vicarius

SOLUTION OVERVIEW

NIS2 directive: How Vicarius vRx helps

Background

The NIS2 Directive raises the bar for cybersecurity across the European Union, extending mandatory requirements to a broader set of sectors and enforcing stricter obligations around risk management, incident reporting, and supply chain security. Organizations subject to NIS2 must move beyond checkbox compliance and build demonstrable, continuous security practices across their entire attack surface.

Challenges

NIS2 imposes significant obligations and heavy fines for non-compliance, yet ticking boxes alone does not translate into genuine security. The threat landscape has shifted fundamentally: vulnerabilities are now exploited within hours of disclosure, more than 130 new CVEs are introduced every day, and 80% of exploits are published before a CVE is even formally assigned leaving defenders with a structural 23-day blind spot.

Key implementation challenges include:

- Speed Crisis: Organisation's scan monthly while attackers exploit in minutes, creating a dangerous window of exposure.
- Accuracy Crisis: Traditional vulnerability tools generate overwhelming noise with over 95% of alerts estimated as false positives drowning security teams before they can act.
- Remediation Crisis: Most platforms stop at detection. Without a validated path from discovery to fix, 70% of security team time is consumed by triage rather than remediation.
- Compliance Complexity: Aligning NIS2 controls across multi-vendor environments and EU member-state interpretations demands a unified, audit-ready evidence trail.
- Incident Reporting: NIS2's strict notification timelines require real-time asset visibility and pre-built reporting workflows that many organisations lack.

Solution

Vicarius vRx is the first platform to continuously validate, prioritize, and remediate vulnerabilities at enterprise scale combining intelligence, agentic AI validation, and three distinct automated remediation methods (vPatch, vScript, vShield) in a single unified platform. Built on a unique intelligence engine, vRx ingests and normalizes data from any security scanner, enriches findings with live threat intelligence and orchestrates remediation through a closed-loop workflow of Detect → Analyze → Validate → Remediate → Re-Validate → Monitor.

vRx's vScore engine fuses CVSS, EPSS, KEV, threat intelligence and customer generated contexual data with contextual asset metadata to reduce false positives by 94–95%, enabling security teams to focus exclusively on vulnerabilities that pose real, validated risk. The AI Red Team module provides agentic exploit validation without production disruption, delivering proof of exploitability in minutes. When remediation is executed, Re-Validation confirms fixes actually work providing the audit-ready proof of closure that NIS2 enforcement will demand.

Supported by vRadar for passive and active discovery across network, cloud, container, and web application assets, CIS Discovery with 100+ benchmarks for compliance posture, and a GRC Rules engine for risk acceptance and governance policies, vRx delivers comprehensive NIS2 alignment across Article 21's core requirements.

Key benefits

Close the Remediation Gap

From detection to validated fix in one platform vPatch, vScript, and vShield cover every remediation scenario including zero-days and legacy systems.

95% Noise Reduction

vScore's contextual risk engine fuses CVSS, EPSS, KEV and Contexual data to eliminate false positives and focus teams on vulnerabilities that matter.

AI Agentic Validation

The AI Red Team verifies whether vulnerabilities are actually exploitable in your environment without disrupting production in minutes.

Continuous Discovery

vRadar provides passive discovery, web app, cloud, and container scanning for complete, real-time asset and vulnerability visibility.

Proof of Closure

Post-fix re-validation confirms every remediation worked, generating the audit-ready evidence chain NIS2 requires.

CIS + Compliance Reporting

40+ certified CIS benchmarks and compliance reports with the ability to schedule, export compliance evidence for regulators and auditors.

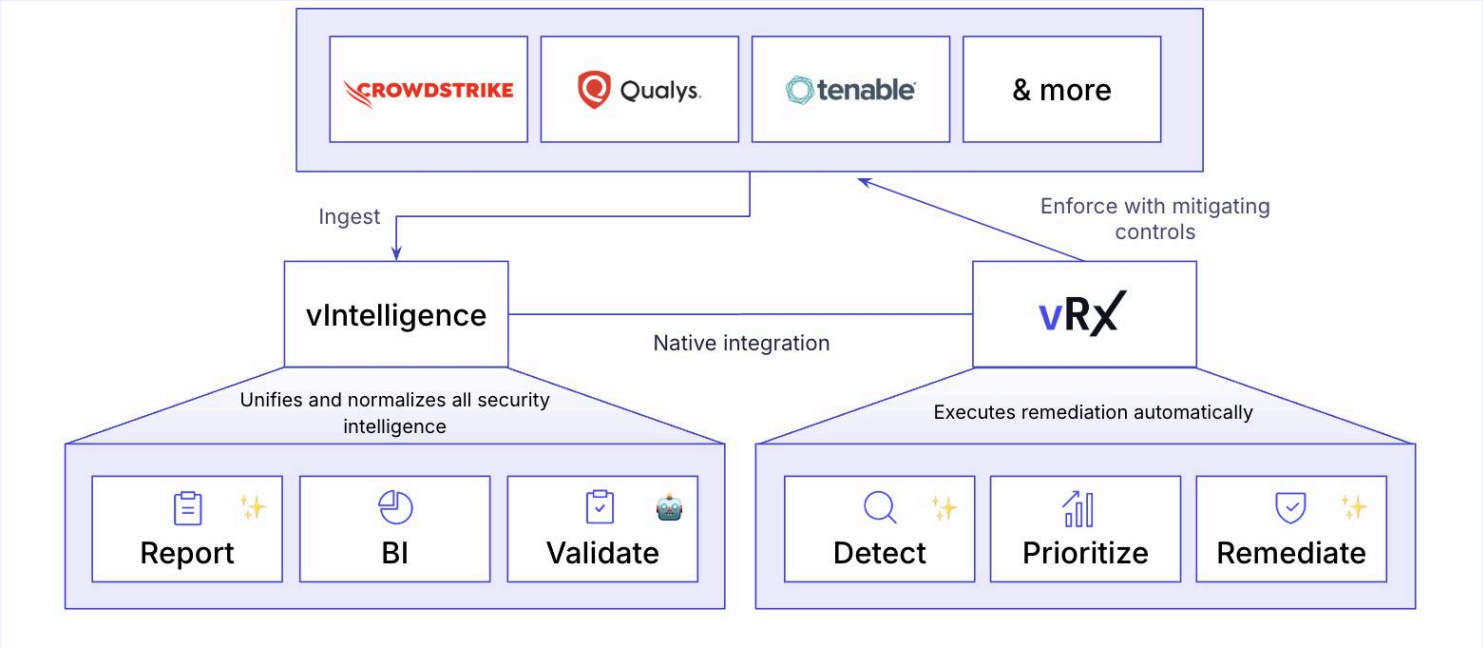
Enterprise Multi-Tenancy

ReBAC access control, SSO, MFA, and unlimited scalability support multi-site, complex enterprise and MSSP environments with sub-second updates.

GRC & Risk Governance

Built-in GRC Rules for risk acceptance, patch and software exclusions, and Remediation Policy enforcement align security operations with business risk appetite.

Platform Architecture



vRxi Platform Architecture Diagram Autonomous Exposure Management Ecosystem

Closed-Loop Remediation Workflow

1 Detect → 2 Analyze → 3 Validate → 4 Remediate → Re-Validate → 5 Monitor

Mapping Vicarius vRx Capabilities to NIS2 Directive Requirements

The table below maps the capabilities delivered by the Vicarius vRx platform to the requirements set forth by the NIS2 Directive under Chapter IV, Article 21:

Chapter IV, Article 21 Cybersecurity Risk-Management Measures	
NIS2 DIRECTIVE REQUIREMENT	How Vicarius vRx Helps
2(a) Policies on risk analysis and information system security	vRx's vRadar continuously discovers all assets including network devices, cloud workloads, containers, and web applications through agent-based, agentless, and passive scanning. The vScore engine enriches every vulnerability with CVSS, EPSS, CISA KEV, Customer generated context and MITRE ATT&CK context, applying Inventory Grouping (AI-driven, query-based) and asset criticality metadata to produce a contextual, continuously-updated risk picture. CIS Discovery runs 100+ benchmarks across operating systems and applications to assess configuration posture. Natural-language querying and customisable dashboards enable security teams to model and document risk policy decisions with full audit trails.
2(b) Incident Handling	vRx's closed-loop workflow (Detect → Analyze → Validate → Remediate → Re-Validate → Monitor) provides real-time detection and response capability. Event-driven and time-based Scan Policies trigger assessment automatically when changes occur. The AI Red Team validates exploitability in minutes, enabling rapid triage. vShield (virtual patching) can be applied immediately as a mitigating control while patches are prepared, dramatically reducing incident dwell time. Integration with ITSM platforms (ServiceNow, Jira, SysAid) and SIEM solutions via the Open API automates ticket creation and alert escalation, supporting NIS2's strict incident notification timelines.
2(c) Business continuity, backup management, disaster recovery, and crisis management	vShield (formerly Patchless Protection) uses memory-level mitigating controls to maintain application availability during patch gaps critical for high-availability systems where emergency patching would cause unacceptable downtime. Automated Remediation Policies (vPatch, vScript, vShield) with Ring Deployment enable gradual, controlled rollouts to minimise disruption across large estates. Re-Validation confirms every fix is effective before closure, preventing the recurrence that could trigger a business continuity event. GRC Rules for risk acceptance and exclusions allow organisations to formally document accepted residual risk within continuity plans.
2(e) Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	vRx addresses the maintenance and vulnerability handling dimensions of this requirement end-to-end: it covers the full vulnerability lifecycle from discovery through validated remediation across 20,000+ third-party applications on Windows, Linux, and macOS. Inventory Discovery ingests SBOM data (SPDX/CycloneDX), providing software composition visibility for supply chain acquisition decisions. The Enrichment Layer maps findings to MITRE ATT&CK, threat actors, and attack vectors, supporting structured vulnerability disclosure workflows. For the acquisition dimension, vRx's asset and software inventory provides the visibility needed to assess the security posture of newly onboarded systems. Compliance reports in CSV, PDF, and XLSX support auditor submission. Note: Organisations should complement it with SAST/DAST tooling to fully address the development dimension of 2(e).

Chapter IV, Article 21 Cybersecurity Risk-Management Measures	
NIS2 DIRECTIVE REQUIREMENT	How Vicarius vRx Helps
2(c) Business continuity, backup management, disaster recovery, and crisis management	vShield (formerly Patchless Protection) uses memory-level mitigating controls to maintain application availability during patch gaps critical for high-availability systems where emergency patching would cause unacceptable downtime. Automated Remediation Policies (vPatch, vScript, vShield) with Ring Deployment enable gradual, controlled rollouts to minimise disruption across large estates. Re-Validation confirms every fix is effective before closure, preventing the recurrence that could trigger a business continuity event. GRC Rules for risk acceptance and exclusions allow organisations to formally document accepted residual risk within continuity plans.
2(e) Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	vRx addresses the maintenance and vulnerability handling dimensions of this requirement end-to-end: it covers the full vulnerability lifecycle from discovery through validated remediation across 20,000+ third-party applications on Windows, Linux, and macOS. Inventory Discovery ingests SBOM data (SPDX/CycloneDX), providing software composition visibility for supply chain acquisition decisions. The Enrichment Layer maps findings to MITRE ATT&CK, threat actors, and attack vectors, supporting structured vulnerability disclosure workflows. For the acquisition dimension, vRx's asset and software inventory provides the visibility needed to assess the security posture of newly onboarded systems. Compliance reports in CSV, PDF, and XLSX support auditor submission. Note: Organisations should complement it with SAST/DAST tooling to fully address the development dimension of 2(e).
2(f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	The Re-Validation engine provides 100% post-fix verification confirming that every remediation has actually resolved the vulnerability rather than simply closing a ticket. vScore tracks risk reduction over time, enabling organisations to measure the effectiveness of their risk-management programme quantitatively. Reports & dashboards expose MTTR trends, SLA adherence, and exposure window metrics, and where vRxi's BI layer surfaces deteriorating trends or SLA breaches, the AI Chat Interface enables teams to identify the contributing controls gap and feed findings directly back into vRx remediation policies, completing the assess → identify gaps → update controls → re-validate loop 21(2)(f) requires. The vRx Maturity Model maps controls to NIST CSF 2.0, CIS Controls v8, and ISO/IEC 27001, providing a universal compliance translation layer. GRC Rules enforce risk acceptance and exclusion policies, creating a formal, documented governance framework.

Chapter IV, Article 21 Cybersecurity Risk-Management Measures	
NIS2 DIRECTIVE REQUIREMENT	How Vicarius vRx Helps
2(g) Basic cyber hygiene practices and cybersecurity training	CIS Discovery runs 100+ CIS benchmark checks across all major operating systems and applications, continuously assessing configuration compliance against hygiene standards including password policies, firewall settings, and service hardening. Multi-Tenancy with ReBAC (Relationship-Based Access Control), SSO, and MFA enforces least-privilege access across teams and asset groups. Automated Remediation Policies operationalise hygiene at scale, automatically patching or scripting fixes for high-risk misconfigurations. AI insights provides natural-language insights and scheduled reports enabling teams at all levels to understand and act on hygiene posture. Vicarius's Training & Workshops programme satisfies the cybersecurity training obligation directly: Customer and Partner Technical and Architect Training build team capability in vulnerability identification, prioritisation, and remediation policy, while hands-on Workshops, including Incident Response, Practical Scripting for System Hardening, and Purple Team exercises, provide the documented, structured training pathway required
2(h) Policies and procedures regarding the use of cryptography and encryption	vRx's CIS Discovery and compliance scanning detects encryption-related misconfigurations across operating systems and applications, identifying weaknesses such as deprecated cipher suites, insecure protocol configurations, and certificate issues. The vScript engine can execute custom remediation scripts to enforce cryptographic policy configurations including disabling weak protocols, configuring TLS settings, and applying registry-level cryptographic controls across Windows, Linux, and macOS endpoints at scale. All vRx platform data is secured with AES-256 encryption at rest and TLS 1.2+ in transit, with SOC 2 Type II certification providing independent verification.
2(i) Human resources security, access control policies, and asset management	vRx's Multi-Tenancy architecture implements ReBAC (Relationship-Based Access Control), a granular model where every user, team, and asset group relationship is explicitly governed. Administrators assign roles (Owner, Admin, Viewer) linked to specific asset scopes, ensuring users can only access and act on assets within their defined perimeter. SSO integration with Microsoft Entra ID, Okta, OneLogin, supports enterprise identity governance. SSO federation also enforces the human resources security dimension of 21(2)(i): when a user is deprovisioned in Entra ID, Okta, OneLogin, access to vRx is revoked automatically, ensuring that leavers, role-changers, and contractors lose access immediately without relying on manual offboarding processes. Inventory Discovery maintains a continuously-updated asset register covering software, hardware, SBOM components, and network devices, the authoritative asset inventory NIS2's asset management requirement demands. GRC Rules provide the governance layer above the technical controls, enabling organisations to document and enforce formal access control policies, defining least-privilege principles, acceptable use boundaries, and exception handling, creating the auditable policy framework 21(2)(i) requires alongside the technical enforcement vRx delivers.

Chapter IV, Article 21 Cybersecurity Risk-Management Measures	
NIS2 DIRECTIVE REQUIREMENT	How Vicarius vRx Helps
2(j) Use of multi-factor authentication, secured communications, and emergency communication systems	vRx natively supports Multi-Factor Authentication (MFA) as part of its Multi-Tenancy security stack, alongside SSO via SAML federation with major identity providers. The Open API provides complete, authenticated access to all platform entities, enabling integration with emergency communication and escalation workflows. All platform communications are encrypted via TLS 1.2+. The iPaaS Integration layer and native n8n workflow automation support automated alerts to Slack, email, and ITSM systems ensuring security teams receive validated, prioritised notifications through secured channels without alert fatigue.

About Vicarius

Vicarius is an Exposure Assessment & Vulnerability Remediation company. Founded in 2016 and headquartered in New York, Vicarius serves 1000+ customers across 70+ countries, protecting over 4 million digital assets and remediating millions of vulnerabilities. Recognised as a Niche Player in the 2025 Gartner Magic Quadrant for Exposure Assessment Platforms and as a Major Player in the IDC MarketScape for Worldwide Exposure Assessment Platforms 2025, Vicarius has established itself as a leading platform for organisations seeking to operationalise Exposure Management & vulnerability management at enterprise scale.
vRx comprising the vRxi intelligence engine and the vRx remediation platform working natively together is the first solution to close the entire remediation gap in a single product: from multi-vendor intelligence ingestion through agentic AI validation to automated, re-validated remediation with proof of closure. For organisations navigating NIS2 compliance, vRx provides the technical controls Article 21 demands.