Data Requests for Active Directory

**AD Management**

1. Please provide evidence showing the documented process you undertake for setting up domain controllers and undertaking server post check to make sure server meets expectations. (They said it is tailored to enterprise policy)
2. Please provide the most recent AD stat sheet (excel) for December 2021 showing all the domain controllers, DCs, users, groups, computers, forestGPOs. Also provide query used to generate the AD excel stats sheet.
3. Please provide documented policies and procedures adhered to by your team to undergo management reporting (KPI/KRI).
4. Please provide any reporting performed and documented during any downtime and outages, and communication that occurred notifying responsible parties. Also provide the remediation that was performed to fix the outage.

**Secure AD Boundaries**

1. Please provide supporting document showing that only a one-way trust relationship was established between caremarkRX.net and MinClinic.local. Also provide evidence showing the security review performed by your team.
2. Please provide evidence showing the established domain trust relationships.
3. Please provide an updated architecture diagram of the active directory enterprise domain structure showing the domains and the sub-domains for each forest as well as additional domains.
4. Please provide document process taken when your team undergoes the process of shutting down a non-essential domain and approval process taken.
5. Please provide documented evidence of the default Group policy management leveraged by your team for individual domains, domain wide and the platform. Also provide any exceptions utilized for specific domains.
6. Please provide screenshots of the password configuration for admin accounts.
7. Please provide documentation of the change process performed by your team and include the QA testing performed, and approval by responsible parties.

**Security of Domain Controllers**

1. Please provide the archer policies, enterprise configuration, and change control procedures leveraged by your team.
2. Please provide the full list of all the antivirus and malware protection application installed on the domain controllers.
3. Please provide documentation showing the QA testing, approval and deployment performed when installing service packs and updates unto domain controllers.
4. Please provide the weekly vulnerability scans performed by your team, including the criticality assigned to each vulnerability, and remediation performed to fix issues identified.
5. Please provide documentation showing routine scanning performed by your team for checking availability of active domain controllers. For any issues identified, provide remediation performed.
6. Please provide a full listing of all the changes performed and documentation retained within ServiceNow.
7. Please provide defined policies and procedures adhered to by your team when ordering a new 3-year lease cycle for the domain controllers, servers and process undertaken when decommissioning a domain controller.

**AD Administrative Practices**

1. Please provide documentation of the process undertaken to grant access to admins and the approvals by responsible parties. (SNOW ticketing)

**Logging and Monitoring**

1. Please provide a full listing of all the logs received by your team. Logs should include failed sign-ins, account lockouts, log failures recorded.
2. Please provide the alerts received by your team, type of alert triggered, responsible part to remediate alert, and remediation performed to fix issue.
3. Please provide any defined SLAs leveraged by your team to address an incident/alert that is triggered, and the timeframe and escalation required to remediate issue.