Common Metric – Where to Start

Coverage - Knowing the systems that are scanned for problems

Open Critical – How many big problems there are

Number of Closed Vulnerabilities – Shows the program progress

The first one needs to be calculated from scanner data and asset inventory data.
Other two should be available straight from the scanners.
Mean Time to Resolve – Tells how long it takes from discovery to remediation
  - Will need to know date/time for when first time found and when remediated
Mean Time to Detect – How long is it taking to find the problems once they are published
  - Will need to know date/time for published dates and when first found
Exclusions – How many there are and which are approaching their expiry date
  - Most likely will need to track this manually (some tools do)
Bonus Metrics – Others that are helpful

• Vulnerability Reopen Rate – How many problems were closed, but come back
  • Will most likely need to track this manually

• Vulnerability Churn – New problems compared to closed problems. Is the program making headway?
  • Need closed problems and new problems numbers