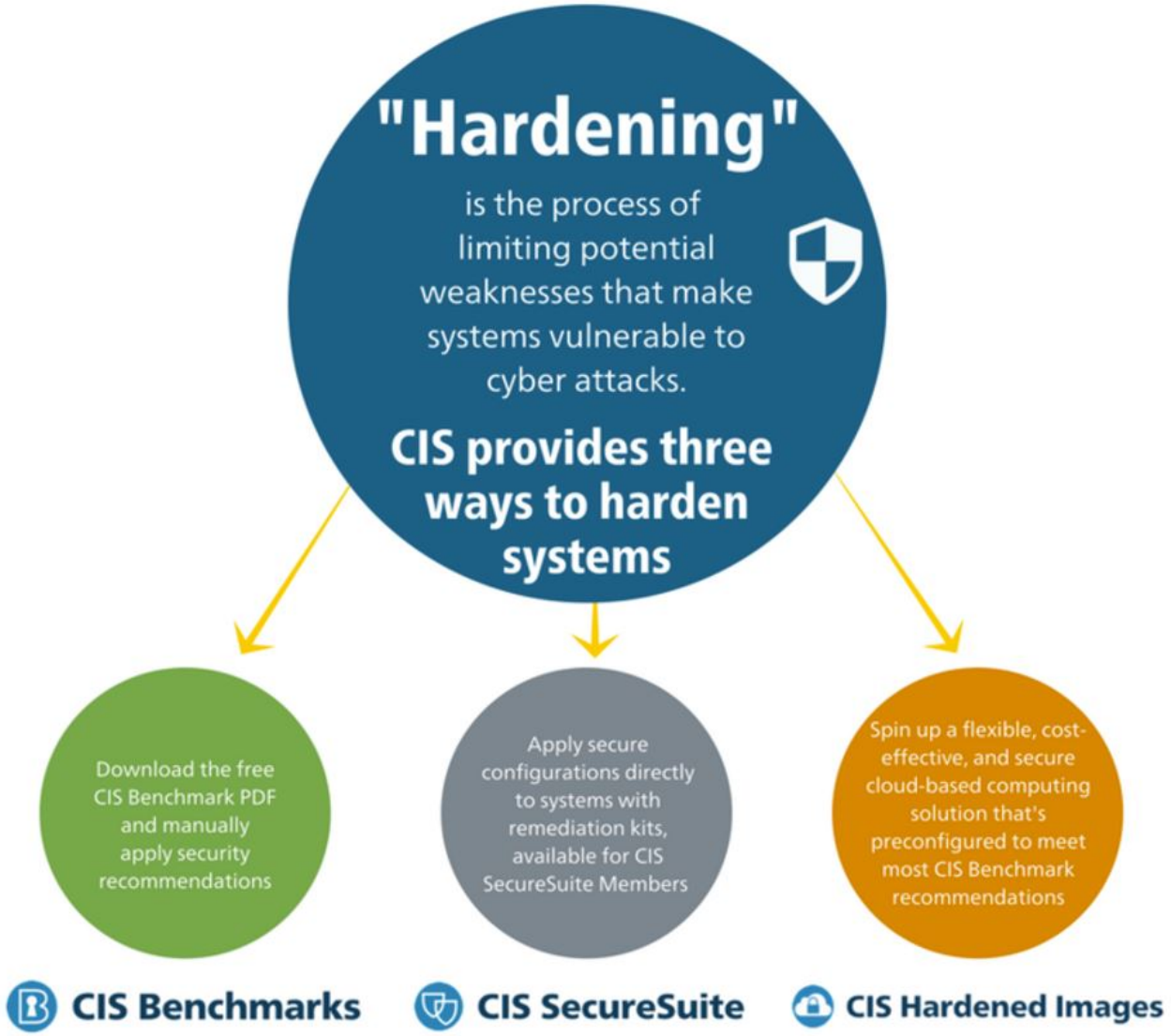
Operating System, Application and Network Hardening Resources

Information Technology is becoming more challenging these days, hence IT Security is a key area when it comes to Operating Systems, Applications and Networking.

The process of securing an operating system is referred to as “**hardening**” or at times as “**lock down**” It is important to an organization’s security because it reduces the chances of attack. Issues come up because various operating systems require different hardening processes within a data center. For example, a system administrator may have deep expertise in one operating system but may possess limited or even no expertise with the other operating systems. System administrators also have a task of ensuring that each server remains locked down consistently to avoid vulnerabilities.

Most of the IT Administrators will have difficulties finding the properly defined set of Hardening guides. To overcome the such issues, **Center for Internet Security (CIS)** has published well defined and detailed hardening guides to the public (**FREE**).

https://nvd.nist.gov/ncp/repository



With the above repository, you will get the change to download all the hardening guides on Windows OS, Mac OS, Linux OS, Applications, Network devices & etc.

For the ease of access, i have attached two common hardening guides as below;

- **CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.3.0**
- **CIS_Red_Hat_Enterprise_Linux_6_Benchmark_v2.1.0**