Measure Your Bad Self

The SIEMquel

Craig Bowser
@reswob10
How are your SOC Analysts Doing?
How are your SOC Tools Doing?
Search took .1 seconds
No hits

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Org</th>
<th>Handle</th>
<th>Job</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Search for speaker “SANS Tactical Detection Summit 2018” taken within the last 5 minutes.

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Org</th>
<th>Handle</th>
<th>Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>Craig</td>
<td>Dept</td>
<td></td>
<td>Sr Sec Engineer</td>
<td></td>
</tr>
</tbody>
</table>
Search for speaker “SANS Tactical Detection Summit 2018”
time=[-5m TO now] | table First Last Org Handle Job

Search took .1 seconds
One hit

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Org</th>
<th>Handle</th>
<th>Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>Craig</td>
<td>Bowser</td>
<td>Dept Energy</td>
<td>@reswob10</td>
<td>Sr Sec Engineer</td>
</tr>
</tbody>
</table>
What is the health of the data your tools are collecting?

Are you collecting everywhere?

Are you collecting everything?

Are you collecting from every time?

Are you collecting in a timely manner?
Are you getting logs from everywhere?
Are you getting logs from everything?
Percentage change in the number of events

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVG Number of Events</td>
<td>13066</td>
</tr>
<tr>
<td>Number of Recent Events</td>
<td>14956</td>
</tr>
<tr>
<td>Broke Ratio</td>
<td>1.1446502372570029</td>
</tr>
<tr>
<td>Status</td>
<td>NORMAL</td>
</tr>
</tbody>
</table>
Percentage change in the number of events

<table>
<thead>
<tr>
<th>AVG Number of Events</th>
<th>Number of Recent Events</th>
<th>Broke Ratio</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2102.8</td>
<td>7743</td>
<td>3.6822</td>
<td>ADDED</td>
</tr>
</tbody>
</table>
Percentage change in the number of Devices

```
index=syswin earliest=-5h
| stats dc(host) as oldnumdev
| appendcols
|   [ search index=syswin earliest=-1h
|       | stats dc(host) as newnumdev]
| eval isbroke = (newnumdev/oldnumdev)
| eval Status = case(isbroke<=0.9,"MISSING",isbroke>=1.1,"ADDED",true(),"NORMAL")
| rename oldnumdev as "Number old Devices", newnumdev as "Number new Devices", isbroke as "Broke Ratio"
| table "Number old Devices" "Number new Devices" "Broke Ratio" Status
```
Percentage change in the number of Devices

```
index=syswin earliest=-12h
| stats dc(host) as oldnumdev
| appendcols
  [ search index=syswin earliest=-1h
  | stats dc(host) as newnumdev]
  | eval isbroke = (newnumdev/oldnumdev)
  | eval Status = case(isbroke<=0.9,"MISSING",isbroke>=1.1,"ADDED",true(),"NORMAL")
  | rename oldnumdev as "Number old Devices", newnumdev as "Number new Devices", isbroke as "Broke Ratio"
| table "Number old Devices" "Number new Devices" "Broke Ratio" Status
```
<table>
<thead>
<tr>
<th>Node ID</th>
<th>Description</th>
<th>Location Path</th>
<th>Purpose</th>
<th>CMD8 Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.10.28.21</td>
<td>ACME Data Center</td>
<td>Ground Floor &gt; Comp. Production</td>
<td>in operation</td>
<td>-</td>
</tr>
<tr>
<td>16.10.28.22</td>
<td>ACME Data Center</td>
<td>Ground Floor &gt; Comp. Production</td>
<td>in operation</td>
<td>-</td>
</tr>
<tr>
<td>16.10.28.23</td>
<td>ACME Data Center</td>
<td>Ground Floor &gt; Comp. Production</td>
<td>in operation</td>
<td>-</td>
</tr>
<tr>
<td>16.10.28.24</td>
<td>ACME Data Center</td>
<td>Ground Floor &gt; Comp. Production</td>
<td>in operation</td>
<td>-</td>
</tr>
<tr>
<td>16.10.28.25</td>
<td>ACME Data Center</td>
<td>Ground Floor &gt; Comp. Production</td>
<td>planned</td>
<td>-</td>
</tr>
</tbody>
</table>

**Screenshot from i-doit.org for OpenCMDB**
New Devices

New Search

1. *  
2. NOT  
3. [inputlookup homepage]  
4. | fields host  
5. | dedup host  
6. | table host

2 events (11/26/18 10:00:00.000 PM to 11/27/18 10:30)

Missing Devices

New Search

1. | inputlookup homepage  
2. | where NOT  
3. | search *  
4. | dedup host  
5. | table host

4 results (11/26/18 10:00:00.000 PM to 11/27/18 10:30)

Events  Patterns  Statistics (4)

20 Per Page  Format  Preview

<table>
<thead>
<tr>
<th>host</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.106</td>
</tr>
<tr>
<td>192.168.1.107</td>
</tr>
<tr>
<td>192.168.1.108</td>
</tr>
<tr>
<td>192.168.1.109</td>
</tr>
</tbody>
</table>

host

mshedgewin12

DESKTOP-2ANBKHC
Percentage of Missing Devices

```plaintext
| inputlookup host
| where NOT
|   [search *
|     | dedup host
|     | table host ]
| stats count as Missing
| appendcols
|   [ | inputlookup host
|     | stats count as Total ]
| eval PercentMissing = (Missing/Total)*100
| table Total Missing PercentMissing

1 result (11/28/18 4:48:00.000 PM to 11/28/18 8:48:44.000 PM) No Event Sampling

<table>
<thead>
<tr>
<th>Events</th>
<th>Patterns</th>
<th>Statistics (1)</th>
<th>Visualization</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Events</th>
<th>Patterns</th>
<th>Statistics (1)</th>
<th>Visualization</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Total</th>
<th>Missing</th>
<th>PercentMissing</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>5</td>
<td>55.5555555555556</td>
</tr>
</tbody>
</table>
Search for Logs in the Past 30 Minutes

No Alert
Search for Logs in the Past 30 Minutes

Alert! No results found. Try expanding the time range.
Are you getting logs from every time?
Time Series with Moving Average

```
| index=main earliest=-24h |
| timechart count as Events span=1h |
| trendline sma3(Events) as avgEvents |
```

Events (241,113)
Time Series with Moving Average

```
| index=syswin  earliest=-3h
| timechart count as Events span=10m
| trendline ema3(Events) as avgEvents
```

8,885 events (11/28/18 5:10:59.000 PM to 11/28/18 8:10:59.465 PM)
Are you getting logs in a timely manner?
Log Delay by host

```
index=_internal earliest=-3h latest=-1h
| rename _indextime as IndexTime
| eval diff=IndexTime - _time
| convert ctime(IndexTime) as IndexTime
| eval diff=if(diff<0, "0", diff)
| table _time IndexTime host diff
| sort - diff
```
Log Delay by Event

sourcetype=bro*
ed | eval IndexTime= _indextime
ed | eval TimeStamp = _time
ed | eval delta = IndexTime - TimeStamp
ed | eval Raw = _raw
ed | where delta > 300
c | convert ctime(IndexTime) | convert ctime(TimeStamp) | table TimeStamp IndexTime delta host Raw | sort -delta

326 events (12/2/18 11:00:00.000 AM to 12/3/18 11:28:00.000 AM) No Event Sampling

Events (326) Patterns Statistics (326) Visualization

<table>
<thead>
<tr>
<th>TimeStamp</th>
<th>IndexTime</th>
<th>delta</th>
<th>host</th>
<th>Raw</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/02/2018 14:02:18</td>
<td>12/02/2018 14:09:36</td>
<td>438</td>
<td>192.168.1.100</td>
<td>Dec 2 14:02:18 192.168.1.100 Dec 2 19:02:23 raspberrypi BROIDS: 1543777342.804105 Fts29x3rAuDSTY88Gd 192.168.0.111 192.168.0.113 CMKarP1n9ngJHNeq3f HTTP 0 SHA1,MD5 application/xml - 0.000000 TF F5806 5806 00 F - 27032ff514e95d4f5226af0da2314d6 0845c109fd75414b72b377d6e81cd77bea131d0 - - -</td>
</tr>
<tr>
<td>12/02/2018 14:02:18</td>
<td>12/02/2018 14:09:36</td>
<td>438</td>
<td>192.168.1.100</td>
<td>Dec 2 14:02:18 192.168.1.100 Dec 2 19:02:23 raspberrypi BROIDS: 1543777342.804105 CMKarP1n9ngJHNeq3f 192.168.0.113 42672 192.168.0.111 2869 GET 192.168.0.111 /uploadhost/udhisapi.dll?content=uuid:17d9093c-9900-451e-830a-f5075f5218f5 - 1.1 Linux/3.10.105, UPnP/1.0, Portable SDK for UPnP devices/1.6.21 0 5806 200 OK - (empty) - - - - - - - Fts29x3rAuDSTY88Gd - application/xml 62 Linux/3.10.105v2c UPnP/1.0v2c Portable SDK for UPnP devices/1.6.21</td>
</tr>
<tr>
<td>12/02/2018 11:49:06</td>
<td>12/02/2018 11:56:24</td>
<td>438</td>
<td>192.168.1.100</td>
<td>Dec 2 11:49:06 192.168.1.100 Dec 2 16:49:10 raspberrypi BROIDS: 1543769350.854050 Cx32ui4nMIAkWkNHi 192.168.0.113 42492 192.168.0.111 2869 GET 192.168.0.111 /uploadhost/udhisapi.dll?content=uuid:17d9093c-9900-451e-830a-f5075f5218f5 - 1.1 Linux/3.10.105, UPnP/1.0, Portable SDK for UPnP devices/1.6.21 0 5806 200 OK - (empty) - - - - - - - Fi4NhZaJCnkp0nTMf - application/xml 62 Linux/3.10.105v2c UPnP/1.0v2c Portable SDK for UPnP devices/1.6.21</td>
</tr>
</tbody>
</table>
Other Metrics:

- Today’s usage vs license max
- SIEM Server resource usage
- Current and Archive log storage
- Alerts (triggered/unused, FP rate)
BUT... WHERE DO I EVEN START??
Um...

I have additional questions.
Craig Bowser
@reswob10
www.shadowtrackers.net
https://shmooconepilogue.com

January 21st 2019
9 AM to 9 PM

CFP coming soon