OSINT CASE STUDY

TechNova Solutions Intelligence Assessment

Detail	Information
Author	Astral
Date	February 6, 2026
Target Type	Corporate Intelligence (Open Sources Only)
Engagement	Open Source Intelligence (OSINT) Assessment
Methodology	DNS Reconnaissance → Infrastructure Analysis → Public Records Research → Security Assessment
Note	All data gathered from publicly available open sources per OSINT best practices

⚠️ CONFIDENTIAL - OPEN SOURCES ONLY
Sensitive data redacted per OSINT best practices. All information gathered exclusively from publicly available open sources.

Executive Summary

This OSINT case study presents a comprehensive intelligence assessment of TechNova Solutions and TechNova Imaging Systems, conducted entirely through

publicly available open sources. The assessment includes infrastructure analysis, technology stack identification, leadership mapping, organizational structure analysis, and security assessment of the primary website.

Methodology

Open Source Intelligence (OSINT) Methods Used:

1. **DNS Reconnaissance**
2. Subdomain enumeration
3. Public DNS record analysis
4. IP address and ASN identification
5. **Public Records Research**
6. WHOIS data analysis
7. Public domain registration records
8. Publicly accessible company information
9. **Professional Network Analysis**
10. Public LinkedIn profile research
11. Public company pages
12. Professional network mapping
13. **Infrastructure Analysis**
14. Public SSL certificate analysis
15. Public hosting provider identification
16. Technology stack identification from public headers
17. **Public Website Analysis**
18. Publicly accessible website content
19. Public documentation review
20. Public API endpoint discovery

21. **Security Assessment**

22. OWASP PTK automated security scanning
23. Technology stack fingerprinting
24. Security headers analysis

Key Findings

Infrastructure Exposure

- **4 Subdomains Identified:** demo, nms, odoo17, wap
- **Hosting Provider:** Hetzner Online GmbH (Germany)
- **Technology Stack:** Odoo 17 ERP system identified
- **Risk Level:** Medium-High (publicly accessible internal systems)

Organizational Structure

- **Parent Company:** TechNova Imaging Systems (P) Ltd.
- **Subsidiary:** TechNova Solutions
- **Leadership:** CEO/COO (Amit Khurana), CFO/CTO (Piyush Kapadia)
- **Recent Changes:** COO promoted to CEO (2022-2026)

Digital Assets

- **3 Domains:** technovaworld.com, technovaindia.com, technovasolutions.io
- **5 Corporate Emails:** Structured department-based system
- **International Presence:** Qatar operations identified

Security Assessment - www.technovaworld.com

Technology Stack Identified

Technology	Version	Category
Google Font API	-	Font scripts

Technology	Version	Category
Bootstrap	3.4.1	UI frameworks
jQuery	3.7.1	JavaScript libraries
jQuery UI	1.14.1	JavaScript libraries
HSTS	-	Security
nopCommerce	-	E-commerce
Zoho CRM	-	CRM
Microsoft ASP.NET	-	Web frameworks
Google Analytics	GA4	Analytics
Zoho PageSense	-	A/B Testing, Personalisation
FortiWeb (Fortinet)	-	WAF

Security Headers Analysis

Findings: - **CSP (Content Security Policy):** Allows inline/eval or wildcards in script/style - **CSP 'frame-ancestors':** Missing or overly broad - **HSTS (HTTP Strict Transport Security):** Max-age too low or missing includeSubDomains - **X-Frame-Options:** Header is a legacy directive - **X-XSS-Protection:** Header is a legacy directive

Risk Assessment: - **Medium Risk:** Security headers configuration needs improvement - **Recommendation:** Implement stricter CSP policies and update security headers

Web Application Framework

- **Primary Framework:** Microsoft ASP.NET
- **E-commerce Platform:** nopCommerce

- **WAF:** FortiWeb (Fortinet) - Web Application Firewall detected
- **CRM Integration:** Zoho CRM

Third-Party Services

- **Analytics:** Google Analytics GA4
- **A/B Testing:** Zoho PageSense
- **CRM:** Zoho CRM
- **CDN/Fonts:** Google Font API

Security Posture

- **WAF Protection:** FortiWeb (Fortinet) detected - indicates active security measures
- **HTTPS:** HSTS enabled (configuration needs improvement)
- **Legacy Headers:** Some security headers using deprecated directives

Data Sources

All information in this report was gathered exclusively from: - Public DNS records - Publicly accessible websites - Public LinkedIn profiles - Public domain registration data - Public infrastructure analysis - OWASP PTK automated security scanning (public website analysis)

No closed sources, breach databases, or proprietary data were used in this assessment.

Related Reports

- Intelligence Analysis - Master Report
- Intelligence Analysis - Technology Stack
- Intelligence Analysis - Digital Infrastructure
- Infrastructure Recon - technovasolutions.io
- Open Sources

⚠️ **CONFIDENTIAL - OPEN SOURCES ONLY**

All information in this report gathered exclusively from publicly available open sources. No closed sources, breach databases, or proprietary data were used.
