Secure Host Baseline

What is a Secure Host Baseline?

A Secure Host Baseline (SHB) is a pre-configured and security hardened machine-ready image that contains an organization's common Operating Systems (OS) and application software. SHB images are developed with the latest relevant standards and policies which include a layered security architecture enabling the implementation of best practice mitigation strategies to counter cyber threats.

An SHB image can be generated for any OS and common application software used by an organization. The image can be deployed across an office's host systems to include desktops, laptops, servers, tablets, and mobile devices. This provides administrators with a common core operating picture that makes it easier to identify and isolate anomalies. An SHB simplifies the implementation of robust security practices and technologies such as Application Whitelisting, Host Intrusion Prevention Systems (HIPS), Enhanced Experience Mitigation Toolkit (EMET), and other anti-exploitation capabilities. It also ensures that the security features of each host residing on a network are consistent with the organization's security policies and directives.

Advantages of Secure Host Baseline

In addition to reducing security risks, building an SHB image lowers the overall cost of managing a network. The development process takes advantage of economies of scale by leveraging the expertise of government and vendor communities to establish the baselines and coordinate testing and production. External issues such as licensing and distribution rights are also worked out at high levels by legal and policy staff to pave the way for deployment of SHB.

By providing common baselines and generating criteria for enterprise licensing initiatives, SHB also accelerates implementation of other efficiency strategies. Within the Department of Defense (DoD), some examples include Single Security Architecture (SSA), Security Automation, Secure Configuration Management (SCM), Continuous Monitoring (CM), and Enterprise Software Initiative (ESI).

Challenges of Secure Host Baseline

In order to be successful in implementing SHB, organizations must be prepared to provide continual updates for all supported baseline Operating Systems and application software for maintenance and sustainment purposes. SHB deployment must be aligned with other IT efforts and timelines and accepted throughout the organization. Longer term, organizations must manage lifecycle and end-of-life timelines for OS and applications to ensure that the security features remain current.

SHBs for the DoD, the military services, and other government organizations are currently in various stages of development. For information on the DoD's SHB initiative, consult the DISA site listed below.

- **Defense Information Systems Agency (DISA)**
  Security Technical Implementation Guides (STIG)
  http://iase.disa.mil/stigs

Other Resources for Security Guidelines

- **National Institute of Standards and Technology (NIST)**
  U.S. Government Configuration Guidelines (USGCB)
  http://usgcb.nist.gov/

  National Checklist Program (NCP)
  http://www.nist.gov/itl/csd/scm/ncp.cfm

  Security Content Automation Protocol (SCAP)
  http://scap.nist.gov/
- **National Security Agency (NSA)**
  Configuration Guides
  http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/
- **National Information Assurance Partnership (NIAP)**
  Protection Profiles (PP)
  http://www.niap-ccevs.org/pp/

Disclaimer of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

Contact Information

Industry Inquiries
410-854-6091
bao@nsa.gov

USG/IC Customer Inquiries
410-854-4790

DoD/Military/COCOM Customer Inquiries
410-854-4200

General Inquiries
NSA Information Assurance Service Center
niasc@nsa.gov