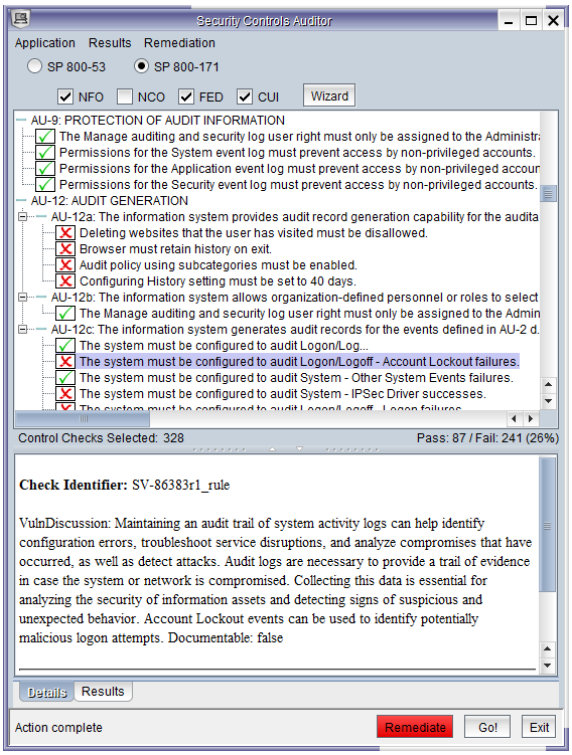
ThreatGuard

Security Controls Auditor

Security controls define administrative and technical safeguards and countermeasures to protect information systems from attack. The controls help protect the confidentiality, integrity, and availability of information. The National Institute of Standards and Technology (NIST) maintains a comprehensive set of controls for the Federal Government in their Special Publication 800-53. They recently released similar and more accessible guidance for nonfederal organizations in Special Publication 800-171. This new guidance focuses on protecting Controlled Unclassified Information (CUI) when the information does not reside on government systems. 800-171 introduces a mechanism called "tailoring" that enables nonfederal organizations to select a subset of 800-53 controls appropriate to their needs. Tailoring does not diminish the level of protection but rather simplifies the implementation of the guidance.



The Department of Defense (DoD) now requires all prime and subcontractors to implement 800-171 (defined in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. NASA and the GSA have similar requirements for contractors. While implementing the 800-171 guidance is a great idea for any organization, it is no longer optional for contractors who handle CUI.

ThreatGuard's Security Controls Auditor (SCA) product reduces the time required to audit and remediate baseline configurations of computer systems from over 8 hours per computer when done manually to less than 2 minutes with 100% accuracy. SCA processes automated configuration guidance from the federal government (USGCB) and the DoD (STIGs) and maps the rules to the respective NIST controls.

SCA will save you time and money and is easy to use with features designed for efficiency and simplicity.

Key Features:

Configuration Remediation, Undo, & Restore
- Automatically modifies local configuration and security settings to address any discrepancies
- Perform remediation undo of individual rules or full system restore using multiple restore points
- Manual remediation instructions included for each rule
- Perfect for creating and managing baseline configurations

Includes DoD and NIST Security Content Automation Files
- Assessment engine supports Security Content Automation Protocol (SCAP) v1.2 and below
- Provides runtime notes, allowing auditors and security engineers to validate assessment decisions

Security Reporting & Data Export
- Included 800-53 and 800-171 reports suitable for printing and emailing
- Reports timestamped to provide historical record of configuration status
- Option for exporting results to XML for import into spreadsheet or other system

Architecture & Supported Platforms
- The product runs on Microsoft Windows desktop and server computers
- Automated update system keeps application and assessment content current
- Requires Java Run-time Environment 1.5x or greater (embedded 1.8x included)
- Can be installed locally or run from thumb drive or other removable media