Using CIS Controls with AIX

Contributed by Michael Felt

As an author of the AIX benchmark for CIS Security I have been reorginizing the benchmark - not to be a reflection of the command aixpert which is likely only understandable by AIX/UNIX/Linux administrators to one that follows the organization of the CIS Controls themselves.

There are a lot of organizations that are still committed to CIS Controls Version 7.1. However, earlier this year (2021) the newest version of CIS Controls Version 8 was released. With this new release the control numbers have changed greatly. Historically, CIS ised the order of the Controls as a means to focus cybersecurity activites performed by an organization - with the first 6 controls labeled "cyber hygiene". In version 7 CIS started a new method of guidance (while leaving the order of chapters largely intact). The new guidance was called Implementation Groups (IGs). FYI: In version 7.1 the Controls were still grouped by chapter order in three categories: Basic, Foundational, and Organizational.

CIS Controls v8 - It's not about the list

Starting with CIS Controls v8 implementaion is not following the list directly. Instead - you need to review all the controls and look at the recommended IG. Basically, IG1 should be included in any organizational cybersecurity activities. IG2 and IG3 are respectively, more stringent controls - where IG2 includes all of IG1, and IG3 includes all of IG2 and IG3.

Implementation Group or Benchmark Level

The benchmarks also have a differentiation based on Level. Roughly speaking, Level 1 are recommendations (remember CIS controls are not platform recommendations - they are controls (guidelines) that recommendations are meant to implement.) that are seen as easy to implement with minimal impact on platform operations or useability. Level 2 recommendations are seen as complex and/or could impact standard (better, read unsecured) practice.

Do not confuse IG with Label. Most Level 1 recommendations are IG1 and some are IG2 or IG3. However, there may be Level 2 recommendations that are still IG1.