Nanitor

Improve CyberSecurity

Center for Internet Security

Nanitor is a certified product vendor member of CIS

CIS® (Center for Internet Security, Inc.)

“A forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.”

Nanitor

Center for Internet Security

Multi-State Information Sharing and Analysis Center® (MS-ISAC®)

“The go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government.”

Nanitor

Center for Internet Security

The CIS Controls™ and CIS Benchmarks™

“The global standard and recognized best practices for securing IT systems and data against the most pervasive attacks.

These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals.”

Nanitor

Center for Internet Security

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

The CIS Benchmarks

Cisecurity.org,

Benchmark PDF example

Nanitor quick demo

Nanitor

Center for Internet Security

CERT/CC Research

“CERT/CC (the federally funded research and development center operated by Carnegie Mellon University) reports that nearly **99% of all intrusions resulted from exploitation of known vulnerabilities or configuration errors.**

Essentially, malicious intrusions are avoidable if companies adopt a strong security policy and adhere to regular ongoing vulnerability assessments and proactive remediation strategies”

Nanitor

Center for Internet Security

Nanitor