Walkthrough Brainstorm Questions

Tuesday, November 23, 2021

------------------------

1. **AD Management**

* What does the active directory management environment look like?
* Who are the main players involved?
* Understanding all the team members in the Active directory
* What are the policies they follow? Are the documented?
* Does Segregation of Duties exist in the AD environment?
* What are the SLAs that are being followed? Any KPIs reported to the senior management? What is being reported to senior management. The decks presented if meetings are scheduled on a quarterly basis.

1. **Active Directory Design/ Secure AD Boundaries**

* What is theAD design? Conceptual diagram.
* How many domain controllers are there?
* How is group policies managed? Are there several group policies? Are there separate group policies or are they inherited?
* Does segregation of duties exist for critical AD functions?

1. **Security of Doman Controllers?**

* What are some of the configuration settings?
* How are updates for Service Packs managed and deployed? (Change Management) Who signs off (approver)
* What are the change management process for policy settings? And what are the processes for making these changes?
* When the active domain shuts down, do you switch unto a backup domain controller? What measures are taken?
* How do you ensure the domain controllers are available and secure? Who is responsible?

1. **AD Administrative Practices**

* What are the different types of privileged users?
* What are the distinctions between the administrative account and non-administrative accounts? How are the activities performed in the system? How many accounts do these accounts have access to.
* What are the operations done by the privilege users? Are they tracked and logged?
* Do admin and non-Admin accounts share functions?
* Any concerns with admins using their accounts for non-administrative functions?

1. **Logging and Monitoring**

* What events are logged? Sign-ins? Etc. If failed attempts are repeated multiple times, are log failures recorded and identified?
* Are logs sent to Splunk? Understanding Splunk as a whole.
* Any concerns with the logging activities?
* What triggers log reviews? (Alerts) - Through email, phone calls etc. Walk us through an event that took place. Who gets alerted?
* What actions are taken to remediate alerts? Timeframe
* What corporate standards are being leveraged?