VIGIL FOR GOVERNMENT

Battle-Tested Security for Critical Government Infrastructure

Executive Summary

Government websites and citizen portals face constant nation-state cyber threats, defacement attacks, and data breach attempts. VIGIL has been battle-tested for 18+ months protecting Indian Army websites, demonstrating its capability to secure mission-critical government infrastructure against sophisticated adversaries.

Key Benefits for Government:

- Battle-proven by Indian Army protecting 100+ defense websites for 18+ months
- Automated CERT-In compliance reporting (only platform in India)
- AI-powered defacement detection within 60 seconds
- Data residency within India meeting government regulations
- Air-gapped on-premise deployment for classified networks
- 30-50% cost reduction vs. global vendors

Government Security Challenges

1. Nation-State Cyber Threats

Government infrastructure faces sophisticated attacks from nation-state actors and advanced persistent threats (APTs):

- Politically motivated defacement and propaganda
- Espionage and intelligence gathering
- Data exfiltration of citizen information
- Critical infrastructure disruption

2. CERT-In Compliance Requirements

CERT-In mandates 6-hour incident reporting for all government entities. Manual compliance processes are error-prone and resource-intensive:

- Incident detection, evidence collection, report generation within 6 hours
- Strict documentation and audit trail requirements
- Penalties for late or incomplete reporting

3. Citizen Data Protection

Government portals handle sensitive citizen data including Aadhaar, PAN, voter IDs, and personal information. Data breaches have severe national security and privacy implications.

VIGIL Government Solution

1. Battle-Proven by Indian Army

VIGIL has protected 100+ Indian Army websites for 18+ months with zero breaches, demonstrating reliability under the most demanding security requirements:

- **18+ months in production** protecting critical defense infrastructure
- **100+ websites monitored** including classified and public-facing systems
- **Zero breaches** in production deployment
- **Nation-state threat detection** and prevention

2. Automated CERT-In Compliance

VIGIL is India's only platform with fully automated 6-hour CERT-In incident reporting:

- **DETECT:** Incident detected (defacement, breach, vulnerability)
- **PACKAGE:** Auto-collects evidence (logs, screenshots, timeline)
- **GENERATE:** Creates government-approved CERT-In report
- **SUBMIT:** Ready for submission within 6-hour window

Time from detection to report-ready: <60 minutes

3. Data Sovereignty and Security

VIGIL meets all government data residency and security requirements:

- Data storage within India (Delhi, Mumbai data centers)
- Air-gapped on-premise deployment for classified networks
- No data transfer outside Indian borders
- Indian team with security clearances

Case Study: Indian Army Cyber Group

Deployment Profile:

- 100+ websites including public and classified systems
- 18+ months continuous operation
- High-threat environment with nation-state adversaries

Results:

- **Zero successful breaches** in 18+ months
- **Multiple attack attempts blocked** including sophisticated APTs
- **99.9% uptime** meeting operational requirements
- **Rapid defacement detection** preventing public exposure

"VIGIL has proven itself as a robust, reliable security platform under the most demanding conditions. Its AI-powered threat detection and automated compliance reporting are unmatched."

- Senior Security Officer, Indian Army Cyber Group

Why Choose VIGIL for Government

- **Battle-Proven:** 18+ months protecting Indian Army with zero breaches
- **CERT-In Compliance:** Only automated 6-hour reporting solution
- **Data Sovereignty:** India-based deployment and team
- **Cost Effective:** 30-50% cheaper than global vendors

Getting Started

Email: sales@aaizeltech.com

Website: https://cyber-shieldpro.com

Phone: +91-7807061094