Website Security & Uptime Monitoring

NIS2 Article 21 Compliance & Evidence Pack (EU 2022/2555)

portal.nordiccloud-demo.eu • Zero-Agent Live Scan • 2026-11-11 09:30:00 UTC • vioro.io

MONITORED SITE PLAN	TLS/SSL & HEADERS	SECURITY FINDINGS	LIVE FRONTEND SBOM
Compliance	**Valid**	**1**	**4**
Verified Site Ownership	HSTS: Yes, CSP: Yes	1 web exposure findings	9 external JS scripts

NIS2 ART. 21(2)(f)

Executive Summary & Outside-In Assessment Methodology

The Vioro website security and uptime monitoring platform, operated by Cyze AS (Norway) on European infrastructure, has supported businesses since 2024 with continuous outside-in security auditing. Vioro's approach is completely agentless and works without server software, CMS plugins, or access to private source-code repositories and internal configuration. Vioro inspects live websites over public HTTPS from an external perspective, focusing on what visitors' browsers load and what a potential attacker can observe across TLS/SSL certificates, browser security headers, email anti-spoofing, exposed files, leaked client-side credentials, live software inventories (SBOM), and availability. This report provides automated outside-in technical evidence supporting EU NIS2 Directive (2022/2555) Art. 21(2)(c), (d), (e), (f), and (h) and Implementing Regulation (EU) 2024/2690, complementing the organization's internal governance, incident reporting (Art. 23), and access-control policies.

SITE & OWNERSHIP

Monitored Site, Ownership Verification & Monitoring Authorization

Monitored Site: portal.nordiccloud-demo.eu
Report ID: 3d8b1f40-92c4-4e57-8a11-94c62b70e415 (Generated 2026-11-11 09:30:00 UTC)
Active Plan & Ownership: Compliance, Verified via DNS TXT / HTTP Token
Monitoring Authorization: Recorded on 2026-11-01 14:12:00 UTC (Statement 2026-11-v1)

NIS2 ART. 21(2)(h)

TLS/SSL Certificates, Browser Security Headers & Email Anti-Spoofing

- **TLS Certificate Posture**
  - Certificate Status: Valid (Cryptographic TLS certificate is trusted and within validity dates)
  - Certificate Issuer: Let's Encrypt (E6) (Certificate Authority that signed the site's public key)
  - Trust Chain Length: 3 certificates (Server leaf, intermediate CA, and root trust chain)
- **Browser Security Headers**
  - HTTP Strict Transport Security (HSTS): Yes (Instructs browsers to connect exclusively over HTTPS)
  - Content-Security-Policy (CSP): Yes (Browser policy restricting unauthorized script execution and XSS)
  - Clickjacking Protection (X-Frame-Options): Yes (Prevents external sites from embedding pages in hidden iframes)
  - MIME-Sniffing Protection (X-Content-Type-Options): Yes (Prevents browsers from executing non-script files as code)
- **HTTPS Redirect Hygiene**
  - HTTP-to-HTTPS Redirect Enforced: Yes (Unencrypted port 80 HTTP requests redirect to HTTPS)
  - Final Destination Uses HTTPS: Yes (Final landing URL after all redirects stays on encrypted HTTPS)
  - HTTPS Downgrade Protection: Passed, no downgrade (Encrypted HTTPS requests never redirect back to HTTP)
- **Domain & Email Anti-Spoofing**
  - Certificate Authority Authorization (CAA): Yes (DNS record restricting which CAs may issue TLS certificates)
  - Mail Exchange (MX) Records Present: Yes (DNS records routing inbound email for this domain)
  - Sender Policy Framework (SPF): Yes (DNS allowlist of mail servers authorized to send for this domain)
  - DMARC Policy Present: Yes (DNS policy instructing receivers how to reject or quarantine spoofed emails)

NIS2 ART. 21(2)(e)

Live Vulnerability Alerts, Exposed Secrets & Web Hygiene

- **Vulnerability & Exposure Summary**
  - JavaScript Library Advisories: 1 (CVEs/GHSAs in client-side JS libraries loaded by visitors' browsers)
  - Web & JS Framework Advisories: 0 (CVEs/GHSAs in frameworks such as Next.js, React, or Angular)
  - Web Server, Runtime & CMS Advisories: 0 (CVEs in web servers, server runtimes like PHP, or CMS stacks)
  - Exposed Files & Web Hygiene Findings: 1 (Publicly reachable backups, header gaps, or configuration issues)
  - Exposed Client-Side API Keys: 1 (Cleartext credentials or tokens embedded in public HTML/JS)

```
[GHSA-8hc4-vh64-cxmj / CVE-2024-39338] [JS Library] axios 1.7.2 | CVSS 7.5 [Confirmed] Range: >= 1.3.2, < 1.7.4 - Server-Side Request Forgery path-relative URL handling resolved in 1.7.4
```

```
[HYGIENE:MEDIUM] BACKUP_FILES_ROOT (/config.bak.json (200 OK))
```

```
[SECRET:stripe_restricted_key] rk_live_****8F2A in portal.nordiccloud-demo.eu
```

NIS2 ART. 21(2)(d) Zero-Access Live SBOM, CMS & Third-Party Supply Chain

- **Live Browser Script Telemetry**
  - External Scripts Discovered: 9, 9 fetched (First- and third-party JavaScript files loaded by the page)
  - Subresource Integrity (SRI) Protected Scripts: 8 (Cryptographic hashes verifying external scripts are unmodified)
  - Inline Scripts Observed: 1 (Executable <script> blocks embedded directly in the HTML document)
  - Exposed Source Maps (.map): 1 (Publicly downloadable debug maps exposing unminified client source code)
- **Live Software Inventory (SBOM)**
  - CMS Extensions: 0 Plugins, 0 Themes
  - Live Detected Components (JS Libraries, Frameworks & Server Stack): 4

```
Component [Web/JS Framework]: React (19.0.0)
```

```
Component [JS Library]: axios (1.7.2)
```

```
Component [JS Library]: zod (3.23.8)
```

```
Component [JS Library]: @sentry/browser (8.38.0)
```

NIS2 ART. 21(2)(c) Service Availability, DNS Resilience & Hosting Footprint (Supporting Art. 21(2)(c))

- **Availability & Edge Response**
  - 30-Day Uptime: 99.99% (Rolling availability percentage from external HTTPS health checks)
  - Latest Response Speed: 74 ms (End-to-end HTTPS response latency from the latest check)
  - Web Server Header: cloudflare (Server software banner disclosed in HTTP response headers)
- **DNS & Hosting Infrastructure**
  - Authoritative Nameservers: ns1.nordiccloud-demo.eu, ns2.nordiccloud-demo.eu
  - Hosting Network (ASN): AS24940, Hetzner Online GmbH (EU/DE) (Autonomous System routing public traffic for the site)