Security of Domain Controllers Walkthrough Questions

Friday, December 3, 2021

1. What does the domain controller contain? What information is contained.

* Are there any updates/service packs required in the domain controller? If so, how these deployed? When do you update the hardware/server? Do you wait till when it is no longer supported or end of life?
* **Can you walk us through a domain controller on screen?**
* What operating systems are contained in AD?
* How many users can be deployed into a domain controller? (Scalability perspective)

1. Who else has access to the into the domain controller (outside of the active directory). Is it only the infrastructure team that has access?
2. Why are there the certain numbers of domain controllers in the AD as seen in the excel doc. Some domain controllers have 5, others have a varied number…why?
3. What happens when a domain controller shuts down? Is there a back-up.
4. What are the procedures to get a faulty domain back up and running? Is backup located within the Active directory or outside. Any defined SLAs?

* Are there regular back up of the primary domain controllers? Batch or real time?

1. What are the procedures taken to set up a domain controller?
2. What are the process for decommission a domain controller? What teams are involved? Is this documented?
3. When a domain controller is compromised, what alerts are received, time frame.