CIS Center for Internet Security®

31 Tech Valley Drive
East Greenbush, NY 12061 USA
518.266.3460
media@cisecurity.org

STIG Benchmark and Hardened Image

- CIS has launched a new CIS Red Hat Enterprise Linux 7 STIG Benchmark and an associated CIS Hardened Image.
  - Organizations can now rely on CIS Benchmarks™ and CIS Hardened Images® for STIG compliance.
- The Department of Defense Cloud Computing Security Requirements Guide (aka DoD Cloud Computing SRG, ver 1, Rel 3) specifically calls out CIS Benchmarks as being acceptable in place of a STIG.
  - https://www.cisecurity.org/cis-hardened-images/ato-on-aws/
- Feedback is that many organizations still need to align with STIGs, so we developed this initial CIS STIG Benchmark which we used to create corresponding CIS STIG Hardened Images. We plan to continue to expand coverage accordingly based on additional feedback from our stakeholders.
- The CIS Red Hat Enterprise Linux (RHEL) 7 STIG Hardened Image reflects the CIS Benchmark STIG profiles. This profile encompasses the existing RHEL 7 Level 1 and Level 2 profiles mapped to STIG recommendations as applicable. To further expand coverage specific to STIG recommendations, a third profile was added. As a result, when customers are applying CIS Benchmarks and need to be STIG compliant, they'll be able to apply the Level 3 profile and address the gaps quickly.
- AWS has released their own STIG Amazon Machine Images (AMIs) for Windows.
  - CIS will have STIG CIS Hardened Images for Red Hat Enterprise Linux.
- Cloud customers clearly see the value in CIS Hardened Images. Our userbase in the AWS marketplace has grown by more than 80% in 2019.
- Key components of ALL Hardened Images:
  - Every CIS Hardened Image includes a CIS-CAT® Pro report showing conformance to the CIS Benchmark, as well as an exception report showing configurations that cannot be applied in the cloud.
  - CIS updates Hardened Images every month to address patching and vulnerabilities.