overwrites-custom-warnings.xml

```
<!-- Modify it at your will. -->
<group name="overwrites-custom-warnings">
  <rule id="60107" level="4" overwrite="yes">
    <if_sid>60104</if_sid>
    <field name="win.system.eventID">^577$|^4673$</field>
    <options>no_full_log</options>
    <description>Failed attempt to perform a privileged operation.</description>
  </rule>
<rule id="110001" level="4">
    <if_sid>92213</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\(?i)cleanmgr\.exe</field>
    <description>CleanMGR - Downlevel Info</description>
</rule>
   <rule id="110002" level="4">
      <if_sid>510</if_sid>
      <field name="file">/usr/sbin/apachectl</field>
      <description>Ignoring the rootcheck alert for the file: $(data.file).</description>
  </rule>
  <rule id="110003" level="4">
    <if_sid>550</if_sid>
    <field name="syscheck.path"
type="pcre2">\/etc\/cups\/subscriptions\.conf|\/etc\/cups\/subscriptions\.conf\.O</field>
    <description>Known file</description>
  </rule>
  <rule id="110004" level="4">
    <if_sid>533</if_sid>
    <description>Netstart Warnings move down</description>
  </rule>
  <rule id="110005" level="4">
    <if_sid>92151</if_sid>
    <field name="win.eventdata.image" type="pcre2">C:\\\\Program
```

```
Files\\\\Veeam\\\\\.+\\\\Veeam\.\w+\.\w+\.exe</field>
    <description>Powershell started by Veeam</description>
  </rule>
   <rule id="110006" level="4">
    <if_sid>92152</if_sid>
    <field name="win.eventdata.imageLoaded"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)System32\\\\spool\\\\drivers\\\\x64\\\\3\\\\PrintConfig.
dll</field>
    <description>Printer Powershell commands</description>
  </rule>
  <rule id="110007" level="4">
    <if_sid>92204</if_sid>
    <field name="win.eventdata.image" type="pcre2">C:\\\\Program Files|Program Files
\(x86\)\\\\Google\\\\Chrome\\\\Application\\\\chrome\.exe</field>
    <field name="win.eventdata.imageLoaded"
type="pcre2">C:\\\\Users\\\\.+\\\\AppData\\\\Local\\\\Temp\\\\.+\\\\software_reporter_tool\.ex
e</field>
    <description>Chrome Software Reporter</description>
  </rule>
  <rule id="110008" level="4">
    <if_sid>92204</if_sid>
    <field name="win.eventdata.image" type="pcre2">C:\\\\Program Files|Program Files
\(x86\)\\\\Google\\\\Update\\\\GoogleUpdate\.exe</field>
    <field name="win.eventdata.imageLoaded"
type="pcre2">C:\\\\Users\\\\.+\\\\AppData\\\\Local\\Temp\\\\.+\.exe</field>
    <description>Chrome Update</description>
  </rule>
  <rule id="110009" level="6">
    <if_sid>5402</if_sid>
    <description>Successful sudo to ROOT executed (Higher leveled).</description>
  </rule>
    <rule id="110010" level="6">
    <if_sid>5501</if_sid>
    <description>PAM: Login session opened (Higher leveled).</description>
  </rule>
    <rule id="110011" level="6">
    <if_sid>5502</if_sid>
    <description>PAM: Login session closed (Higher leveled).</description>
  </rule>
  <rule id="110012" level="6">
```

```
    <if_sid>5403</if_sid>
    <description>First time user executed sudo (Higher leveled).</description>
  </rule>
  <rule id="110013" level="6">
    <if_sid>5715</if_sid>
    <description>sshd: authentication success (Higher leveled).</description>
  </rule>
  <rule id="110014" level="4">
    <if_sid>5104</if_sid>
    <field name="description">Interface entered in promiscuous(sniffing) mode.</field>
    <description>Interface entered in promiscuous(sniffing) mode - Cortex Analyzer
working</description>
  </rule>
  <rule id="110015" level="4">
    <!-- Test: <if_sid>5402</if_sid> -->
    <if_sid>110009</if_sid>
    <field name="agent.name">pihole</field>
    <field name="data.srcuser">www-data</field>
    <description>Successful sudo to ROOT executed (Higher leveled).</description>
  </rule>
      <rule id="110016" level="4">
    <if_sid>5502</if_sid>
    <field name="name.agent">pihole</field>
    <field name="data.srcuser">www-data</field>
    <description>PAM: Login session closed (Down leveled).</description>
  </rule>
    <rule id="110017" level="4">
    <if_sid>92151</if_sid>
    <field name="win.eventdata.image" type="pcre2">C:\\\\Program
Files\\\\Veeam\\\\Backup365\\\\Veeam\.Archiver\.Service\.exe/gm</field>
    <description>Veeam starts Powershell commands</description>
  </rule>
  <rule id="110018" level="4">
    <if_sid>100651, 100653</if_sid>
    <field name="win.eventdata.parentimage" type="pcre2">C:\\\\Program Files|Program Files
\(x86\)\\\\TeamViewer\\\\Update\\\\update\.exe</field>
    <options>no_full_log</options>
    <description>TeamViewer Update</description>
</rule>
<rule id="110019" level="4">
```

```
    <if_sid>550</if_sid>
    <field name="syscheck.path" type="pcre2">/etc/pihole/\.+</field>
    <description>Ignoring PIHOLE Updates config</description>
  </rule>
  <rule id="110021" level="3">
    <if_sid>92151</if_sid>
    <field name="win.eventdata.user">BITSYSTEMS-
GMBH\\\\svc_monitoring|RESDOM\\\\svc_prtg</field>
    <description>Powershell started by PRTG</description>
  </rule>

  <rule id="110022" level="3">
    <if_sid>92151</if_sid>
    <field
name="win.eventdata.image">C:\\\\(?i)Windows\\\\(?i)System32\\\\(?i)ServerManager\.exe</field>
    <description>Powershell started by Servermanager</description>
  </rule>
  <rule id="110023" level="3">
    <if_sid>92151</if_sid>
    <field name="win.eventdata.image">C:\\\\Program Files \(x86\)\\\\Trend Micro\\\\Security
Agent\\\\utilCmdletWrapper\.exe</field>
    <description>Powershell started by TrendMicro</description>
  </rule>
  <rule id="110024" level="3">
    <if_sid>92151</if_sid>
    <field name="win.eventdata.image" type="pcre2">\w:\\\\Exchange
Server\\\\Bin\\\\Microsoft.Exchange.Store.Worker.exe</field>
    <description>Powershell started by Exchange Server</description>
  </rule>
  <rule id="110025" level="3">
    <if_sid>92204</if_sid>
    <field name="win.eventdata.image">C:\\\\Program Files (x86)\\\\Citrix\\\\ICA
Client\\\\receiver\\\\Receiver.exe</field>
    <field
name="win.eventdata.targetFilename">C:\\\\Users\\\\\w+\\\\AppData\\\\Local\\\\Temp\\\\\d\\\.+\
\\\CitrixReceiverUpdater.exe</field>
    <description>Citrix Receiver Update</description>
  </rule>
  <rule id="110026" level="3">
    <if_sid>119003</if_sid>
```

```
    <field name="misp.value">127.0.0.1|aka.ms</field>
    <description>Misp IoC's downgrade (false/positive)</description>
  </rule>
  <rule id="110027" level="3">
    <if_sid>9224</if_sid>
    <field
name="win.eventdata.image">C:\\\\Users\\\\\w+\\\\Downloads\\\\MicrosoftEdgeSetup\.exe</field>
    <field
name="win.eventdata.targetfilename">C:\\\\Users\\\\\.+\\\\AppData\\\\Local\\\\Temp\\\\\.+\\\\\
.+\\\\MicrosoftEdgeUpdate\w+\.exe</field>
    <description>Edge Update</description>
  </rule>
  <rule id="110028" level="3">
    <if_sid>510</if_sid>
    <field name="file">/var/tmp/tmccinstcheck\.dat</field>
    <description>TrendMicro Mac Updatecheck</description>
  </rule>
  <rule id="110029" level="3">
    <if_sid>510</if_sid>
    <field name="file">/tmp/ubuntu-advantage/candidate-version</field>
    <description>Ubuntu Advantage File</description>
  </rule>
  <rule id="110030" level="4">
    <if_sid>92204</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\sdiagnhost\.exe</field>
    <options>no_full_log</options>
    <description>CleanMGR - Downlevel Info</description>
  </rule>
  <rule id="110031" level="0">
    <if_sid>100652</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\schtasks\.exe</field>
    <field name="win.eventdata.CurrentDirectory" type="pcre2">C:\\\\Program Files\\\\Common
Files\\\\Microsoft Shared\\\\ClickToRun</field>
    <description>Office 365 Softwareupdate</description>
  </rule>
   <rule id="110032" level="3">
    <if_sid>92900</if_sid>
    <field name="win.eventdata.sourceImage"
```

```
type="pcre2">C:\\\\ProgramData\\\\Microsoft\\\\Windows
Defender\\\\Platform\\\\.+\\\\MsMpEng\.exe</field>
    <field name="win.eventdata.targetImage"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\(?i)lsass\.exe</field>
    <description>Defender Scan lsass.exe</description>
  </rule>
   <rule id="110033" level="3">
    <if_sid>92201</if_sid>
    <match>PSScriptPolicyTest</match>
    <description>Powershell PSScriptPolicyTest</description>
  </rule>
  <rule id="110034" level="4">
    <if_sid>92213</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\ServerManager\.exe</field>
    <description>ServerManager - Downlevel Info</description>
  </rule>
  <rule id="110035" level="0">
    <if_sid>100652</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\(?i)schtasks\.exe</field>
    <field name="win.eventdata.parrentImage" type="pcre2">C:\\\\(?i)Program
Files\\\\(?i)Common Files\\\\(?i)microsoft
shared\\\\(?i)ClickToRun\\\\(?i)officesvcmgr\.exe</field>
    <description>Office 365 Softwareupdate</description>
  </rule>
  <rule id="110036" level="3">
    <if_sid>92900</if_sid>
    <field name="win.eventdata.sourceImage"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\svchost\.exe|C:\\\\(?i)Windows\\\\(?i)system
32\\\\(?i)MRT\.exe</field>
    <field name="win.eventdata.targetImage"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\(?i)lsass\.exe</field>
    <description>SVChost/Defender access lsass.exe</description>
  </rule>
  <rule id="110037" level="3">
    <if_sid>510</if_sid>
    <field name="file" type="pcre2">/tmp/filter.lock</field>
    <description>Downlevel Anomalidetection</description>
  </rule>
```

```
  <rule id="110038" level="3">
    <if_sid>87702</if_sid>
    <srcip>192.168.33.240</srcip>
    <description>OPNsense: $(agent.name) on $(hostname) - Source $(srcip) Destionation
$(dstip)</description>
  </rule>
   <rule id="110039" level="4">
      <if_sid>510</if_sid>
      <field name="file"> /bin/diff</field>
      <description>Ignoring the rootcheck alert for the file: $(data.file).</description>
  </rule>
  <rule id="110040" level="4">
    <if_sid>92213</if_sid>
    <field name="win.eventdata.image" type="pcre2">C:\\\\(?i)Windows\\\\(?i)Application
Compatibility Scripts\\\\(?i)acregl\.exe</field>
    <description>ServerManager - Downlevel Info</description>
  </rule>
  <rule id="110041" level="0">
    <if_sid>92213</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\Windows\\\\system32\\\\wsmprovhost.exe</field>
    <field name="win.eventdata.targetFilename"
type="pcre2">AppData\\\\Local\\\\Temp\\\\__PSScriptPolicyTest_*</field>
    <description>Ignore PSScript PolicyTest</description>
  </rule>
  <rule id="110042" level="0">
    <if_sid>92213</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\(?i)wsmprovhost\.exe|C:\\\\(?i)Windows\\\\(?
i)system32\\\\(?i)sdiagnhost\.exe</field>
    <field name="win.eventdata.targetFilename"
type="pcre2">C:\\\\(?i)Users\\\\\w+\\\\(?i)AppData\\\\(?i)Local\\\\(?i)Temp\\\\__PSScriptPolic
yTest_\w+\.\w+\.ps1</field>
    <description>Ignore PSScript PolicyTest</description>
  </rule>
  <rule id="110043" level="5">
    <if_sid>92657</if_sid>
    <field name="agent.name" type="pcre2">MGMT-SRV</field>
    <description>MGMT-SRV RDP Logon downlevel</description>
  </rule>
```

```
  <rule id="110044" level="3">
    <if_sid>60602</if_sid>
    <field name="win.eventdata.library"
type="pcre2">C:\\\\(?i)Windows\\\\(?i)system32\\\\(?i)ntdsperf\.dll</field>
    <description>Windows Perflib downlevel</description>
  </rule>
  <rule id="110045" level="3">
    <if_sid>100652</if_sid>
    <field name="win.eventdata.parentimage" type="pcre2">C:\\\\(?i)Program Files\\\\(?i)Common
Files\\\\(?i)microsoft shared\\\\(?i)ClickToRun\\\\(?i)officesvcmgr\.exe</field>
    <description>Schedular Officeupdate downlevel</description>
  </rule>
</group>
```

Revision #2
Created 2024-01-03 07:38:50 UTC by Peter Leibling
Updated 2024-02-15 07:25:38 UTC by Peter Leibling