Peer Response

by Nkosana Mlambo - Thursday, 20 October 2022, 10:42 PM

Hi Kwok Wai, thank you for your post, I do agree with the sentiments you share about CVSS. We have been using CVSS for a number of years to tackle vulnerability management in IT environments, prioritising vulnerabilities based on their CVSS score and to some extent, CVSS has provided guidance and visibility on outdated systems that need to be patched, misconfigured systems, systems using default passwords, and systems merely running unnecessary services, or having open ports not required by a system. However, the issue with the CVSS system is the one size fits all perspective and will rate a business-critical system and a non-critical system with completely different functionalities and requirements the same way. To some extent, I believe the CVSS system can be improved by making it more customisable and automated and be used at an operational level and be used in conjunction with the SSVC system that can provide a risk-based approach. Do you think this would work as I think it might identify gaps and help provide a more holistic approach in tackling vulnerabilities and risks within an environment.