overwrites-custom-sophos.xml

```
<!-- Modify it at your will. -->
<!-- Rules for Sophos UTM Custom -->

<group name="syslog,sophos,">
  <rule id="117001" level="3">
    <decoded_as>sophos-utm-custom</decoded_as>
    <description>Sophos: log without rule</description>
  </rule>

  <rule id="117002" level="3">
    <if_sid>117001</if_sid>
    <status>Authentication successful|AFC Alert|strict TCP</status>
    <description>Sophos: $(status) on $(hostname) - $(module): $(status)</description>
  </rule>

  <rule id="117003" level="12">
    <if_sid>117001</if_sid>
    <status>Authentication failed</status>
    <description>Sophos: $(status) on $(location) - User $(dstuser) [$(srcip)]</description>
  </rule>

    <!-- rule id="117004" level="12">
    <if_sid>117001</if_sid>
    <sub>up2date</sub>
    <description>Sophos: $(hostname) Service $(sub) - Status $(name)</description>
  </rule -->

  <rule id="117009" level="12">
    <if_sid>117001</if_sid>
    <hostname>smtp</hostname>
    <description>Sophos: $(status) on $(hostname) - User $(dstuser) [$(srcip)]</description>
  </rule>

   <rule id="117010" level="3">
    <if_sid>117001</if_sid>
```

```
    <status>Packet accepted</status>
    <description>Sophos: $(status) on $(hostname) - Source $(srcip) Destionation
$(dstip)</description>
  </rule>

  <rule id="117011" level="6">
    <if_sid>117001</if_sid>
    <status>Packet dropped</status>
    <description>Sophos: $(status) on $(hostname) - Source $(srcip) Destionation
$(dstip)</description>
  </rule>

  <rule id="117012" level="6">
    <if_sid>117001</if_sid>
    <status>Packet dropped (GEOIP)</status>
    <description>Sophos: $(status) on $(hostname) - Source $(srcip) Destionation
$(dstip)</description>
  </rule>

  <rule id="117013" level="6">
    <if_sid>117001</if_sid>
    <match>/var/chroot-httpd/var/webadmin/extra/httpd_session_cleanup</match>
    <description>Sophos: httpdcleanup on $(hostname)</description>
  </rule>

</group>
```

Revision #2
Created 2024-01-03 07:41:28 UTC by Peter Leibling
Updated 2024-02-15 07:27:02 UTC by Peter Leibling