BIOMÉRIEUX

SCANRDI®

Cybersecurity by design

Your Ally in Advancing Quality

PIONEERING DIAGNOSTICS

CYBERSECURITY BY DESIGN

PROACTIVITY

- Development and maintenance of the SCANRDI® software is performed following a secure development lifecycle integrating mandatory security activities and in compliance with standards and guidelines such as 21 CFR part 11.
- A cybersecurity risk assessment is performed before each SCANRDI® software release to ensure safety, security, and privacy.
- Continuous upgrades are released for the SCANRDI® software, meaning the latest features and cybersecurity improvements are always made available to bioMérieux customers.

SURVEILLANCE

- The SCANRDI® platform is scanned for cybersecurity threats using an external reference tool. All vulnerabilities are assessed (impact/criticality) and corrected in a patch if necessary.
- A cybersecurity bulletin is issued internally.

SCANRDI® is a non-growth-based rapid microbial method (RMM). As it not only detects viable microbial cells that can be isolated using a broth or agar plate, but also VBNC* microorganisms, including stressed and fastidious microorganisms that may not be recovered by standard culture methods, SCANRDI® is more sensitive than growth-based methods.
The current software version for this system is SCANRDI® software V5.0.

EXPERTISE

- Whether at rest or in transit, bioMérieux enforces data protection by implementing security features following current standards such as role-based access control, malware protection, or backup and restore process.
- For every new SCANRDI® software release, penetration tests are performed by external companies to detect new vulnerabilities and threats.

*Viable But Non-Culturable.

How does SCANRDI® ensure compliance with the Highest International Standards?

Benefits	Requirements	SCANRDI® Features
Authentication & Authorization	Automatic logoff	The SCANRDI® software forces automatic logoff after a customizable period of inactivity.
	Authorization	The SCANRDI® software leverages Windows user rights management and built-in Software Accounts Authorization, which enables role-based access control. SCANRDI® software applications are designed to run in non-administrative operating system accounts to prevent tampering.
	Person Authentication	There are two levels of person authentication: • Operating system: authentication is performed through the local machine Windows password policy. • SCANRDI® software: person authentication is performed through the local software policy.
	Configuration of Security Features	The software authentication service can be configured (based on three levels) according to the security policy of the customer.
Availability	Network Controls	The SCANRDI® software implements network controls through Windows Firewall configuration, restricting traffic only to specific ports and services.
	Malware Detection/ Protection	Microsoft Windows Defender anti-virus software is installed by default on the system. Customers can also install their corporate anti-malware solution, and apply their own security policy.
Data	Classification(s) of Data Stored	The SCANRDI® software doesn't store or process any sensitive data, but it could eventually store personal data like usernames.
	Data Integrity and Authenticity	The system includes integrity monitoring features that alert on potential failures that could affect data integrity.
	Data Backup and Disaster Recovery	The SCANRDI® software system enables authorized users to perform manual data backups in an encrypted format and store them on a local drive. The system can be restored to a prior date with the assistance of bioMerieux support. *Audit trail backup is subject to a different process.
Audit	Audit Controls	Audit Trail records cannot be deleted, are stamped and can be exported.
	Regulatory Compliance	The SCANRDI® software is designed to support 21 CFR11 compliance.
Maintenance	System and Application Hardening	Cybersecurity risk assessments, penetration testing, static code security testing, vulnerability monitoring, and manual code review are performed. Vulnerabilities appropriately remediated as part of the secure SDLC to ensure the system and application are hardened appropriately according to Windows 10 STIG V1 standard.
	Cybersecurity product updates	SCANRDI® will receive updates as needed to remediate uncontrolled security risks.
	Third-party Components in Product Lifecycle Roadmaps	Software Composition Analysis is performed to facilitate SBOM generation and to identify libraries and third-party components utilized to ensure all components and libraries stay up to date.
Other	Security Guides	A detailed Product Security Technical Whitepaper is available for the SCANRDI® software
	Note	These features have been assessed for the SCANRDI® software V5.0, differences may apply in case of future releases.

bioMérieux S.A. • 69280 Marcy l'Étoile • France • Tel.: + 33 (0)4 78 87 20 00 • Fax: +33 (0)4 78 87 20 90
www.biomerieux.com