Wazuh Denoising

> [Rule 510]: Trojaned version of file detected (/bin/diff)

Lösung:

- Copy https://github.com/ossec/ossec-hids/blob/master/src/rootcheck/db/rootkit_trojans.txt to /var/ossec/etc/shared/ on your hub server.
- upgrade from source out of master

Weitere Informationen: https://github.com/ossec/ossec-hids/issues/2020

> [Rule 92213]: Executable file dropped in folder commonly used by malware (cleanmgr.exe)

Lösung:

Erstellen/erweitern der overwrites-custom-warnings.xml mit folgenden Inhalt (ggf. Rule ID anpassen):

```
  <rule id="110030" level="4">
    <if_sid>92204</if_sid>
    <field name="win.eventdata.image"
type="pcre2">C:\\\\Windows\\\\system32\\\\sdiagnhost\.exe</field>
    <options>no_full_log</options>
    <description>CleanMGR - Downlevel Info</description>
  </rule>
```

> [Rule 510]: Host-based anomaly detection event (/var/lib/docker/overlay2 und /var/lib/docker/volume)

Anpassen der Konfigurationsdatei im Bereich Rootcheck, anschließend Manager neu starten:

```
  <ignore>/var/lib/docker/overlay2/</ignore>
  <ignore>/var/lib/docker/volume/</ignore>
```

> Keine Vulnerability detects für Ubuntu 22.04

Hinzufügen zu der Konfiguration im Abschnitt Vulnerability-detector / Provider Canonical - anschließend speichern und Manager neustarten:

```
    <os>jammy</os>
```

> [Rule: 92201]: powershell.exe created a new scripting file under Windows Temp or User data folder (PSPolicyScript)

Lösung:

Erstellen/erweitern der overwrites-custom-warnings.xml mit folgenden Inhalt (ggf. Rule ID anpassen):

```
<rule id="110031" 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>PSScript PolicyTest ignorieren</description>
  </rule>
```

Quelle:
https://www.reddit.com/r/Wazuh/comments/174enng/create_exclusion_for_false_positive/?rdt=50834

Revision #8
Created 2024-01-03 07:04:07 UTC by Peter Leibling
Updated 2024-01-03 07:37:27 UTC by Peter Leibling