



Best Practices from a Qualys Customer













Paris

Thursday 23 January



Best Practices from a Qualys Customer

Once upon a time... More than a vulnerability scan program

-  #1 Computing a score for each scope creates positive competition between each region
-  #2 Some IT admins and managers have a part of their annual bonus calculated based on the score
-  #3 Some Business Units are not fairly assessed as scanning of all their IP addresses is not mandatory
-  #4 Creation of a fairplay score to have BU register more assets, but difficult to keep up-to-date
-  #5 Local teams don't always have the time to work on the service (ex : business value)
-  #6 Choose a popular and well-known programming language! (Python vs Ruby)
-  #7 Adapting our scripts took time
-  #8 Exploring and playing with the scanning profiles and report templates helps to find the ones we need
-  #9 We can't rely on these reports only as we need to communicate the VuDiP score
-  #10 Establish a trustworthy relationship with our OT contacts
-  #11 Communication (contents & format) to Directors and Managers is not to be neglected
-  #12 Invest time to properly delegate scanning rights (allowed scope, training)