CASE NOTE

AZURE MONITOR CUSTOM WORKBOOKS

risual

www.risual.com

MICROSOFT DEFENDER FOR CLOUD

The client makes extensive use of a security feature called Microsoft Defender for Cloud (MDfC), a product that reports on missing server patches. Virtual machines running in Azure report as healthy (fully patched), unhealthy (missing patches) or “not applicable” (failure to report e.g. switched off or a genuine problem). The team responsible for addressing security recommendations had no obvious way of identifying if computers were legitimately switched off or genuinely had a problem with the reporting agent software.

The Azure Monitor tool provides sample workbooks to present useful information in a very user-friendly way (e.g. tables, charts and graphs). However, the supplied samples do not always offer the data that you need. Hence, a custom workbook was developed to identify which virtual machines were running but had a problem reporting to MDfC.

PROVIDING IMMEDIATE IDENTIFICATION WITH OUR CUSTOM WORKBOOK

The custom workbook itself provided immediate identification of computers worth investigating, where re-installing the agent for instance provided a swift resolution. There was also great value in demonstrating how the custom workbook was developed and how it could be modified in future by the company's security teams.

The overall aim was to provide a dashboard that all support teams can use. Showing them how it was created empowered them to develop it further and create new ones if needed.

Microsoft plans to consider the client's workbook as a sample offering that may be offered to a general Azure audience with potential for something similar to be included in future MDfC versions.

If you enjoyed this story, or have an upcoming project in mind, please don't hesitate to contact us via **enquiries@risual.com** or 0300 303 2044. Alternatively, you can submit an enquiry here **Contact – risual**