<form stylesheet="timepicker.css">

<label>Performances Monitoring</label>...<fieldset submitButton="true" autoRun="true">

<input type="dropdown" token="tok\_filtersite" searchWhenChanged="true">

<label>SITE</label>

<fieldForLabel>SITE</fieldForLabel>

<fieldForValue>SITE</fieldForValue>

<search>

<query>| inputlookup lookup\_cmdb\_fo\_all.csv

| fields SITE

| dedup SITE

| table SITE

| sort +SITE</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<default>\*</default>

<initialValue>\*</initialValue>

<choice value="\*">\*</choice>

<choice value="Toul\*">Toul\*</choice>

</input>

</fieldset>

<row>

<panel>

<html>

<p>

<img width="25" height="26" src="/static/app/SA\_AI\_NR\_CF60\_FOAnalyser\_IndustrialPC\_Monitoring\_sh/images/home.jpg" align="middle"/> <a href="/app/SA\_AI\_NR\_S180\_FOAnalyser\_sh">Home</a>

</p>

</html>

</panel>

</row>

<row>

<panel>

<html>

<div class="chapter">System crashes - Blue Screen of Death Monitoring</div>

</html>

</panel>

</row>

<row id="first">

<panel>

<title>Crashes - Volume percentage (%)</title>

<single id="test">

<title>Source : Windows Event Viewer (ID 6008) - Slot time : last 30 days</title>

<search>

<query>[| inputlookup host.csv

| table host] index="ai-wkst-wineventlog-fr" sourcetype=XmlWinEventLog source="XmlWinEventLog:System" EventCode=1067 (Level=1 OR Level=2 OR Level=3)

| dedup host

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats dc(host) as NbEventCodeHost

| appendcols

[| inputlookup host.csv

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats dc(host) as NbIndHost

]

| eval Perc=round((NbEventCodeHost/NbIndHost)\*100,2). " %" + " / " + NbIndHost + " machines "

| table Perc</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<option name="colorMode">none</option>

<option name="drilldown">all</option>

<option name="rangeColors">["0x65a637","0xd93f3c","0xd93f3c"]</option>

<option name="rangeValues">[0,1]</option>

<option name="refresh.display">progressbar</option>

<option name="useColors">1</option>

<drilldown>

<link target="\_blank">/app/SA\_AI\_NR\_CF60\_FOAnalyser\_IndustrialPC\_Monitoring\_sh/performances\_monitoring\_\_crashes\_volume\_details?SITE=$tok\_filtersite|s$</link>

</drilldown>

</single>

</panel>

<panel>

<title>Crashes - Count of impacted host</title>

<single>

<title>Source : Windows Event Viewer (ID 6008) - Slot time : last 30 days</title>

<search>

<query>[| inputlookup host.csv

| table host] index="ai-wkst-wineventlog-fr" sourcetype=XmlWinEventLog source="XmlWinEventLog:System" EventCode=1067 (Level=1 OR Level=2 OR Level=3)

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats dc(host)</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<option name="colorMode">none</option>

<option name="drilldown">none</option>

<option name="rangeColors">["0x65a637","0xd93f3c"]</option>

<option name="rangeValues">[0]</option>

<option name="refresh.display">progressbar</option>

<option name="useColors">1</option>

</single>

</panel>

<panel>

<title>Crashes -Top 10 by host</title>

<table>

<title>Source : Windows Event Viewer (ID 6008) - Slot time : last 30 days</title>

<search>

<query>[| inputlookup host.csv

| table host] index="ai-wkst-wineventlog-fr" sourcetype=XmlWinEventLog source="XmlWinEventLog:System" EventCode=1067 (Level=1 OR Level=2 OR Level=3)

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats count(EventCode) as Total by host

| sort -Total limit=10</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<option name="count">10</option>

<option name="drilldown">row</option>

<option name="refresh.display">progressbar</option>

<format type="color" field="Total">

<colorPalette type="minMidMax" maxColor="#D93F3C" minColor="#F5A9A9"></colorPalette>

<scale type="minMidMax"></scale>

</format>

<drilldown>

<link target="\_blank">/app/SA\_AI\_NR\_CF60\_FOAnalyser\_IndustrialPC\_Monitoring\_sh/performances\_monitoring\_\_crashes\_host\_details?SITE=$tok\_filtersite|s$</link>

</drilldown>

</table>

</panel>

</row>

<row>

<panel>

<title>Last 10 crashes by host</title>

<table>

<title>Source : Windows Event Viewer (ID 6008) &amp; CMDB (ITOP, SCCM) - Slot time : last 30 days</title>

<search>

<query>(index="ai-wkst-wineventlog-fr" sourcetype=XmlWinEventLog source="XmlWinEventLog:System" EventCode=1067 (Level=1 OR Level=2 OR Level=3))

[| inputlookup host.csv

| table host]

| table \_time host EventCode

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE ROOM TOWN COUNTRY OS

| lookup patchlevel.csv "Computer" as host

| search SITE=$tok\_filtersite|s$

| eval time = strftime(\_time, "%m/%d/%Y %H:%M")

| stats latest(time) as time values(COUNTRY) as COUNTRY values(TOWN) as TOWN values(SITE) as SITE values(ROOM) as ROOM values(OS) as OS values(flag\_patch\_version) as PatchLevel by host

| table time host COUNTRY TOWN SITE ROOM OS PatchLevel

| sort -time - COUNTRY limit=10</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<option name="count">10</option>

<option name="drilldown">row</option>

<option name="refresh.display">progressbar</option>

<drilldown>

<link target="\_blank">/app/SA\_AI\_NR\_CF60\_FOAnalyser\_IndustrialPC\_Monitoring\_sh/performances\_monitoring\_\_crashes\_last\_details?SITE=$tok\_filtersite|s$</link>

</drilldown>

</table>

</panel>

</row>

<row id="second">

<panel>

<html>

<div class="chapter">CPU process alert Monitoring - Threshold : CPU &gt; 80% and Duration &gt;= 3 minute</div>

</html>

</panel>

</row>

<row>

<panel>

<title>CPU alert volume (%)</title>

<single id="test3">

<title>Source : Windows Perfmon Monitor - Slot time : last 30 days</title>

<search>

<query>[| inputlookup host.csv

| table host] index="ai-wkst-perfmon-fr" sourcetype="perfmonmk:process"

| where process\_cpu\_used\_percent&gt;80

| bucket \_time span=3m

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats dc(host) as NbHostProcessSup80

| appendcols

[| inputlookup host.csv

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats dc(host) as NbIndHost]

| eval Perc=round((NbHostProcessSup80/NbIndHost)\*100,2). " %" + " / " + NbIndHost + " machines "

| table Perc</query>

<earliest>0</earliest>

<latest></latest>

</search>

<option name="drilldown">all</option>

<option name="refresh.display">progressbar</option>

<drilldown>

<link target="\_blank">/app/SA\_AI\_NR\_CF60\_FOAnalyser\_IndustrialPC\_Monitoring\_sh/performances\_monitoring\_\_cpu\_volume\_alert\_details?SITE=$tok\_filtersite|s$</link>

</drilldown>

</single>

</panel>

<panel>

<title>CPU alert - Top 10 by host</title>

<table>

<title>Source : Windows Perfmon Monitor - Slot time : last 30 days</title>

<search>

<query>[| inputlookup host.csv

| table host] index="ai-wkst-perfmon-fr" sourcetype="perfmonmk:process"

| bucket \_time span=3m

| where process\_cpu\_used\_percent&gt;80

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats dc(process\_name) as Total by host

| sort -Total limit=10</query>

<earliest>0</earliest>

<latest></latest>

</search>

<option name="count">10</option>

<option name="drilldown">row</option>

<option name="refresh.display">progressbar</option>

<format type="color" field="Total">

<colorPalette type="minMidMax" maxColor="#D93F3C" minColor="#F5A9A9"></colorPalette>

<scale type="minMidMax"></scale>

</format>

<drilldown>

<link target="\_blank">/app/SA\_AI\_NR\_CF60\_FOAnalyser\_IndustrialPC\_Monitoring\_sh/performances\_monitoring\_\_cpu\_host\_details?SITE=$tok\_filtersite|s$</link>

</drilldown>

</table>

</panel>

</row>

<row>

<panel>

<title>CPU alert - Top 10 by process</title>

<chart>

<title>Source : Windows Perfmon Monitor - Slot time : last 30 days</title>

<search>

<query>[| inputlookup host.csv

| table host] index="ai-wkst-perfmon-fr" sourcetype="perfmonmk:process"

| bucket \_time span=3m

| where process\_cpu\_used\_percent&gt;80

| dedup host process\_name

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats count(host) as Total by process\_name

| sort -Total limit=10</query>

<earliest>0</earliest>

<latest></latest>

</search>

<option name="charting.axisTitleX.visibility">visible</option>

<option name="charting.axisTitleY.visibility">visible</option>

<option name="charting.axisTitleY2.visibility">visible</option>

<option name="charting.chart">pie</option>

<option name="charting.drilldown">none</option>

<option name="charting.legend.placement">right</option>

<option name="refresh.display">progressbar</option>

</chart>

</panel>

<panel>

<title>CPU alert - Last 10 alerts by host timechart</title>

<chart>

<title>Source : Windows Perfmon Monitor - Slot time : last 30 days</title>

<search>

<query>[| inputlookup host.csv

| table host] index="ai-wkst-perfmon-fr" sourcetype="perfmonmk:process"

| bucket \_time span=3m

| where process\_cpu\_used\_percent&gt;80

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| timechart avg(process\_cpu\_used\_percent) as process\_cpu\_used\_percent by host</query>

<earliest>0</earliest>

<latest></latest>

</search>

<option name="charting.axisTitleX.visibility">visible</option>

<option name="charting.axisTitleY.text">process\_cpu\_used\_percent</option>

<option name="charting.axisTitleY.visibility">visible</option>

<option name="charting.axisTitleY2.visibility">visible</option>

<option name="charting.axisY.abbreviation">none</option>

<option name="charting.axisY.maximumNumber">100</option>

<option name="charting.axisY.scale">linear</option>

<option name="charting.chart">line</option>

<option name="charting.chart.nullValueMode">connect</option>

<option name="charting.drilldown">none</option>

<option name="charting.layout.splitSeries">0</option>

<option name="charting.legend.placement">right</option>

<option name="refresh.display">progressbar</option>

</chart>

</panel>

</row>

<row id="third">

<panel>

<html>

<div class="chapter">Compliance Monitoring</div>

</html>

</panel>

</row>

<row>

<panel>

<title>Patches non-compliance volume (%)</title>

<single id="test2">

<title>Source : DCM Report - Slot time : last 30 days</title>

<search>

<query>| inputlookup host.csv

| lookup patchlevel.csv "Computer" as host

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats count by flag\_patch\_version

| stats sum(count) as NbNonCompliantPatchesIndHost

| appendcols

[| inputlookup host.csv

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats count(host) as NbIndHost]

| eval Perc=round((NbNonCompliantPatchesIndHost/NbIndHost)\*100,2). " %" + " / " + NbIndHost + " machines "

| table Perc</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<option name="drilldown">none</option>

<option name="rangeColors">["0x65a637","0xd93f3c","0xd93f3c"]</option>

<option name="rangeValues">[0,30]</option>

<option name="refresh.display">progressbar</option>

<option name="useColors">1</option>

</single>

</panel>

<panel>

<title>Patches non-compliance by host</title>

<table>

<title>Source : DCM Report - Slot time : last 30 days</title>

<search>

<query>| inputlookup host.csv

| lookup patchlevel.csv "Computer" as host

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats count by host flag\_patch\_version

| where isnotnull(flag\_patch\_version)

| rename flag\_patch\_version as PatchLevel

| fields - count

| sort +PatchLevel limit=10</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<option name="count">10</option>

<option name="drilldown">row</option>

<option name="refresh.display">progressbar</option>

<format type="color" field="Patch\_Level">

<colorPalette type="minMidMax" maxColor="#31A35F" minColor="#FFFFFF"></colorPalette>

<scale type="minMidMax"></scale>

</format>

<drilldown>

<link target="\_blank">/app/SA\_AI\_NR\_CF60\_FOAnalyser\_IndustrialPC\_Monitoring\_sh/performances\_monitoring\_\_patches\_host\_details?SITE=$tok\_filtersite|s$</link>

</drilldown>

</table>

</panel>

</row>

<row>

<panel>

<title>Patches non-compliance count by Patch Level</title>

<table>

<title>Source : DCM Report - Slot time : last 30 days</title>

<search>

<query>| inputlookup host.csv

| lookup patchlevel.csv "Computer" as host

| lookup lookup\_cmdb\_fo\_all.csv HOSTNAME as host output SITE

| search SITE=$tok\_filtersite|s$

| stats count as Total by flag\_patch\_version, OSVersion

| rename flag\_patch\_version as PatchLevel, OSVersion as OS

| sort -Total</query>

<earliest>-30d@d</earliest>

<latest>now</latest>

</search>

<option name="count">10</option>

<option name="drilldown">row</option>

<format type="color" field="count">

<colorPalette type="minMidMax" maxColor="#D93F3C" minColor="#F5A9A9"></colorPalette>

<scale type="minMidMax"></scale>

</format>

<format type="color" field="Total">

<colorPalette type="minMidMax" maxColor="#D93F3C" minColor="#F5A9A9"></colorPalette>

<scale type="minMidMax"></scale>

</format>

</table>

</panel>

</row>

</form>