T01:26:09.607+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":3,"mail":true,"groups":["windows","windows_security","authentication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"],"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706138769.36939","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24T23:26:07.0507577Z","eventRecordID":"18008","processID":"1224","threadID":"1276","channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the

account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 23:15:05.456 172.16.21.47
{"true":1706138104.616967,"timestamp":"2024-01-25T01:15:04.431+0200","rule":{"level":3,"description":"Software protection service scheduled successfully.","id":"60642","firedtimes":2,"mail":true,"groups":["windows","windows_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706138104.35347","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","providerGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software Protection Platform Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x80000000000000","systemTime":"2024-01-24T23:15:02.8857940Z","eventRecordID":"1514","processID":"10224","threadID":"0","channel":"Application","computer":"test-pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software Protection service for re-start at 2024-01-25T09:26:02Z. Reason: RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:26:02Z, RulesEngine"}}},"location":"EventChannel"}
2024-01-24 23:14:05.456 172.16.21.47
{"true":1706138041.612116,"timestamp":"2024-01-25T01:14:01.282+0200","rule":{"level":3,"description":"Software protection service scheduled successfully.","id":"60642","firedtimes":1,"mail":true,"groups":["windows","windows_application"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706138041.33757","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-SPP","providerGuid":"{E23B33B0-C8C9-472C-A5F9-F2BDFEA0F156}","eventSourceName":"Software Protection Platform Service","eventID":"16384","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x80000000000000","systemTime":"2024-01-24T23:13:59.7361291Z","eventRecordID":"1512","processID":"2584","threadID":"0","channel":"Application","computer":"test-pc","severityValue":"INFORMATION","message":"\"Successfully scheduled Software Protection service for re-start at 2024-01-25T09:25:59Z. Reason: RulesEngine.\""},"eventdata":{"data":"2024-01-25T09:25:59Z,

RulesEngine"}}},"location":"EventChannel"}
2024-01-24 23:13:35.456 172.16.21.47
{"true":1706138012.609661,"timestamp":"2024-01-25T01:13:32.290+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":2,"mail":true,"groups":["windows","windows_security","authentication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"],"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706138012.26412","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24T23:13:29.7447512Z","eventRecordID":"18006","processID":"1224","threadID":"6844","channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$

","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-1
8","targetUserName":"SYSTEM","targetDomainName":"NT
AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","aut
henticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000
000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin
kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 23:01:55.457 172.16.21.47
{"true":1706137314.55129,"timestamp":"2024-01-25T01:01:54.189+0200","rule":{"level"
:3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":1,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706137314.19067","decoder":{"name":"windows_eventchannel"},"data":{"win
":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{
54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","
task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24
T23:01:51.6369108Z","eventRecordID":"17991","processID":"1224","threadID":"9248","c
hannel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"
\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID

is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 22:30:15.456 172.16.21.47
{"true":1706135412.390324,"timestamp":"2024-01-25T00:30:11.994+0200","rule":{"level":3,"description":"Service startup type was changed","id":"61104","info":"This does not appear to be logged on Windows 2000","firedtimes":2,"mail":true,"groups":["windows","windows_system","policy_changed"],"pci_dss":["10.6"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706135411.17244","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Service Control Manager","providerGuid":"{555908d1-a6d7-4695-8e1e-26931d2012f4}","eventSourceName":"Service Control Manager","eventID":"7040","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x8080000000000000","systemTime":"2024-01-24T22:30:09.4563966Z","eventRecordID":"1548","processID":"1200","threadID":"5564","channel":"System","computer":"test-pc","severityValue":"INFORMATION","message":"\"The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.\""},"eventdata":{"param1":"Background Intelligent Transfer Service","param2":"auto start","param3":"demand start","param4":"BITS"}}},"location":"EventChannel"}
2024-01-24 22:27:45.456 172.16.21.47
{"true":1706135264.37747,"timestamp":"2024-01-25T00:27:43.558+0200","rule":{"level":3,"description":"Service startup type was changed","id":"61104","info":"This does not appear to be logged on Windows 2000","firedtimes":1,"mail":true,"groups":["windows","windows_system","policy_changed"],"pci_dss":["10.6"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706135263.15421","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Service Control Manager","providerGuid":"{555908d1-a6d7-4695-8e1e-26931d2012f4}","eventSourceName":"Service Control Manager","eventID":"7040","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x8080000000000000","systemTime":"2024-01-24T22:27:41.0263342Z","eventRecordID":"1547","processID":"1200","threadID":"5564","channel":"System","computer":"test-pc","severityValue":"INFORMATION","message":"\"The start type of the Background Intelligent Transfer Service service was changed from demand start to auto

start.\""},"eventdata":{"param1":"Background Intelligent Transfer
Service","param2":"demand start","param3":"auto
start","param4":"BITS"}}},"location":"EventChannel"}
2024-01-24 22:27:45.456 172.16.21.47
{"true":1706135263.377345,"timestamp":"2024-01-25T00:27:43.372+0200","rule":{"level
":3,"description":"Windows logon
success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense
Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid
Accounts"]},"firedtimes":2,"mail":true,"groups":["windows","windows_security","auth
entication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"]
,"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"
]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"waz
uh"},"id":"1706135263.8077","decoder":{"name":"windows_eventchannel"},"data":{"win"
:{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{5
4849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","t
ask":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24T
22:27:40.8526607Z","eventRecordID":"17987","processID":"1224","threadID":"7360","ch
annel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"\
"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the

length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 22:26:40.458 172.16.21.47
{"true":1706135200.372259,"timestamp":"2024-01-25T00:26:39.975+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":1,"mail":true,"groups":["windows","windows_security","authentication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"],"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706135199.734","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-24T22:26:37.4263994Z","eventRecordID":"17985","processID":"1224","threadID":"5264","channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process

in the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-18","targetUserName":"SYSTEM","targetDomainName":"NT AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","authenticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLinkedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 22:01:00.456 172.16.21.47
{"true":1706133655.455135,"timestamp":"2024-01-25T00:00:03.065+0200","rule":{"level":3,"description":"Apparmor DENIED","id":"52002","firedtimes":2,"mail":true,"groups":["local","syslog","apparmor"]},"agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1706133603.365","full_log":"Jan 25 00:00:02 wazuh kernel: [137071.206901] audit: type=1400 audit(1706133602.575:71): apparmor=\"DENIED\" operation=\"capable\" class=\"cap\" profile=\"/usr/sbin/cupsd\" pid=45059 comm=\"cupsd\" capability=12 capname=\"net_admin\"","predecoder":{"program_name":"kernel","timestamp":"Jan 25 00:00:02","hostname":"wazuh"},"decoder":{"parent":"kernel","name":"kernel"},"data":{"status":"DENIED","extra_data":"capable"},"location":"/var/log/kern.log"}
2024-01-24 22:01:00.456 172.16.21.47
{"true":1706133655.455121,"timestamp":"2024-01-25T00:00:03.065+0200","rule":{"level":3,"description":"Apparmor DENIED","id":"52002","firedtimes":1,"mail":true,"groups":["local","syslog","apparmor"]},"agent":{"id":"000","name":"wazuh"},"manager":{"name":"wazuh"},"id":"1706133603.0","full_log":"Jan 25 00:00:02 wazuh kernel: [137071.206901] audit: type=1400 audit(1706133602.575:71): apparmor=\"DENIED\" operation=\"capable\" class=\"cap\" profile=\"/usr/sbin/cupsd\" pid=45059 comm=\"cupsd\" capability=12 capname=\"net_admin\"","predecoder":{"program_name":"kernel","timestamp":"Jan 25 00:00:02","hostname":"wazuh"},"decoder":{"parent":"kernel","name":"kernel"},"data":{"status":"DENIED","extra_data":"capable"},"location":"/var/log/syslog"}
2024-01-24 21:45:10.456 172.16.21.47
{"true":1706132709.163679,"timestamp":"2024-01-24T23:45:09.044+0200","rule":{"level":3,"description":"Windows logon success.","id":"60106","mitre":{"id":["T1078"],"tactic":["Defense Evasion","Persistence","Privilege Escalation","Initial Access"],"technique":["Valid Accounts"]},"firedtimes":2,"mail":true,"groups":["windows","windows_security","authentication_success"],"gdpr":["IV_32.2"],"gpg13":["7.1","7.2"],"hipaa":["164.312.b"],"nist_800_53":["AC.7","AU.14"],"pci_dss":["10.2.5"],"tsc":["CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706132709.597654","decoder":{"name":"windows_eventchannel"},"data":{"win":{"system":{"providerName":"Microsoft-Windows-Security-Auditing","providerGuid":"{54849625-5478-4994-a5ba-3e3b0328c30d}","eventID":"4624","version":"3","level":"0","task":"12544","opcode":"0","keywords":"0x8020000000000000","systemTime":"2024-01-2

4T21:45:06.5330722Z","eventRecordID":"17983","processID":"1224","threadID":"1276","
channel":"Security","computer":"test-pc","severityValue":"AUDIT_SUCCESS","message":
"\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tTEST-PC$\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tRemote Credential
Guard:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated
Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew
Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount
Domain:\t\tNT AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon
ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon
GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess
Information:\r\n\tProcess ID:\t\t0x4b0\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork
Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-\r\n\tSource
Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon
Process:\t\tAdvapi \r\n\tAuthentication Package:\tNegotiate\r\n\tTransited
Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis
event is generated when a logon session is created. It is generated on the computer
that was accessed.\r\n\r\nThe subject fields indicate the account on the local
system which requested the logon. This is most commonly a service such as the
Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe
logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the
account for whom the new logon was created, i.e. the account that was logged
on.\r\n\r\nThe network fields indicate where a remote logon request originated.
Workstation name is not always available and may be left blank in some
cases.\r\n\r\nThe impersonation level field indicates the extent to which a process
in the logon session can impersonate.\r\n\r\nThe authentication information fields
provide detailed information about this specific logon request.\r\n\t- Logon GUID
is a unique identifier that can be used to correlate this event with a KDC
event.\r\n\t- Transited services indicate which intermediate services have
participated in this logon request.\r\n\t- Package name indicates which
sub-protocol was used among the NTLM protocols.\r\n\t- Key length indicates the
length of the generated session key. This will be 0 if no session key was
requested.\""},"eventdata":{"subjectUserSid":"S-1-5-18","subjectUserName":"TEST-PC$
","subjectDomainName":"WORKGROUP","subjectLogonId":"0x3e7","targetUserSid":"S-1-5-1
8","targetUserName":"SYSTEM","targetDomainName":"NT
AUTHORITY","targetLogonId":"0x3e7","logonType":"5","logonProcessName":"Advapi","aut
henticationPackageName":"Negotiate","logonGuid":"{00000000-0000-0000-0000-000000000
000}","keyLength":"0","processId":"0x4b0","processName":"C:\\\\Windows\\\\System32\
\\\services.exe","impersonationLevel":"%%1833","virtualAccount":"%%1843","targetLin
kedLogonId":"0x0","elevatedToken":"%%1842"}}},"location":"EventChannel"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131819.087571,"timestamp":"2024-01-24T23:30:18.825+0200","rule":{"level
":3,"description":"VirusTotal: Alert - No records in VirusTotal
database","id":"87103","firedtimes":4,"mail":true,"groups":["virustotal"]},"agent":
{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"
1706131818.596835","decoder":{"name":"json"},"data":{"virustotal":{"found":"0","mal
icious":"0","source":{"alert_id":"1706131816.555283","file":"HKEY_LOCAL_MACHINE\\Sy

stem\\CurrentControlSet\\Services\\SharedAccess\\Epoch","md5":"048cc4245ad1a8f2e00a
e663bc496051","sha1":"262d839b8d81e5f78cab7d6855d91950d4608470"}},"integration":"vi
rustotal"},"location":"virustotal"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131818.087424,"timestamp":"2024-01-24T23:30:17.594+0200","rule":{"level
":3,"description":"VirusTotal: Alert - No records in VirusTotal
database","id":"87103","firedtimes":3,"mail":true,"groups":["virustotal"]},"agent":
{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"
1706131817.596014","decoder":{"name":"json"},"data":{"virustotal":{"found":"0","mal
icious":"0","source":{"alert_id":"1706131815.552762","file":"HKEY_LOCAL_MACHINE\\Sy
stem\\CurrentControlSet\\Services\\rdyboost\\Parameters","md5":"b88587404e5f113f180
512d62815ac45","sha1":"06aa4c7cb25ab1463a2459beee1f82537bd9fcf1"}},"integration":"v
irustotal"},"location":"virustotal"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.595046,"timestamp":"2024-01-24T23:30:17.477+0200","rule":{"level
":5,"description":"Registry Value Entry
Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense
Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify
Registry"]},"firedtimes":11,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1
.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","P
I1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"
172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.595249","full_log":"Regi
stry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{EAD2CB2F-FAA5-43B3-A9B6
-0970BD6604AD}' deleted\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser
vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa
llRules","mode":"scheduled","arch":"[x32]","value_name":"{EAD2CB2F-FAA5-43B3-A9B6-0
970BD6604AD}","value_type":"REG_SZ","size_after":"365","md5_after":"ada453d7cfda4be
69e8f622c5dc6153d","sha1_after":"5e8c786a0723d002efb29fa1c2cf624eb8de448e","sha256_
after":"54927ab126fe2f06c813c53f2f3893d3eb9994b043f6cb9173238a1edd308570","event":"
deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck
"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.595031,"timestamp":"2024-01-24T23:30:17.461+0200","rule":{"level
":5,"description":"Registry Value Entry
Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense
Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify
Registry"]},"firedtimes":10,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1
.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","P
I1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"
172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.594484","full_log":"Regi
stry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{DB16F1F8-8E0E-413C-B2DD
-EF09ADFE097F}' deleted\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser

vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa
llRules","mode":"scheduled","arch":"[x32]","value_name":"{DB16F1F8-8E0E-413C-B2DD-E
F09ADFE097F}","value_type":"REG_SZ","size_after":"684","md5_after":"3ac485f3727b573
0183aec5154283027","sha1_after":"adc7eb254b6fa3ec68223a39108cf9bef1a908c5","sha256_
after":"6787d9a8457b2aa0a8054f0059e28e4f67cae949e6016da7e80fcc78fa9e8d27","event":"
deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck
"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.595007,"timestamp":"2024-01-24T23:30:17.446+0200","rule":{"level
":5,"description":"Registry Value Entry
Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense
Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify
Registry"]},"firedtimes":9,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.
f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI
1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"1
72.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.593719","full_log":"Regis
try Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{CD9BE4B2-A936-4D5F-B21B
-1A673AEA8122}' deleted\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser
vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa
llRules","mode":"scheduled","arch":"[x32]","value_name":"{CD9BE4B2-A936-4D5F-B21B-1
A673AEA8122}","value_type":"REG_SZ","size_after":"539","md5_after":"5854f5f5b1eb0d5
eb1d3651db914b4e7","sha1_after":"87f63b26bc5665d14482bf6f25d7f5e4b5d8ac4f","sha256_
after":"e16556b687b75d1466d1256dce2185f83661ceb32f7adc1d80672277a2981c0f","event":"
deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck
"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.446789,"timestamp":"2024-01-24T23:30:17.430+0200","rule":{"level
":5,"description":"Registry Value Entry
Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense
Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify
Registry"]},"firedtimes":8,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.
f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI
1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"1
72.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.592954","full_log":"Regis
try Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{A1D0B247-4436-4724-BF0E
-C2256E29F7F1}' deleted\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser
vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa
llRules","mode":"scheduled","arch":"[x32]","value_name":"{A1D0B247-4436-4724-BF0E-C
2256E29F7F1}","value_type":"REG_SZ","size_after":"685","md5_after":"bad2c46055fab1c
90b4a41b92f61e353","sha1_after":"5ea35bb2caf3baa15beb2d04e4e592d9f4796128","sha256_
after":"56c2d4ae2edf6755c88a1c80a36d9ead0b21ff799fa31366f51baf2b42f04051","event":"
deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck

"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.446772,"timestamp":"2024-01-24T23:30:17.415+0200","rule":{"level":5,"description":"Registry Value Entry Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify Registry"]},"firedtimes":7,"mail":true,"groups":["ossec","syscheck","syscheck_entry_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.592189","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{9FEE1EAF-17A8-45F6-A9E5-59BE93009970}' deleted\nMode: scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules","mode":"scheduled","arch":"[x32]","value_name":"{9FEE1EAF-17A8-45F6-A9E5-59BE93009970}","value_type":"REG_SZ","size_after":"671","md5_after":"188c72281d10167ad082c680024c9ed8","sha1_after":"d60e14382e3733065b45ca94a14211467ce37b5a","sha256_after":"c48dfd8db8ae5f24e5499c5e350facf20a96ac284bf6b58fa7969e8d6ce474be","event":"deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.446748,"timestamp":"2024-01-24T23:30:17.399+0200","rule":{"level":5,"description":"Registry Value Entry Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify Registry"]},"firedtimes":6,"mail":true,"groups":["ossec","syscheck","syscheck_entry_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.591424","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{9C262C34-BB5F-4ED1-9CE6-A6658C354014}' deleted\nMode: scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules","mode":"scheduled","arch":"[x32]","value_name":"{9C262C34-BB5F-4ED1-9CE6-A6658C354014}","value_type":"REG_SZ","size_after":"672","md5_after":"3d167320eb7848aed0a9787bb431a29a","sha1_after":"12aad32555d93252a7fe2e1977e0b057b2faf2c3","sha256_after":"d7729d076a4bdcd6b0aa7fb287f540d00a1ae073de7b985b58b89094aa5217b9","event":"deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.399785,"timestamp":"2024-01-24T23:30:17.383+0200","rule":{"level":5,"description":"Registry Value Entry Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify

Registry"]},"firedtimes":5,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.
f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI
1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"1
72.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.590659","full_log":"Regis
try Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{8463B8CF-06F1-434F-ACEE
-C274EA492ABB}' deleted\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser
vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa
llRules","mode":"scheduled","arch":"[x32]","value_name":"{8463B8CF-06F1-434F-ACEE-C
274EA492ABB}","value_type":"REG_SZ","size_after":"366","md5_after":"fdb49e9ca991c75
899872b09d1f81f57","sha1_after":"7743e21ae682d99b4efe6d940175c4d22d4e5a7f","sha256_
after":"e8975012250a65aa11587f7efb54bf13019f211f463b9ad3f7ddef0ba325d3ad","event":"
deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck
"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.39977,"timestamp":"2024-01-24T23:30:17.368+0200","rule":{"level"
:5,"description":"Registry Value Entry
Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense
Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify
Registry"]},"firedtimes":4,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.
f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI
1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"1
72.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.589894","full_log":"Regis
try Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{7031D32A-0E73-441B-B312
-6C2EE2747812}' deleted\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser
vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa
llRules","mode":"scheduled","arch":"[x32]","value_name":"{7031D32A-0E73-441B-B312-6
C2EE2747812}","value_type":"REG_SZ","size_after":"540","md5_after":"6046726dbb95622
591a00cf14fb9d13b","sha1_after":"563f6af58b15df1116b092f1bd9280587d57dedb","sha256_
after":"c49c91f2edbdd384619724ec5d7798b6e2d65fd4e24ca89308b3f22990504c96","event":"
deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck
"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.399744,"timestamp":"2024-01-24T23:30:17.352+0200","rule":{"level
":5,"description":"Registry Value Entry
Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense
Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify
Registry"]},"firedtimes":3,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.
f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI
1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"1
72.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.589129","full_log":"Regis
try Value '[x32]

HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{1E2AC6EA-5C48-44E5-A5F3-B0F41A57EA38}' deleted\nMode: scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules","mode":"scheduled","arch":"[x32]","value_name":"{1E2AC6EA-5C48-44E5-A5F3-B0F41A57EA38}","value_type":"REG_SZ","size_after":"672","md5_after":"5d7e4d08b477b4a9cee4a80acb7c0e69","sha1_after":"1323b4829a8d66732a3925f7b29f00cbd08787c3","sha256_after":"0986d9fc50c5a139c7f996be992df3c03dec7f4074adea92dc72c7ed7646d536","event":"deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.352782,"timestamp":"2024-01-24T23:30:17.349+0200","rule":{"level":5,"description":"Registry Value Entry Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify Registry"]},"firedtimes":2,"mail":true,"groups":["ossec","syscheck","syscheck_entry_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.588390","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules\\{A5B8C996-BB3A-4865-B66F-F2F371F0B9CC}' deleted\nMode: scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules","mode":"scheduled","arch":"[x32]","value_name":"{A5B8C996-BB3A-4865-B66F-F2F371F0B9CC}","value_type":"REG_SZ","size_after":"616","md5_after":"18bcb7377311dfd40559ac031e6a4144","sha1_after":"0779fabe3d78b9b9e9127042f31699308de327d2","sha256_after":"1191df829f04d9f180aa4bb1433eb79703e1f2cbf1550356db4821e7a191f387","event":"deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck"}
2024-01-24 21:30:20.458 172.16.21.47
{"true":1706131817.352756,"timestamp":"2024-01-24T23:30:17.349+0200","rule":{"level":5,"description":"Registry Value Entry Deleted.","id":"751","mitre":{"id":["T1070.004","T1485","T1112"],"tactic":["Defense Evasion","Impact"],"technique":["File Deletion","Data Destruction","Modify Registry"]},"firedtimes":1,"mail":true,"groups":["ossec","syscheck","syscheck_entry_deleted","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131817.587651","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules\\{05CA7568-AB6B-4CCA-94FE-07A2B9D8343E}' deleted\nMode: scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules","mode":"scheduled","arch":"[x32]","value_name":"{05CA7568-AB6B-4CCA-94FE-07A2B9D8343E}","value_type":"REG_SZ","size_after":"600","md5_after":"807b17a4d01041651bd3eff01d4a71f6","sha1_aft

er":"d9043f8752f581c4de852dc6f3b7bd56d45a35f3","sha256_after":"3c9c59bbdd6ea269acf7e98706184f208fdd48db012edda3290ebd49d080c132","event":"deleted"},"decoder":{"name":"syscheck_registry_value_deleted"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131817.087342,"timestamp":"2024-01-24T23:30:16.852+0200","rule":{"level":5,"description":"Registry Key Integrity Checksum Changed","id":"594","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":15,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.586301","full_log":"Registry Key '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\WinDefend\\Security' modified\nMode: scheduled\nChanged attributes: mtime\nOld modification time was: '1706052365', now it is '1706089160'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\WinDefend\\Security","mode":"scheduled","arch":"[x32]","win_perm_after":[{"name":"Users","allowed":["READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"Administrators","allowed":["DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"SYSTEM","allowed":["DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"CREATOR OWNER","allowed":["DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"ALL APPLICATION PACKAGES","allowed":["READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681","allowed":["READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]}],"uid_after":"S-1-5-18","gid_after":"S-1-5-18","uname_after":"SYSTEM","gname_after":"SYSTEM","mtime_before":"2024-01-24T01:26:05","mtime_after":"2024-01-24T11:39:20","changed_attributes":["mtime"],"event":"modified"},"decoder":{"name":"syscheck_registry_key_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131817.087313,"timestamp":"2024-01-24T23:30:16.837+0200","rule":{"level":5,"description":"Registry Key Integrity Checksum Changed","id":"594","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":14,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.584952","full_log":"Registry Key '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\WdFilter\\Security' modified\nMode: scheduled\nChanged attributes: mtime\nOld modification time was: '1706052365', now it is '1706089160'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\WdFilter\\Security","mode":"scheduled","arch":"[x32]","win_perm_after":[{"name":"Users","allowed":["READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name"

:"Administrators","allowed":["DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","REA
D_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"SYSTEM
","allowed":["DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_D
ATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"CREATOR
OWNER","allowed":["DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WR
ITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"ALL APPLICATION
PACKAGES","allowed":["READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"S-1
-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264
122-3456934681","allowed":["READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]}],"uid_
after":"S-1-5-18","gid_after":"S-1-5-18","uname_after":"SYSTEM","gname_after":"SYST
EM","mtime_before":"2024-01-24T01:26:05","mtime_after":"2024-01-24T11:39:20","chang
ed_attributes":["mtime"],"event":"modified"},"decoder":{"name":"syscheck_registry_k
ey_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.837787,"timestamp":"2024-01-24T23:30:16.821+0200","rule":{"level
":5,"description":"Registry Value Integrity Checksum
Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense
Evasion"],"technique":["Stored Data Manipulation","Modify
Registry"]},"firedtimes":12,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.
1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","
PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":
"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.583805","full_log":"Reg
istry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\TimeProviders\\Nt
pClient\\SpecialPollTimeRemaining' modified\nMode: scheduled\nChanged attributes:
md5,sha1,sha256\nOld md5sum was: 'eee0619cd2bdad945fca72b62b7d6810'\nNew md5sum is
: '9357dc7c66a81f7a5460134feac572f6'\nOld sha1sum was:
'f14ea7f82f1462a8a9cea1fcb5853c877eda34ca'\nNew sha1sum is :
'7c782c5dc37da4bdd9ede42104925717b060f73c'\nOld sha256sum was:
'9a99c69d739ea8ebef495d930881f829f40d8eb8327ccc7f994b640fcb8c19f7'\nNew sha256sum
is :
'7bd4b709a1989e05cd648875bfa81872f0625635d5387b72b6cca6d0b36fd188'\n","syscheck":{"
path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\TimeProvid
ers\\NtpClient","mode":"scheduled","arch":"[x32]","value_name":"SpecialPollTimeRema
ining","value_type":"REG_MULTI_SZ","size_after":"36","md5_before":"eee0619cd2bdad94
5fca72b62b7d6810","md5_after":"9357dc7c66a81f7a5460134feac572f6","sha1_before":"f14
ea7f82f1462a8a9cea1fcb5853c877eda34ca","sha1_after":"7c782c5dc37da4bdd9ede421049257
17b060f73c","sha256_before":"9a99c69d739ea8ebef495d930881f829f40d8eb8327ccc7f994b64
0fcb8c19f7","sha256_after":"7bd4b709a1989e05cd648875bfa81872f0625635d5387b72b6cca6d
0b36fd188","changed_attributes":["md5","sha1","sha256"],"event":"modified"},"decode
r":{"name":"syscheck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.837751,"timestamp":"2024-01-24T23:30:16.805+0200","rule":{"level
":5,"description":"Registry Key Integrity Checksum
Changed","id":"594","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense
Evasion"],"technique":["Stored Data Manipulation","Modify
Registry"]},"firedtimes":13,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.
1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","

PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":
"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.582345","full_log":"Reg
istry Key '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\TimeProviders\\Nt
pClient' modified\nMode: scheduled\nChanged attributes: mtime\nOld modification
time was: '1706037982', now it is
'1706124382'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\
Services\\W32Time\\TimeProviders\\NtpClient","mode":"scheduled","arch":"[x32]","win
_perm_after":[{"name":"Users","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA",
"READ_EA","WRITE_EA"]},{"name":"Administrators","allowed":["GENERIC_ALL","DELETE","
READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","REA
D_EA","WRITE_EA","EXECUTE"]},{"name":"SYSTEM","allowed":["GENERIC_ALL","DELETE","RE
AD_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_
EA","WRITE_EA","EXECUTE"]},{"name":"NETWORK
SERVICE","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]
},{"name":"W32Time","allowed":["GENERIC_READ","GENERIC_WRITE","DELETE","READ_CONTRO
L","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA"]},{"name":"Network
Configuration
Operators","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA
"]},{"name":"autotimesvc","allowed":["GENERIC_READ","GENERIC_WRITE","DELETE","READ_
CONTROL","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA"]}],"uid_after"
:"S-1-5-18","gid_after":"S-1-5-18","uname_after":"SYSTEM","gname_after":"SYSTEM","m
time_before":"2024-01-23T21:26:22","mtime_after":"2024-01-24T21:26:22","changed_att
ributes":["mtime"],"event":"modified"},"decoder":{"name":"syscheck_registry_key_mod
ified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.806475,"timestamp":"2024-01-24T23:30:16.790+0200","rule":{"level
":5,"description":"Registry Value Integrity Checksum
Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense
Evasion"],"technique":["Stored Data Manipulation","Modify
Registry"]},"firedtimes":11,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.
1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","
PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":
"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.581217","full_log":"Reg
istry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits\
\SecureTimeLow' modified\nMode: scheduled\nChanged attributes: md5,sha1,sha256\nOld
md5sum was: 'b11d9c3b12b6bcde55939c59d653fef4'\nNew md5sum is :
'f3984469016e9225465fea0637c23b74'\nOld sha1sum was:
'743c8f5eee4fa559802eebf7fee613db58f14099'\nNew sha1sum is :
'5793f4c472d8cfce3123f9425d56b69c9e5555b6'\nOld sha256sum was:
'bd349bc13951ebe01108a6a9730e445e30763dcd5cd960c0dc20215c3689dad7'\nNew sha256sum
is :
'd5ac3e2ccd2ec14d0822c6461f5b2243358efc2b8b5d139d5d909669f2ceb2b2'\n","syscheck":{"
path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTime
Limits","mode":"scheduled","arch":"[x32]","value_name":"SecureTimeLow","value_type"
:"REG_QWORD","size_after":"8","md5_before":"b11d9c3b12b6bcde55939c59d653fef4","md5_
after":"f3984469016e9225465fea0637c23b74","sha1_before":"743c8f5eee4fa559802eebf7fe
e613db58f14099","sha1_after":"5793f4c472d8cfce3123f9425d56b69c9e5555b6","sha256_bef

ore":"bd349bc13951ebe01108a6a9730e445e30763dcd5cd960c0dc20215c3689dad7","sha256_after":"d5ac3e2ccd2ec14d0822c6461f5b2243358efc2b8b5d139d5d909669f2ceb2b2","changed_attributes":["md5","sha1","sha256"],"event":"modified"},"decoder":{"name":"syscheck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.806437,"timestamp":"2024-01-24T23:30:16.774+0200","rule":{"level":5,"description":"Registry Key Integrity Checksum Changed","id":"594","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":12,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.579802","full_log":"Registry Key '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits' modified\nMode: scheduled\nChanged attributes: mtime\nOld modification time was: '1706088386', now it is '1706131587'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits","mode":"scheduled","arch":"[x32]","win_perm_after":[{"name":"Users","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"Administrators","allowed":["GENERIC_ALL","DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"SYSTEM","allowed":["GENERIC_ALL","DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"NETWORK SERVICE","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"LOCAL SERVICE","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"Network Configuration Operators","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"autotimesvc","allowed":["GENERIC_READ","GENERIC_WRITE","DELETE","READ_CONTROL","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA"]}],"uid_after":"S-1-5-18","gid_after":"S-1-5-18","uname_after":"SYSTEM","gname_after":"SYSTEM","mtime_before":"2024-01-24T11:26:26","mtime_after":"2024-01-24T23:26:27","changed_attributes":["mtime"],"event":"modified"},"decoder":{"name":"syscheck_registry_key_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.775451,"timestamp":"2024-01-24T23:30:16.774+0200","rule":{"level":5,"description":"Registry Value Integrity Checksum Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":10,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.578673","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits\\SecureTimeHigh' modified\nMode: scheduled\nChanged attributes:

md5,sha1,sha256\nOld md5sum was: '1b57770727bdd45cc45c5bf391895886'\nNew md5sum is
: '2ba6647837b0c15f86335730af194cb2'\nOld sha1sum was:
'ea8458f7a7bb90782fec3501c75746d47f219eea'\nNew sha1sum is :
'c92d00f46a39319d51a1381f926938033adb17f8'\nOld sha256sum was:
'afdfdbef9186e9068337741814c48bceb9e69fbcb9fad8035b62515825c1ea64'\nNew sha256sum
is :
'a238158feea92cb32685eef51f50aacf9b326bcd95cc482e9cbee295177d72b6'\n","syscheck":{"
path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTime
Limits","mode":"scheduled","arch":"[x32]","value_name":"SecureTimeHigh","value_type
":"REG_QWORD","size_after":"8","md5_before":"1b57770727bdd45cc45c5bf391895886","md5
_after":"2ba6647837b0c15f86335730af194cb2","sha1_before":"ea8458f7a7bb90782fec3501c
75746d47f219eea","sha1_after":"c92d00f46a39319d51a1381f926938033adb17f8","sha256_be
fore":"afdfdbef9186e9068337741814c48bceb9e69fbcb9fad8035b62515825c1ea64","sha256_af
ter":"a238158feea92cb32685eef51f50aacf9b326bcd95cc482e9cbee295177d72b6","changed_at
tributes":["md5","sha1","sha256"],"event":"modified"},"decoder":{"name":"syscheck_r
egistry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.775432,"timestamp":"2024-01-24T23:30:16.774+0200","rule":{"level
":5,"description":"Registry Value Integrity Checksum
Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense
Evasion"],"technique":["Stored Data Manipulation","Modify
Registry"]},"firedtimes":9,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1
.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","P
I1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"
172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.577539","full_log":"Regi
stry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits\
\SecureTimeEstimated' modified\nMode: scheduled\nChanged attributes:
md5,sha1,sha256\nOld md5sum was: '5f94d28226edcec94f5c4b2e9878dbcf'\nNew md5sum is
: '7476c94a0be2224e1c270cdf334538a8'\nOld sha1sum was:
'b61ef4088dd6b9508db9e3d27495df2b43c2f9db'\nNew sha1sum is :
'324354fad8a63951314ae0df39c1a62156b388fa'\nOld sha256sum was:
'9f6ab7377a0110b35cb0532ebeb722d9ad79cb694674a9c7c13d72965cd1f180'\nNew sha256sum
is :
'b79be55da01ff563b9665856cdb9e332353c1be941a361e23863b9bea2fd6cdf'\n","syscheck":{"
path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTime
Limits","mode":"scheduled","arch":"[x32]","value_name":"SecureTimeEstimated","value
_type":"REG_QWORD","size_after":"8","md5_before":"5f94d28226edcec94f5c4b2e9878dbcf"
,"md5_after":"7476c94a0be2224e1c270cdf334538a8","sha1_before":"b61ef4088dd6b9508db9
e3d27495df2b43c2f9db","sha1_after":"324354fad8a63951314ae0df39c1a62156b388fa","sha2
56_before":"9f6ab7377a0110b35cb0532ebeb722d9ad79cb694674a9c7c13d72965cd1f180","sha2
56_after":"b79be55da01ff563b9665856cdb9e332353c1be941a361e23863b9bea2fd6cdf","chang
ed_attributes":["md5","sha1","sha256"],"event":"modified"},"decoder":{"name":"sysch
eck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.775175,"timestamp":"2024-01-24T23:30:16.753+0200","rule":{"level
":3,"description":"VirusTotal: Alert - No records in VirusTotal
database","id":"87103","firedtimes":2,"mail":true,"groups":["virustotal"]},"agent":
{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"

1706131816.576718","decoder":{"name":"json"},"data":{"virustotal":{"found":"0","mal
icious":"0","source":{"alert_id":"1706131815.551598","file":"HKEY_LOCAL_MACHINE\\Sy
stem\\CurrentControlSet\\Services\\rdyboost\\Parameters","md5":"18680b280f1f325657a
386e6845b895e","sha1":"1370db7119b07801357186febb122b26d3c1be88"}},"integration":"v
irustotal"},"location":"virustotal"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.775164,"timestamp":"2024-01-24T23:30:16.727+0200","rule":{"level
":5,"description":"Registry Value Integrity Checksum
Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense
Evasion"],"technique":["Stored Data Manipulation","Modify
Registry"]},"firedtimes":8,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1
.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","P
I1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"
172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.575575","full_log":"Regi
stry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits\
\RunTime\\SecureTimeConfidence' modified\nMode: scheduled\nChanged attributes:
md5,sha1,sha256\nOld md5sum was: 'e5b546a8f4ea5a329bf0879d4fa694ae'\nNew md5sum is
: '0da8b50c79e264eef2fcb9856d22fe76'\nOld sha1sum was:
'8714a3e63d2a34d6fe9f43bbd51ffdac7c630bf9'\nNew sha1sum is :
'0f835c76ae44c0a75a4dba2725adeb99839f4e26'\nOld sha256sum was:
'405391cdcba508299713f0df3491fc39ee8044c599aac506de3456b6b3dd79e6'\nNew sha256sum
is :
'f3e7abbeb6ac146724ce867c5b83e093f2059910f3293d8daca0ddc2e0ec7493'\n","syscheck":{"
path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTime
Limits\\RunTime","mode":"scheduled","arch":"[x32]","value_name":"SecureTimeConfiden
ce","value_type":"REG_DWORD","size_after":"4","md5_before":"e5b546a8f4ea5a329bf0879
d4fa694ae","md5_after":"0da8b50c79e264eef2fcb9856d22fe76","sha1_before":"8714a3e63d
2a34d6fe9f43bbd51ffdac7c630bf9","sha1_after":"0f835c76ae44c0a75a4dba2725adeb99839f4
e26","sha256_before":"405391cdcba508299713f0df3491fc39ee8044c599aac506de3456b6b3dd7
9e6","sha256_after":"f3e7abbeb6ac146724ce867c5b83e093f2059910f3293d8daca0ddc2e0ec74
93","changed_attributes":["md5","sha1","sha256"],"event":"modified"},"decoder":{"na
me":"syscheck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.775133,"timestamp":"2024-01-24T23:30:16.712+0200","rule":{"level
":5,"description":"Registry Value Integrity Checksum
Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense
Evasion"],"technique":["Stored Data Manipulation","Modify
Registry"]},"firedtimes":7,"mail":true,"groups":["ossec","syscheck","syscheck_entry
_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1
.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","P
I1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"
172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.574433","full_log":"Regi
stry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits\
\RunTime\\SecureTimeTickCount' modified\nMode: scheduled\nChanged attributes:
md5,sha1,sha256\nOld md5sum was: 'c69a501509ba75fac0e82efed98bfdb6'\nNew md5sum is
: '26a65e273fa5a82f1839df4144e6f14a'\nOld sha1sum was:
'80e84e6cbe9919773783058329eed269c8884b66'\nNew sha1sum is :

'72cd1f40caab1712a60c48781be242536a06782a'\nOld sha256sum was:
'cf9b98d5b8b61998473f4a3a093ecbe6fbccb9f2a849621e3b46e78a7c97e693'\nNew sha256sum
is :
'f169bfe85c618e73e2a9848757c1a5d05347f29dd3737486c5948af41ea81af2'\n","syscheck":{"
path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTime
Limits\\RunTime","mode":"scheduled","arch":"[x32]","value_name":"SecureTimeTickCoun
t","value_type":"REG_QWORD","size_after":"8","md5_before":"c69a501509ba75fac0e82efe
d98bfdb6","md5_after":"26a65e273fa5a82f1839df4144e6f14a","sha1_before":"80e84e6cbe9
919773783058329eed269c8884b66","sha1_after":"72cd1f40caab1712a60c48781be242536a0678
2a","sha256_before":"cf9b98d5b8b61998473f4a3a093ecbe6fbccb9f2a849621e3b46e78a7c97e6
93","sha256_after":"f169bfe85c618e73e2a9848757c1a5d05347f29dd3737486c5948af41ea81af
2","changed_attributes":["md5","sha1","sha256"],"event":"modified"},"decoder":{"nam
e":"syscheck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.712557,"timestamp":"2024-01-24T23:30:16.697+0200","rule":{"level
":5,"description":"Registry Key Integrity Checksum
Changed","id":"594","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense
Evasion"],"technique":["Stored Data Manipulation","Modify
Registry"]},"firedtimes":11,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.
1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","
PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":
"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.572941","full_log":"Reg
istry Key '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\SecureTimeLimits\
\RunTime' modified\nMode: scheduled\nChanged attributes: mtime\nGroup ownership was
'S-1-5-32-544', now it is 'S-1-5-18'\nOld modification time was: '1706088386', now
it is
'1706131587'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\
Services\\W32Time\\SecureTimeLimits\\RunTime","mode":"scheduled","arch":"[x32]","wi
n_perm_after":[{"name":"Users","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA"
,"READ_EA","WRITE_EA"]},{"name":"Administrators","allowed":["GENERIC_ALL","DELETE",
"READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","RE
AD_EA","WRITE_EA","EXECUTE"]},{"name":"SYSTEM","allowed":["GENERIC_ALL","DELETE","R
EAD_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ
_EA","WRITE_EA","EXECUTE"]},{"name":"NETWORK
SERVICE","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]
},{"name":"LOCAL
SERVICE","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]
},{"name":"Network Configuration
Operators","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA
"]},{"name":"autotimesvc","allowed":["GENERIC_READ","GENERIC_WRITE","DELETE","READ_
CONTROL","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA"]}],"uid_after"
:"S-1-5-32-544","gid_before":"S-1-5-32-544","gid_after":"S-1-5-18","uname_after":"A
dministrators","gname_after":"SYSTEM","mtime_before":"2024-01-24T11:26:26","mtime_a
fter":"2024-01-24T23:26:27","changed_attributes":["mtime"],"event":"modified"},"dec
oder":{"name":"syscheck_registry_key_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.712517,"timestamp":"2024-01-24T23:30:16.692+0200","rule":{"level
":5,"description":"Registry Value Integrity Checksum

Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":6,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.571819","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\Config\\LastKnownGoodTime' modified\nMode: scheduled\nChanged attributes: md5,sha1,sha256\nOld md5sum was: '198ec812bdb2bbb1a81fd663618d7d85'\nNew md5sum is : 'ba879d208a7819f9f2a981af05d76b0d'\nOld sha1sum was: 'f601e80250afe0f064146c592dc48ee023438c08'\nNew sha1sum is : '8ccac4adc2fbe111a63e61132d4126f1445bdee3'\nOld sha256sum was: '4ef2ccde6d7530dc1dd86ddd05a5ff6178cfab9cb19a5f2eb67612ab72647d25'\nNew sha256sum is : 'fa061f5edb424343d5b373d32aed54ba2d90d64b516cb01ceaa354d3a7e2da19'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\Config","mode":"scheduled","arch":"[x32]","value_name":"LastKnownGoodTime","value_type":"REG_QWORD","size_after":"8","md5_before":"198ec812bdb2bbb1a81fd663618d7d85","md5_after":"ba879d208a7819f9f2a981af05d76b0d","sha1_before":"f601e80250afe0f064146c592dc48ee023438c08","sha1_after":"8ccac4adc2fbe111a63e61132d4126f1445bdee3","sha256_before":"4ef2ccde6d7530dc1dd86ddd05a5ff6178cfab9cb19a5f2eb67612ab72647d25","sha256_after":"fa061f5edb424343d5b373d32aed54ba2d90d64b516cb01ceaa354d3a7e2da19","changed_attributes":["md5","sha1","sha256"],"event":"modified"},"decoder":{"name":"syscheck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.693339,"timestamp":"2024-01-24T23:30:16.692+0200","rule":{"level":5,"description":"Registry Key Integrity Checksum Changed","id":"594","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":10,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.570376","full_log":"Registry Key '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\Config' modified\nMode: scheduled\nChanged attributes: mtime\nOld modification time was: '1706037982', now it is '1706124382'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\W32Time\\Config","mode":"scheduled","arch":"[x32]","win_perm_after":[{"name":"Users","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"Administrators","allowed":["GENERIC_ALL","DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"SYSTEM","allowed":["GENERIC_ALL","DELETE","READ_CONTROL","WRITE_DAC","WRITE_OWNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"name":"NETWORK SERVICE","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"W32Time","allowed":["GENERIC_READ","GENERIC_WRITE","DELETE","READ_CONTRO

L","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA"]},{"name":"Network Configuration Operators","allowed":["GENERIC_READ","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]},{"name":"autotimesvc","allowed":["GENERIC_READ","GENERIC_WRITE","DELETE","READ_CONTROL","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA"]}],"uid_after":"S-1-5-18","gid_after":"S-1-5-18","uname_after":"SYSTEM","gname_after":"SYSTEM","mtime_before":"2024-01-23T21:26:22","mtime_after":"2024-01-24T21:26:22","changed_attributes":["mtime"],"event":"modified"},"decoder":{"name":"syscheck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.693227,"timestamp":"2024-01-24T23:30:16.459+0200","rule":{"level":5,"description":"Registry Value Integrity Checksum Changed","id":"750","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":5,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.569264","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\TrustedInstaller\\Start' modified\nMode: scheduled\nChanged attributes: md5,sha1,sha256\nOld md5sum was: 'cc540920e91f05e4f6e4beb72dd441ac'\nNew md5sum is : '82cf9fa647dd1b3fbd9de71bbfb83fb2'\nOld sha1sum was: 'a8eddff2ec7d016b82d3e187c86b100e11502aaa'\nNew sha1sum is : 'f980f325b04d8f18f4fd73bb31f765806b3beda8'\nOld sha256sum was: '5c6bed0d94b9be8afbc5c8cac1e9d4be03f556917c2611ec56f4e6f341ef60d9'\nNew sha256sum is : '50a9b9163ebb829080aecf9a7a5990715de9fd63d48e3ea3734f6bd77aa3df07'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\TrustedInstaller","mode":"scheduled","arch":"[x32]","value_name":"Start","value_type":"REG_DWORD","size_after":"4","md5_before":"cc540920e91f05e4f6e4beb72dd441ac","md5_after":"82cf9fa647dd1b3fbd9de71bbfb83fb2","sha1_before":"a8eddff2ec7d016b82d3e187c86b100e11502aaa","sha1_after":"f980f325b04d8f18f4fd73bb31f765806b3beda8","sha256_before":"5c6bed0d94b9be8afbc5c8cac1e9d4be03f556917c2611ec56f4e6f341ef60d9","sha256_after":"50a9b9163ebb829080aecf9a7a5990715de9fd63d48e3ea3734f6bd77aa3df07","changed_attributes":["md5","sha1","sha256"],"event":"modified"},"decoder":{"name":"syscheck_registry_value_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.6932,"timestamp":"2024-01-24T23:30:16.459+0200","rule":{"level":5,"description":"Registry Key Integrity Checksum Changed","id":"594","mitre":{"id":["T1565.001","T1112"],"tactic":["Impact","Defense Evasion"],"technique":["Stored Data Manipulation","Modify Registry"]},"firedtimes":9,"mail":true,"groups":["ossec","syscheck","syscheck_entry_modified","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.568238","full_log":"Registry Key '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\TrustedInstaller'

modified\nMode: scheduled\nChanged attributes: mtime\nOld modification time was:
'1706088565', now it is
'1706088609'\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\
Services\\TrustedInstaller","mode":"scheduled","arch":"[x32]","win_perm_after":[{"n
ame":"SYSTEM","allowed":["GENERIC_ALL","DELETE","READ_CONTROL","WRITE_DAC","WRITE_O
WNER","READ_DATA","WRITE_DATA","APPEND_DATA","READ_EA","WRITE_EA","EXECUTE"]},{"nam
e":"Administrators","allowed":["GENERIC_READ","GENERIC_EXECUTE","READ_CONTROL","REA
D_DATA","READ_EA","WRITE_EA"]},{"name":"Users","allowed":["GENERIC_READ","GENERIC_E
XECUTE","READ_CONTROL","READ_DATA","READ_EA","WRITE_EA"]}],"uid_after":"S-1-5-32-54
4","gid_after":"S-1-5-32-544","uname_after":"Administrators","gname_after":"Adminis
trators","mtime_before":"2024-01-24T11:29:25","mtime_after":"2024-01-24T11:30:09","
changed_attributes":["mtime"],"event":"modified"},"decoder":{"name":"syscheck_regis
try_key_modified"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.693166,"timestamp":"2024-01-24T23:30:16.211+0200","rule":{"level
":5,"description":"Registry Value Entry Added to the
System","id":"752","mitre":{"id":["T1112"],"tactic":["Defense
Evasion"],"technique":["Modify
Registry"]},"firedtimes":11,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_added","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f
"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1
.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"17
2.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.567466","full_log":"Regist
ry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{93DBD75E-7845-49ED-85F4
-F0457F681D18}' added\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser
vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa
llRules","mode":"scheduled","arch":"[x32]","value_name":"{93DBD75E-7845-49ED-85F4-F
0457F681D18}","value_type":"REG_SZ","size_after":"672","md5_after":"b8293722fd65118
c8af7de8002671ecd","sha1_after":"4125f0b0fc3c67e913e49f842968727bc0b72ae0","sha256_
after":"da2a75fc2c7441b0c90a39e930d773aade193c979079219de5ac18e514d5cae8","event":"
added"},"decoder":{"name":"syscheck_registry_value_added"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.212423,"timestamp":"2024-01-24T23:30:16.196+0200","rule":{"level
":5,"description":"Registry Value Entry Added to the
System","id":"752","mitre":{"id":["T1112"],"tactic":["Defense
Evasion"],"technique":["Modify
Registry"]},"firedtimes":10,"mail":true,"groups":["ossec","syscheck","syscheck_entr
y_added","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f
"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1
.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"17
2.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.566694","full_log":"Regist
ry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\
FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{C0C8D9A9-264F-46FF-8BF2
-BE12B61EF749}' added\nMode:
scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Ser
vices\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\Firewa

llRules","mode":"scheduled","arch":"[x32]","value_name":"{C0C8D9A9-264F-46FF-8BF2-BE12B61EF749}","value_type":"REG_SZ","size_after":"685","md5_after":"d32d6b92c411e8d298153529c4b161d2","sha1_after":"de295b1706b7cb18498f46d5b40231a3a76252da","sha256_after":"c3223a1f70c27d4816772aaba5f57f378d9e573c67269954852115efc29367d0","event":"added"},"decoder":{"name":"syscheck_registry_value_added"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.212401,"timestamp":"2024-01-24T23:30:16.180+0200","rule":{"level":5,"description":"Registry Value Entry Added to the System","id":"752","mitre":{"id":["T1112"],"tactic":["Defense Evasion"],"technique":["Modify Registry"]},"firedtimes":9,"mail":true,"groups":["ossec","syscheck","syscheck_entry_added","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.565922","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{2D56C302-8981-4CC2-97FE-3DC0D9BF16BC}' added\nMode: scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules","mode":"scheduled","arch":"[x32]","value_name":"{2D56C302-8981-4CC2-97FE-3DC0D9BF16BC}","value_type":"REG_SZ","size_after":"684","md5_after":"e6b6f8ef3420dfd7c1d8a41aff8980c7","sha1_after":"b97b66cd42110e995daa3c18b9cf51cac9a595aa","sha256_after":"1d3aeafff4c3f15945e7cad30cd7ce28fc811c80e1f3e2bc9fd628b7e42db9d0","event":"added"},"decoder":{"name":"syscheck_registry_value_added"},"location":"syscheck"}
2024-01-24 21:30:20.457 172.16.21.47
{"true":1706131816.21237,"timestamp":"2024-01-24T23:30:16.164+0200","rule":{"level":5,"description":"Registry Value Entry Added to the System","id":"752","mitre":{"id":["T1112"],"tactic":["Defense Evasion"],"technique":["Modify Registry"]},"firedtimes":8,"mail":true,"groups":["ossec","syscheck","syscheck_entry_added","syscheck_registry"],"pci_dss":["11.5"],"gpg13":["4.13"],"gdpr":["II_5.1.f"],"hipaa":["164.312.c.1","164.312.c.2"],"nist_800_53":["SI.7"],"tsc":["PI1.4","PI1.5","CC6.1","CC6.8","CC7.2","CC7.3"]},"agent":{"id":"003","name":"test-pc","ip":"172.16.21.48"},"manager":{"name":"wazuh"},"id":"1706131816.565150","full_log":"Registry Value '[x32] HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\AppIso\\FirewallRules\\{F2F60CB0-5A25-4FBD-9847-6224CEBD5C5E}' added\nMode: scheduled\n","syscheck":{"path":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\Restrict