NNT
SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

Security Through System Integrity Solution Brief

CIS CRITICAL CONTROLS BACKGROUND

The CIS Critical Security Controls have been formulated to provide clarity and guidance for the bewildering array of security tools and technologies, security standards, training, certifications, vulnerability databases, guidance, best practices and compliance mandates. The goal is to answer the fundamental questions regarding security:

- What are the most critical areas we need to address and how should an enterprise take the first step to mature their risk management program?
- Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals and guidance to measure and improve?
- Which defensive steps have the greatest value?

SECURITY THROUGH SYSTEM INTEGRITY: *DEFINED*

Security through System Integrity starts by ensuring the essential Critical Security Controls are in place to establish a solid security foundation.

Once the Critical Controls are operational, NNT leverages Intelligent Change Control technology to track and analyze changes to your systems' integrity using self-learning whitelisting technology and threat intelligence.

Finally, NNT uses dynamic baselining to ensure your systems align to the most up-to-date, secure, and compliant state possible based on checked, approved, and authorized changes.

CRITICAL SECURITY CONTROLS

The Critical Security Controls include:

- A defined inventory of authorized systems, software, and configurations
- A defined best practice policy for the hardened configuration of systems
- Real time system vulnerability monitoring
- Secure Policy Controls including Controlled use of Administrative Privileges

CIS Controls™

INTELLIGENT CHANGE CONTROL

Once the Critical Controls are in place, apply NNT's sophisticated, state-of-the-art Intelligent Change Control technology to track and analyze changes to the integrity of your IT systems based on contextual information and any associated risk.

Leverage self-learning whitelisting techniques along with threat and vulnerability intelligence to analyze changes and reduce change noise, which in turn significantly improves your ability to spot suspicious activity of any kind.

DYNAMIC POLICY & BASELINE MANAGEMENT

Finally, use NNT's dynamic baselining to constantly adjust your system Integrity to the most up to date, secure and compliant state based on checked, approved, and authorized changes as they occur.

Security through System Integrity - Made possible only with NNT

- Establish the foundational requirements for any successful security and compliance initiative using the essential Critical Security Controls.
- Improve your ability to spot suspicious activity by leveraging self-learning Whitelisting techniques combined with threat and vulnerability intelligence.
- Adjust your system integrity in real-time to the most up to date, secure and compliant state.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative. W: www.newnettechnologies.com E: info@nntws.com

Visit www.newnettechnologies.com for more information and trial software