Information Assurance (IA) System Hardening

RT LOGIC
A KRATOS Company

RT Logic understands the importance of Information Assurance (IA) System Hardening for our government and commercial customers, as well as the challenges associated with adhering to security requirements in an operational Satellite Communications (SATCOM) environment. To help our customers meet their security needs, RT Logic offers optional factory IA System Hardening services for all new equipment purchases, as well as a retro-fit upgrade service for existing customer-owned RT Logic equipment that is deployed operationally.

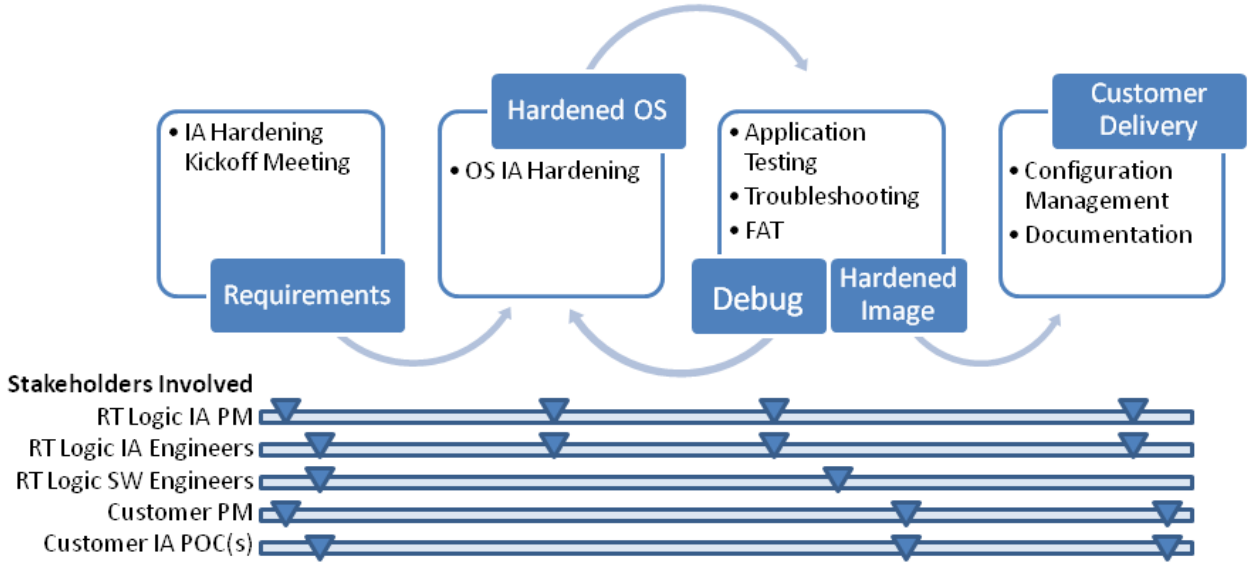
Installing Operating System (OS) patches and service packs in an operational SATCOM environment can sometimes introduce unexpected changes to the system that have a negative impact on RT Logic application functionality or performance. Troubleshooting such problems can be difficult in an operational environment and may require recompilation of application source code, firmware, or device drivers to correct.

RT Logic IA engineers are experienced at performing IA system hardening of Microsoft Windows (2K8/2K3/7/2000/NT/XP) and Linux (RHEL, SLES)-based RT Logic systems in accordance with Department of Defense, Intelligence Community, and Civilian standards, such as DISA, DIACAP, DSS, NIST, NISPOM, and DCID. Our IA Process can be tailored to meet customer-specific requirements, such as Tactical Test Procedures (TTP), Standard Operating Procedures (SOPs), and Site Security Plans (SSP).

Our mature IA hardening process is designed to ensure that customer security requirements are met on-time and on-budget, with verification of no impact to application functionality or performance. Each IA hardening effort is assigned a Project Manager and Project IA Engineer for the duration of the project who serve as the primary customer points of contact.

Our Process

Each project is entered into RT Logic's IA Project Tracking Database and begins with a thorough review of the existing customer system architecture, OS & application versions, and IA security requirements. An IA ticket is used by RT Logic IA engineers to document requirements and is routed to RT Logic engineering for review of application-specific requirements, such as: partition scheme, file system type, required packages, required services, and ports. RT Logic IA engineers then identify available OS patches and service packs, discuss them with RT Logic software engineers, and conduct a Risk Assessment in order to identify any patches which might have a negative impact on application functionality. Results of the Risk Assessment are shared with the customer, along with a recommended course of action. The test environment is then configured to ensure system compatibility and the base OS is installed.



Process Step	Description
IA Hardening Kickoff Meeting	1. A ticket used to gather customer IA requirements 2. Document IA Hardening Standards and Requirements 3. Document application requirements, packages, ports 4. Analyze available OS patches & service packs 5. Perform patch analysis & risk assessment
Operating System IA Hardening	1. Configure test environment 2. Install base Operating System (Windows, SLES, RHEL) 3. Harden OS per appropriate standards 4. Run automated scans and generate IA reports 5. Supplemental reports
Application Testing	1. Configure Test Environment 2. Perform functionality/regression tests 3. Troubleshoot as needed 4. Document Test Report
Configuration Management & Documentation	1. Revise IA documents as needed 2. Check hardened image into Configuration Management 3. Burn images to DVD 4. Send IA documents to customer for review 5. Final delivery to customer

RT Logic IA engineers harden the OS per customer standards (e.g., DISA, DSS, NIST, DCID, etc.) using automated tools such as DISA STIG Viewer, Retina, proprietary RT Logic scripts, and other SCAP-compliant tools. All processes and procedures have been internally vetted to ensure STIG and IAVM compliance. The hardened image is tested in cooperation with both the RT Logic IA engineers and the RT Logic software engineers for application functionality, system regression tests are performed, and if any errors exist, they are corrected on the spot as needed. Finally, the hardened image and documentation are finalized, entered into configuration management, and delivered to the customer.

Features

RT Logic's Information Assurance System Hardening service provides the following features and benefits:

- Performing IA system hardening in-factory, during system development, reduces costs
  - Security requirements are integrated into the development process
  - IA requirements are integrated into Factory Acceptance Test
  - Additional cost savings can be achieved through efficiencies gained when hardening multiple RT Logic platforms concurrently on the same purchase order.
  - Proactive IA system hardening is available as recurring service with quarterly or bi-annual deliveries of IA hardened images and updated IA reports
    - Ensures on-going customer security requirements are met in accordance with customer procurement strategies
    - Guarantees RT Logic IA engineers are resourced to meet customer needs
- IA project database Project Tracker, standard IA milestones, and timelines
- Standard document formats and deliverables
  - DISA STIG Report: STIG (Application/OS) results in VMS and xlxs format
  - Retina Reports: Vulnerability summary in standard vendor format
  - RT Logic Supplemental IA Hardening Reports: Elaboration of findings status
- Standard tools ensure customer requirements are met and baselines maintained
  - DISA STIGs (latest quarterly release via DISA FSO)
  - Retina (latest version available via vendor site)

Pricing

IA System Hardening is currently available as a T&M or hybrid FFP/T&M contract. Contact RT Logic Sales for more information.

12515 Academy Ridge View Colorado Springs, CO 80921, U.S.A.
Tel: 719.598.2801 Fax: 719.598.2655
www.rtlogic.com

RT LOGIC
A KRATOS Company