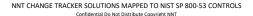
NNT CHANGE TRACKER SOLUTIONS MAPPED TO NIST SP 800-53 CONTROLS **Control Family Key Security Controls** Security Control Highlights NIST 800-53 Supplemental Guidance Precis How does NNT Change Tracker™ Gen 7 R2 satisfy the requirement? AC-3 ACCESS ENFORCEMENT, AC-6 ACCESS CONTROL AC-7 Enforces a limit of consecutive invalid logon attempts by a user during Contemporary Operating System platforms provide support for detailed security policy settings covering LEAST PRIVILEGE, AC-7 UNSUCCESSFUL ATTEMPTS, AC-12 SESSION a defined time period and automatically locks the account/node for a Password and Account Lockout Policies but these must all be set correctly and enforced. NNT is a LOGON ATTEMPTS. AC-8 SYSTEM USE TERMINATION defined time period when the maximum number of unsuccessful attempts is Certified CIS Vendor and as such, accurately delivers the industry-standard configuration hardening **NOTIFICATION, AC-9 PREVIOUS LOGON** exceeded AC-12 This control addresses the termination of user-initiated guidance form the CIS Benchmarks. This means you are assured of always having the latest expert (ACCESS) NOTIFICATION, AC-11 SESSION loaical sessions configuration settings to minimize your organizations attack surface. LOCK, AC-12 SESSION TERMINATION, AC-AT-1 SECURITY AWARENESS AND TRAINING AT-1 SECURITY AWARENESS AND **AWARENESS AND** Security awareness techniques can include, for example, displaying posters, See https://www.newnettechnologies.com/sans-institute-posters-summaries.html TRAINING POLICY TRAINING POLICY offering supplies inscribed with security reminders, generating email advisories AU-2 AUDIT EVENTS, AU-3 CONTENT OF AU-2 AUDIT EVENTS Audit events can include, for example, password changes, failed logons, or Configuration of a comprehensive audit policy is key - get it right and you will capture a forensic audit-**AUDIT AND AUDIT RECORDS, AU-6 AUDIT REVIEW,** failed accesses related to information systems, administrative privilege trail of user activities suitable for pre-empting an attack and for reconstructive forensic analysis post-**ACCOUNTABILITY** ANALYSIS, AND REPORTING, AU-7 AUDIT breach. Get it wrong and you will miss crucial events and likely be swamped with spurious log data. NNT usage, PIV credential usage, or third-party credential usage REDUCTION AND REPORT GENERATION. provide Configuration Remediation Kits to automatically set a NIST Auditor-class audit policy on all **AU-8 TIME STAMPS. AU-9 PROTECTION** platforms, backed with Certified CIS reports to continuously validate and enforce adherence. Note: NNT OF AUDIT INFORMATION Log Tracker™ can also be employed to analyze and backup logs. CA-2 SECURITY ASSESSMENTS. CA-7 CA-2 SECURITY ASSESSMENTS, CA-7 CA-2 Security assessments: ensure that information security is built into SECURITY Change Tracker™s built-in NIST 800-53 report assesses the configured state of your IT estate for organizational information systems; identify weaknesses and deficiencies compliance with the key NIST Security Controls to give a simple percentage score with clear remediation ASSESSMENT AND early in the development process; and ensure compliance to vulnerability guidance where non-compliance highlighted. Thereafter, Change Tracker™ provides real-time **AUTHORIZATION** mitigation procedures CA-7 The terms continuous and ongoing imply that monitoring of core configuration settings covering installed software, running processes, services and organizations assess/analyze security controls and information securitystartup states, registry keys, user accounts, audit and security policy, open network ports and the overall related risks at a frequency sufficient to support organizational risk-based integrity of the file system. decisions CM-2 BASELINE CONFIGURATION, CM-3 CM-2 BASELINE CONFIGURATION, CM. Baseline configurations serve as a basis for future builds, releases, and CONFIGURATION As well as the pre-built NIST compliance reports, any device being monitored can have its configured changes to information systems. Baseline configurations include state captured as a dynamically-generated Baseline Report, providing a Point-in-Time record to compare MANAGEMENT information about information system components (e.g., software packages with other devices or future points in time. CONFIGURATION SETTINGS. CM-7 LEAST SETTINGS installed; current version numbers/patch information on operating systems/applications & configuration settings/parameters). Maintaining For Change Control, Change Tracker™ utilizes a unique control systems known as 'Closed Loop Intelligent baseline configurations requires creating new baselines as organizational Change Control', literally learning which changes within your environment are normal, applying threatinformation systems change over time. based logic to the automation of change approvals. CONTINGENCY CP-1 CONTINGENCY PLANNING POLICY CP-1 CONTINGENCY PLANNING POLICY Backups, Disaster Recovery planning, resources and facilities PLANNING IDENTIFICATION & IA-1 IDENTIFICATION AND IA-1 IDENTIFICATION AND Identity Management and Authentication see Web: http://idmanagement.gov AUTHENTICATION POLICY AUTHENTICATION POLICY **AUTHENTICATION** IR-4 INCIDENT HANDLING **IR-4 INCIDENT HANDLING** Change Tracker™ cuts out the 'alert fatigue' and 'change noise' associated with traditional integrity INCIDENT The organization employs automated mechanisms to support the incident monitoring systems like Tripwire®. By leveraging NNT FAST™ (File Approved-Safe technology) Cloud, file handling process. The organization correlates incident information and RESPONSE individual incident responses to achieve an organization-wide perspective changes are automatically validated using an authoritative file whitelist. This radically reduces the on incident awareness and response. incident response process by highlighting only genuinely suspicious activities. In addition, because Change Tracker™ identifies Who Made the Change, investigation tasks are greatly simplified.



All changes are captured and presented clearly for review and approval.

change profile

Change Tracker™ integrates with change management systems such as ServiceNow® to automate the

flow of approved planned changes, reconciling what actually changed with the expected approved-

The organization: (a) Employs automated mechanisms to schedule,

requested, scheduled, in process, and completed.

conduct, and document maintenance and repairs; and (b) Produces up-to date, accurate, and complete records of all maintenance and repair actions

MA-2 CONTROLLED MAINTENANCE

MAINTENANCE

MA-2 CONTROLLED MAINTENANCE

NNT CHANGE TRACKER SOLUTIONS MAPPED TO NIST SP 800-53 CONTROLS (Page 2 of 2) Security Control Highlights **Control Family Key Security Controls** NIST 800-53 Supplemental Guidance Precis How does NNT Change Tracker™ Gen 7 R2 satisfy the requirement? MP-2 MEDIA ACCESS, MP-5 MEDIA MP-2 MEDIA ACCESS, MP-5 MEDIA MEDIA Information system media includes digital media. Restricting access to digital media includes limiting access to design specifications stored on PROTECTION compact disks in the media library to the project leader and the individuals on the development team. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. PHYSICAL & PE-1 PHYSICAL AND ENVIRONMENTAL PE-1 PHYSICAL AND ENVIRONMENTAL The organization develops, documents, and disseminates a physical and ENVIRONMENTAL PROTECTION POLICY PROTECTION POLICY AND PROCEDURES environmental protection policy. PROTECTION PLANNING PL-1 SECURITY PLANNING POLICY PL-1 SECURITY PLANNING POLICY AND Security plans relate security requirements to a set of security controls and **PROCEDURES** control enhancements PERSONNEL SECURITY PS-1 PERSONNEL SECURITY POLICY PS-1 PERSONNEL SECURITY POLICY AND The organization develops, documents, and disseminates a personnel security **PROCEDURES** RISK ASSESSMENT RA-5 VULNERABILITY SCANNING Vulnerability scanning includes, scanning for patch levels, scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. can be baselined, including the installed version.

