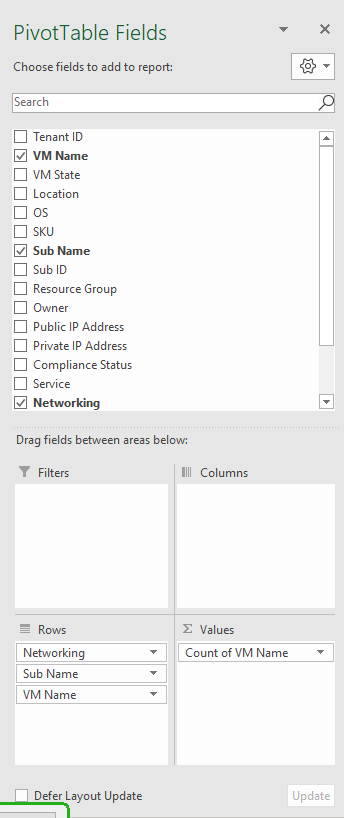
InfoSec agent healthcheck report process

1. Obtain the complete list from PowerBI - [~~CTP-Compliancev3 - Power BI~~](https://app.powerbi.com/groups/me/reports/a17b8a36-2040-471d-bd03-9dcd2445e1b9/ReportSectione037d69aeefdaa385b7f) [SRV CTP Compliance - Power BI](https://app.powerbi.com/groups/me/reports/294049e6-2ed9-4985-a569-6e33993c45e4/ReportSection51ec94fd4e3f9344cbc2)
   * Export data as an Excel file to use as the basis for the Health Check report
   * Filter only the required tenants & remove empty VM name rows
   * Create a fresh sheet and move columns
     + CL to A
     + R to B
     + CM to C
     + AP to D
     + AQ to E
     + CI to F
     + CJ to G
     + CK to H
     + BT to I
     + AR to J
     + AU to K
     + AS to L
     + N to M
     + P to N
     + Q to O
2. Rename first/only tab to **RawData**
3. Clear data filters
4. Filter only by **Qualys Out of compliance** (N) (7 days and not installed) and copy columns A-L on to a new tab. Name tab **Qualys**
5. Clear data filters
6. Filter only by **CarbonBlack Out of compliance** (M) (7 days and not installed) and copy columns A-L on to a new tab. Name tab **CB**
7. Clear data filters
8. ~~Filter only by~~ **~~Linux and CWP out of compliance~~** ~~(7 days and not installed) and copy columns A-L on to a new tab. Name tab~~ **~~CWP~~**
9. ~~Clear data filters~~
10. Filter only by **~~Windows and~~ SEP out of Compliance** (O) (7 days and not installed) and copy columns A-L on to a new tab. Name tab **SEP**
11. Clear data filters
12. Create another tab with the contents of each agent’s tab and **remove the duplicates.** Name tab **Complete List**
13. Keep only the **VM Name**, **Sub Name**, **Resource Group**, **Tenant ID**, & **OS** columns, in that order
14. Create a column named **Tenant**. If the **Tenant ID** column is **5b973f99-77df-4beb-b27d-aa0c70b8482c** then set the Tenant column to **EYGS**. If the value is **4667418b-7015-4ceb-b207-2193896769a8** then set the Tenant column to **EYDEV**. Ignore any other Tenant IDs.
15. Split the list into four separate lists (EYGS/Windows, EYGS/Linux, EYDEV/Windows & EYDEV/Linux) containing VM Name, Sub Name, Resource Group, Tenant ID, OS & Tenant. Export each grouping to a semicolon separated CSV file containing VM Name, Sub Name & Resource Group.
16. Open a Cloud Shell on each Azure environment. On each environment:
    * Upload the Windows & Linux CSV files
    * Copy the Windows list to List.csv and run TriggerHealthCheck.ps1
    * Run getLogs.ps1
    * Copy the Linux list to List.csv and run TriggerHealthCheckLinux
    * Run GetLogsLinux.ps1
17. On Log Analytics Workspace UKSPCTPCFMLAW04, run log query CBHealthcheck\_CL
18. Export results to CSV (all columns)
19. Open in Excel
20. Copy & paste all data to a new tab on the compliance sheet named QueryData
21. Copy headers from last week's sheet to this week's components (SEP, CWP, CB, Qualys)
22. Clear filters
23. Move AzureVMName\_s column of QueryData tab to Column G
24. Fill Columns M & N on SEP tab with
    * =VLOOKUP(B2,RawData!B2:O99999,14,FALSE)
    * =IFERROR(VLOOKUP(B2,QueryData!$G$2:$AJ$*<last row of query data>*,17,FALSE),"Script Did Not Run")
25. Fill Columns M & N on CB tab with
    * =VLOOKUP(B2,RawData!B2:O99999,12,FALSE)
    * =IFERROR(VLOOKUP(B2,QueryData!$G$2:$AJ$*<last row of query data>*,29,FALSE),"Script Did Not Run")
26. Fill Column M & N on Qualys tab with
    * =VLOOKUP(B2,RawData!B2:O99999,13,FALSE)
    * =IFERROR(VLOOKUP(B2,QueryData!$G$2:$AJ$*<last row of query data>*,17,FALSE),"Script Did Not Run")
27. Fill Columns O-Q on SEP, CB & Qualys tabs
    * =IFERROR(VLOOKUP(B2,QueryData!$G$2:$AJ$*<last row of query data>*,10,FALSE),"Script Did Not Run")
    * =IFERROR(VLOOKUP(B2,QueryData!$G$2:$AJ$*<last row of query data>*,23,FALSE),"Script Did Not Run")
    * =IFERROR(VLOOKUP(B2,QueryData!$G$2:$AJ$*<last row of query data>*,4,FALSE),"Script Did Not Run")
28. Create new tab named **Pivot**
29. Copy the four pivot table titles from previous week’s sheet
30. Create four pivot tables from each of the agent tabs using these settings



Windows EYGS – 391

Linux EYGS - 596

Windows EYDEV – 12

Linux EYDEV – 30

