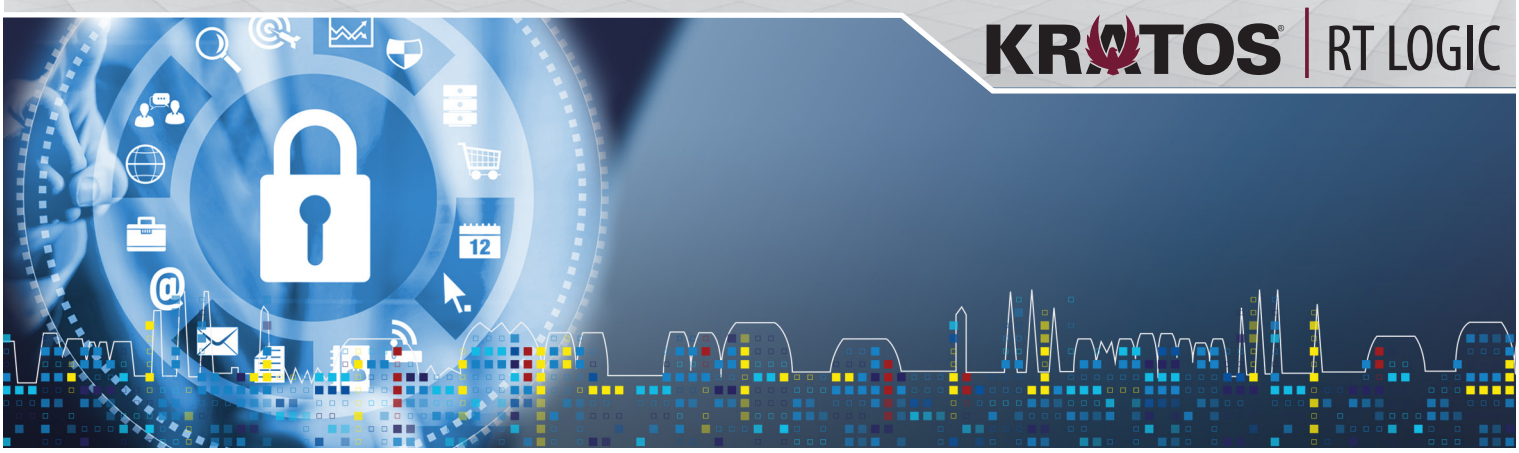
OS IA Hardening



Kratos RT Logic understands the importance of Information Assurance (IA) system hardening to our government and commercial customers, as well as the challenges associated with adhering to security requirements in an operational environment. We provide a set of common baseline operating systems (e.g., openSUSE, Red Hat® Enterprise Linux®, CentOS, Arch Linux®)that are fully patched and maintained quarterly in accordance with DISA Security Technical Implementation Guide (STIG) hardening requirements for the operating system (OS) and common applications: Apache, and Firefox.

Experience

Kratos RT Logic has an extensive portfolio of proven project performance, executing IA hardening on more than 50 customer programs in accordance with DISA STIG guidelines. Our mature IA hardening process is designed to ensure that customer security requirements are met on-time and on a firm-fixed-price budget. Performing operating system (OS) hardening and installing OS patches on operational SATCOM equipment can sometimes introduce unexpected changes to the system that have a negative impact on mission application functionality or performance. Troubleshooting such issues can be difficult in an operational environment and may require recompilation of mission application source code, firmware, or device drivers to correct.

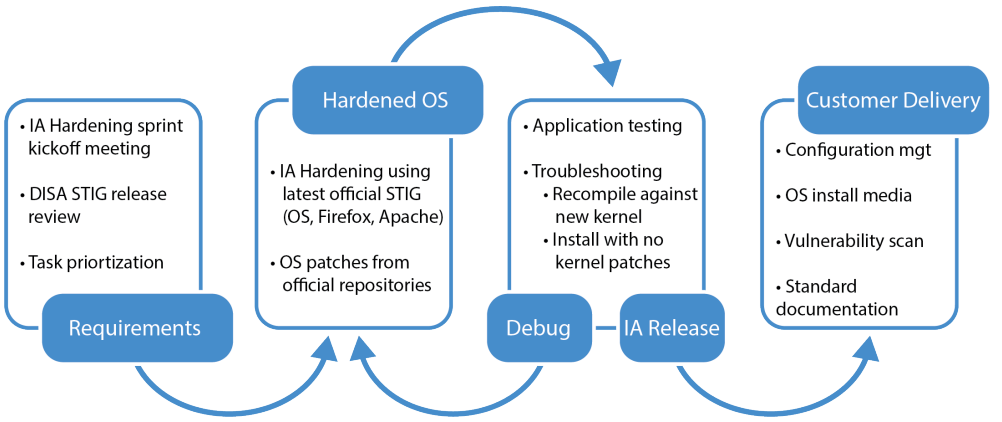


Figure 1: Kratos RT Logic OS Hardening Process

After the quarterly DISA STIGs are released, Kratos RT Logic completes the following for each supported OS:

- Implement OS, Firefox, and Apache STIGs
- Install all patches from official OS repository
- Run vulnerability scans such as Tenable™ Nessus / Assured Compliance Assessment Solution (ACAS)
- Complete quarterly IA hardening documentation
- Generate formal IA OS Quarterly Release
- Conduct application checkout testing by project

Based on the current DISA Release dates, following is a notional Kratos RT Logic IA Release schedule:

DISA STIG Release	DISA Release Date	Kratos RT Logic IA Documentation (~1 Month)	Application Testing (~1 Month)	Kratos RT Logic IA Release Ships / Available for Electronic Delivery
17Q4	10/27/17	Late Nov	Late Dec	Late Jan
18Q1	01/26/18	Late Feb	Late Mar	Late Apr
18Q2	04/27/18	Late May	Late Jun	Late Jul
18Q3	07/27/18	Late Aug	Late Sep	Late Oct
18Q4	10/26/18	Late Nov	Late Dec	Late Dec

Each quarterly IA hardening effort begins with an internal kick-off meeting to review requirements and official changes to applicable DISA STIGs. For each supported operating system, Kratos RT Logic IA Engineers identify the OS patches that are available from the official repositories. We also conduct a risk assessment to identify patches that may have a negative impact on mission application functionality.

Kratos RT Logic IA Engineers harden the OS per DISA STIGs using automated tools such as proprietary Kratos RT Logic hardening scripts, ACAS, and Nessus, as well as manual processes and procedures, to ensure STIG and Information Assurance Vulnerability Management (IAVM) compliance. We then install the mission application(s) on the hardened system and test in our lab environment using a library of automated test scripts (e.g. TestStand and shell scripts) along with manual test procedures as needed to perform mission application testing. When necessary, Kratos RT Logic IA engineers engage mission application software engineers to help troubleshoot and correct any IA/OS patch induced errors. Following the completion of the test/resolve phase, we finalize installation media and documentation, check all artifacts into our configuration management system, and deliver the complete hardened solution as a formal quarterly release.

Value of OS Hardening as a Service

Our mature IA hardening process provides consistent IA hardened OS updates on a quarterly basis. Our centralized approach to OS hardening and mission application testing results in cost-savings achieved through process efficiencies and economies of scale.

Standard tools ensure customer requirements are met and baselines maintained:

- DISA STIG Viewer (latest version available from DISA site)
- ACAS/Nessus (latest version available via vendor site)

Standard Document Formats and Deliverables feed into customer Risk Management Framework (RMF) process:

- IA Version Description Document – includes Operating System (OS), Security Technical Implementation Guide (STIG), and Vulnerability Scanner version details
- Vulnerability Scan Results – includes annotated findings with technical explanations in standard Nessus format
- Installation Instructions
- DISA STIG Report – DISA STIG viewer standard format and annotated Excel spreadsheet

Customer Experience

Each quarter the customer will receive physical and/or electronic delivery of the latest hardened OS and associated documentation. Customers have multiple options for applying the hardened OS to their systems:

- Complete OS Installation
  - This is a 'start from scratch' clean installation of the system that requires reinstalling all applications and reapplying all configurations
  - This will fully patch and update the system with the latest DISA configuration requirements
- Patch Only Installation
  - Patches the system with the latest operating system updates while preserving the installed applications and their configurations
  - Does not add new hardening or change any DISA STIG hardening that is already present on the system
- No Kernel Patch Only Installation
  - Patches the operating system with latest updates not including updating the kernel
  - Does not add new hardening or change any DISA STIG hardening that is already present on the system

Kratos RT Logic provides scripting tools for the customer to use to backup user files and configurations prior to doing the update, then restoring the files and configurations after the update.