Erstellen eines eigenen Decoders

Sollten Sie Systeme mit Syslog erfassen welche noch nicht unterstützt sind, dann sind diese zwar in den Archive Logs (wazuh-archive-*) können jedoch noch keine Alerts erzeugen.

Damit dies funktioniert, müssen sogenannte Decoder erstellt werden. Dies sind XML Dateien, welche die wazuh-archives-* Logs überwachen nach bestimmten Textmustern und dann diese in Alerts umwandeln, welche dann später sogar weiter interagieren können (z.B. Emailalerts, Integrations, Cases erstellen usw.).

Einen Decoder für die Sophos UTM erstelle ich gerade selber, da ich diesen benötige Die Dateien für erstelle ich später auf Github wenn dieser fertig ist.

Einen Beitrag von Wazuh selber, wie man Decoder selber erstellt findet ihr hier:

https://wazuh.com/blog/creating-decoders-and-rules-from-scratch/

Hier ist der aktuelle Stand (Stand 21.12.2022):

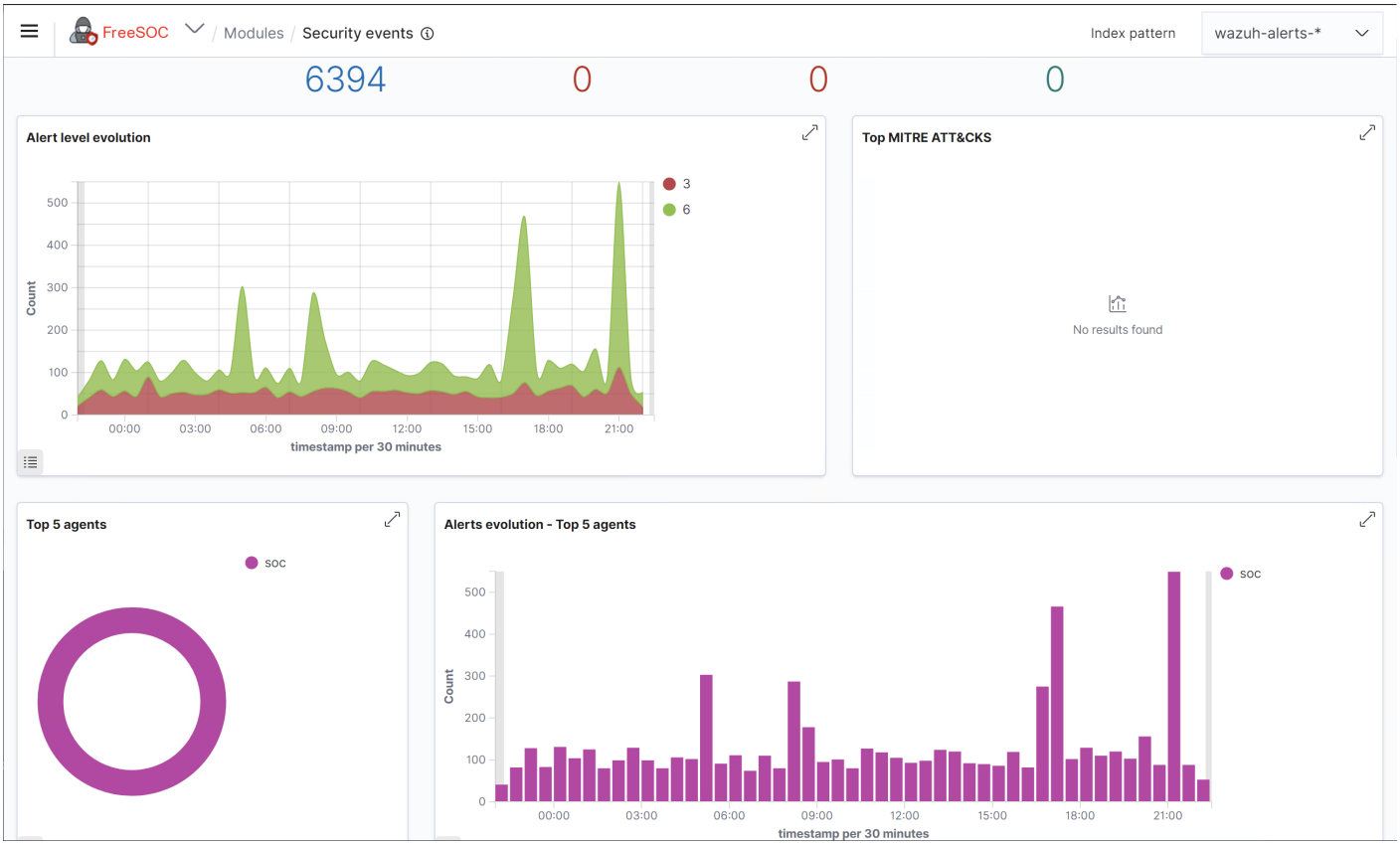
```
<decoder name="sophos-utm-custom">
  <prematch>^\d+:\d+:\d+-\d+:\d+:\d+\s\w+\s\w+[\d+]:\sid="\d+"</prematch>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex>(\d+:\d+:\d+)-(\d+:\d+:\d+)\s(\w+)\s(\w+)</regex>
  <order>date, time, hostname, module</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">name=\p(\w+\s\w+)</regex>
  <order>status</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">severity=\p(\w+\s\w+)</regex>
```

```
  <order>severity</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">sub=\p(\w+\s\w+)</regex>
  <order>sub</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">sys=\p(\w+\s\w+)</regex>
  <order>sys</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">srcip=\p(\d+.\d+.\d+.\d+)\p</regex>
  <order>srcip</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">dstip=\p(\d+.\d+.\d+.\d+)\p</regex>
  <order>dstip</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">srcport=\p(\d+)\p</regex>
  <order>srcport</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">dsport=\p(\d+)\p</regex>
  <order>dstport</order>
</decoder>

<decoder name="sophos-utm-custom-child">
```

```
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">profile=\p(\w+)\p</regex>
  <order>profile</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">filteraction=\p(\w+)\p</regex>
  <order>filteraction</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">url=\p(\S+)\p</regex>
  <order>url</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">referer=\p(\S+)\p</regex>
  <order>referer</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">reputation=\p(\w+)\p</regex>
  <order>reputation</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">categoryname=\p(\w+)\p</regex>
  <order>categoryname</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">user=\p(\w+)\p</regex>
  <order>user</order>
</decoder>
```

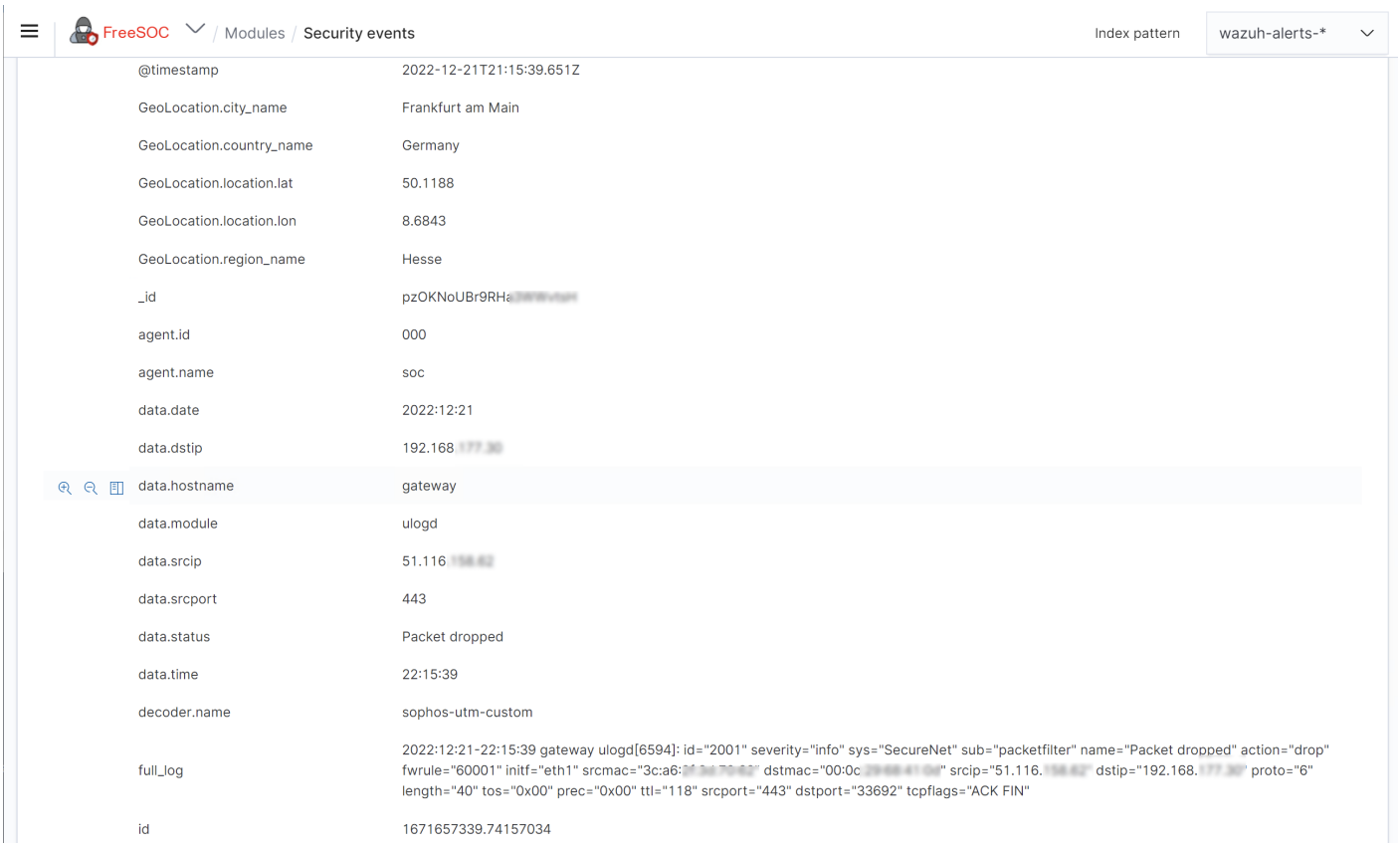
```
<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">group=\p(\w+)\p</regex>
  <order>group</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">id=\p(\d+)\p</regex>
  <order>id</order>
</decoder>

<decoder name="sophos-utm-custom-child">
  <parent>sophos-utm-custom</parent>
  <regex offset="after_parent">reason=\p(\w+)\p</regex>
  <order>action</order>
</decoder>
```

Dazu ein paar Bilder, wie das in Wazuh aussieht:



Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Dec 21, 2022 @ 22:15:39.651	000	soc			Sophos: Packet dropped on soc - Source 51.116.158.62 Destionation 192.168.177.30	6	117011
Dec 21, 2022 @ 22:15:39.651	000	soc			Sophos: Packet dropped on soc - Source 51.116.158.62 Destionation 192.168.177.30	6	117011
Dec 21, 2022 @ 22:15:39.651	000	soc			Sophos: Packet dropped on soc - Source 51.116.158.62 Destionation 192.168.177.30	6	117011
Dec 21, 2022 @ 22:15:13.590	000	soc			Sophos: Packet accepted on soc - Source 192.168.1.1 Destionation 192.168.50.10	3	117010
Dec 21, 2022 @ 22:15:13.590	000	soc			Sophos: Packet accepted on soc - Source 192.168.1.1 Destionation 192.168.50.10	3	117010
Dec 21, 2022 @ 22:15:07.461	000	soc			Sophos: AFC Alert on soc - ulogd: AFC Alert	3	117002
Dec 21, 2022 @ 22:14:52.698	000	soc			Sophos: AFC Alert on soc - ulogd: AFC Alert	3	117002
Dec 21, 2022 @ 22:14:50.150	000	soc			Sophos: Packet dropped on soc - Source 192.168.1.144 Destionation 224.0.0.1	6	117011
Dec 21, 2022 @ 22:14:22.354	000	soc			Sophos: Packet dropped on soc - Source 162.213.33.50 Destionation 192.168.177.30	6	117011



Revision #4
Created 2022-12-21 21:26:35 UTC by Peter Leibling
Updated 2022-12-29 14:37:44 UTC by Peter Leibling