Vulnerability Management Tips

- Identify manageable and unmanageable assets in your environment through scanners.
  - Managed assets – Which can be scanned by scanners.
  - Unmanaged assets – Which cannot be scanned by scanners, but scanners should be able to generate a few details in the dashboard. Asset IP, asset type, manufacture, model version number, etc. This provides greater visibility into the network environment.
- Review network access rules to identify what prevents the scanner from scanning assets based on access control.
- Rate severities of each vulnerability based on access from untrusted networks along with the asset value, proximity and access from high-value assets.
- Identify all accessible assets by an impacted system and review the exact access path and location.
- If assets can't be patched:
  - Isolate them.
  - Mitigate vulnerabilities by providing other means of protection (defense-in-depth) such as placing firewall, IDS, IPS, increased monitoring, increased access and authorization for users/analyst using it, continuous monitoring of IAM, applying workaround patches if available from trusted parties.
- Implement policy-based vulnerability management strategies to avoid the confusion of expectation vs requirement. One size doesn't fit all when it comes to security. Define policies for at least network infrastructure, networking devices, company-owned devices, applications, servers, DB servers, OSes, cloud-hosted servers and applications, VMs.