

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">dstport=\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>

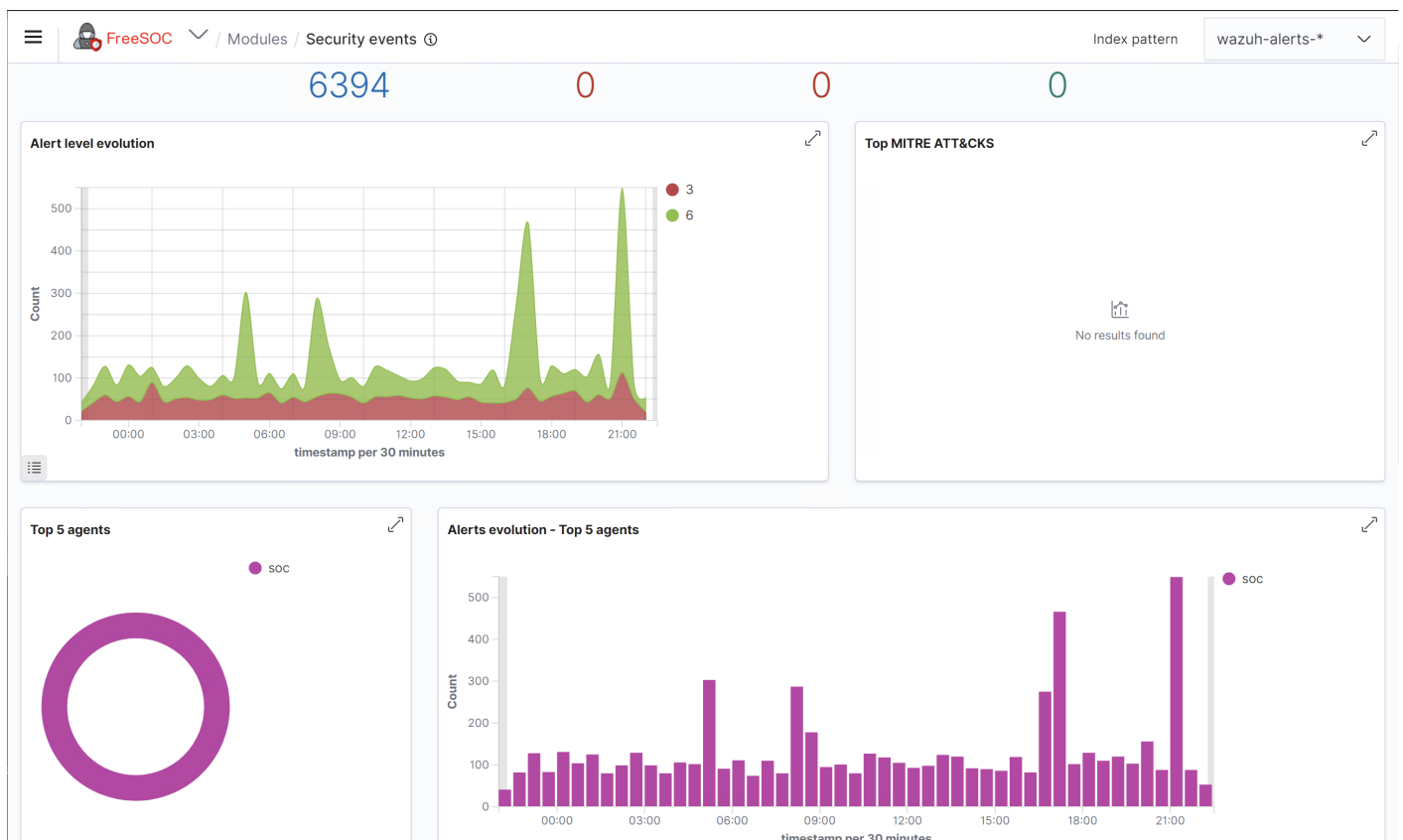
```

```

<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 Destination 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 Destination 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 Destination 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 Destination 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 Destination 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 Destination 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 Destination 192.168.177.30	6	117011

FreeSOC / Modules / Security events Index pattern wazuh-alerts-*

@timestamp	2022-12-21T21:15:39.651Z
GeoLocation.city_name	Frankfurt am Main
GeoLocation.country_name	Germany
GeoLocation.location.lat	50.1188
GeoLocation.location.lon	8.6843
GeoLocation.region_name	Hesse
_id	pzOKNoUBr9RH...
agent.id	000
agent.name	soc
data.date	2022:12:21
data.dstip	192.168.177.30
data.hostname	gateway
data.module	ulogd
data.srcip	51.116.158.62
data.srcport	443
data.status	Packet dropped
data.time	22:15:39
decoder.name	sophos-utm-custom
full_log	2022:12:21-22:15:39 gateway ulogd[6594]: id="2001" severity="info" sys="SecureNet" sub="packetfilter" name="Packet dropped" action="drop" fwrule="60001" initf="eth1" srcmac="3c:a6:31:11:77:53" dstmac="00:0c:29:88:41:00" srcip="51.116.158.62" dstip="192.168.177.30" proto="6" length="40" tos="0x00" prec="0x00" ttl="118" srcport="443" dstport="33692" tcpflags="ACK FIN"
id	1671657339.74157034

Revision #4

Created 2022-12-21 21:26:35 UTC by Peter Leibling

Updated 2022-12-29 14:37:44 UTC by Peter Leibling