2026

seceon

# Strategic Cybersecurity Architecture for the Indian Defence Industry

*This whitepaper details how AI-driven unified cybersecurity enables India's defence industry to withstand state-sponsored cyber warfare, APTs, and hybrid threats.*

## Executive Summary

The Indian Defence Industrial Base (DIB) is undergoing a paradigm shift toward "Indigenization 2.0," characterized by self-reliant deep-tech ecosystems and high-value exports. However, this transition has coincided with an unprecedented surge in cyber hostilities. In 2025 and early 2026, India recorded over 265 million cyberattacks, averaging 505 detections per minute. Geopolitical events, most notably the Operation Sindoor hybrid conflict in May 2025, have proven that digital sabotage is now an inseparable component of modern warfare.

The regulatory environment has responded with the Security Manual for Licensed Defence Industries (SMLDI) 2025 and the July 2025 CERT-In Comprehensive Audit Guidelines, mandating rigorous annual audits, air-gapped operations, and 6-hour incident reporting. To meet these demands, the sector is adopting autonomous, AI-driven defense fabrics. The Seceon Open Threat Management (OTM) platform, particularly the aiSecOT360 module launched in January 2026, has emerged as the definitive solution for protecting legacy industrial controls and indigenous operating systems like MayaOS from sophisticated Advanced Persistent Threats (APTs).

## The Strategic Macro-Environment: Indigenization 2.0

The Indian defense sector outlook remains structurally overweight, supported by a capital outlay projected to grow 10-15% year-on-year.

**Indigenous Digital Ecosystems**

Strategic autonomy is being realized through the development of homegrown platforms:

- **MayaOS:** An Ubuntu-based operating system designed to replace Microsoft Windows across the Ministry of Defence (MoD) to eliminate foreign backdoors.
- **Project ASCON Phase IV:** A ₹7,796 crore initiative creating a secure, IP/MPLS-based communication network with 80% indigenous content for forward areas.
- **Army AI Roadmap 2027:** Integrating drone swarming, real-time surveillance, and smart war rooms by late 2026.

While these indigenous efforts enhance sovereignty, they create unique security requirements. Threat actors are rapidly pivoting their toolkits to exploit these specific platforms, necessitating a shift from signature-based tools to behavioral AI defense.

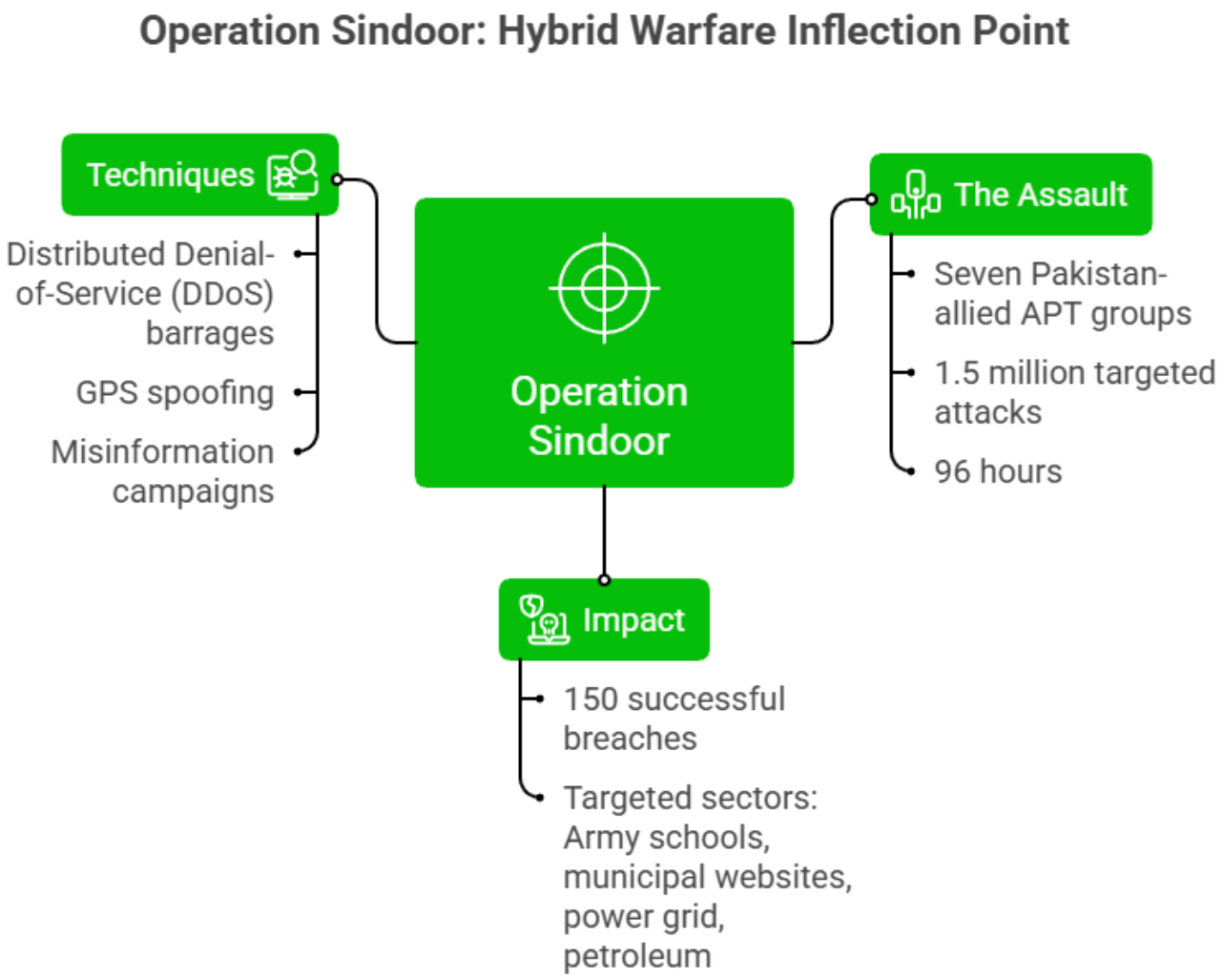
## Threat Landscape Analysis: The Reality of 2025-2026

Cybersecurity in 2026 has moved from a reactive IT function to a "Resilience by Design" imperative.

**Operation Sindoor: The Hybrid Warfare Inflection Point (May 2025)**

Following kinetic responses to the Pahalgam terror attack, India’s digital networks faced a coordinated counter-offensive in which **seven Pakistan-allied APT groups** launched approximately **1.5 million targeted attacks within 96 hours**. While **99.99 percent of attacks were thwarted**, the remaining successful breaches targeted **Army schools, municipal websites**, and attempted intrusions into the **power grid and petroleum sectors**.

The campaign employed **Distributed Denial-of-Service barrages, GPS spoofing, and coordinated misinformation operations**, reflecting the integrated use of cyber techniques to undermine operational stability and public confidence.




**Attack Statistics and Sectoral Risks**

**Volume** data indicates that Seqrite recorded 265.52 million detections across 8 million endpoints in the past year, highlighting the scale of hostile cyber activity. **Prevalence** analysis shows that Trojans and file infectors account for nearly 70 percent of all malware detections. **OT Vulnerabilities** remain a critical concern, with the average attacker dwell time inside industrial networks reaching 85 days as adversaries exploit unmonitored legacy SCADA systems.

## Advanced Persistent Threat (APT) Profiles

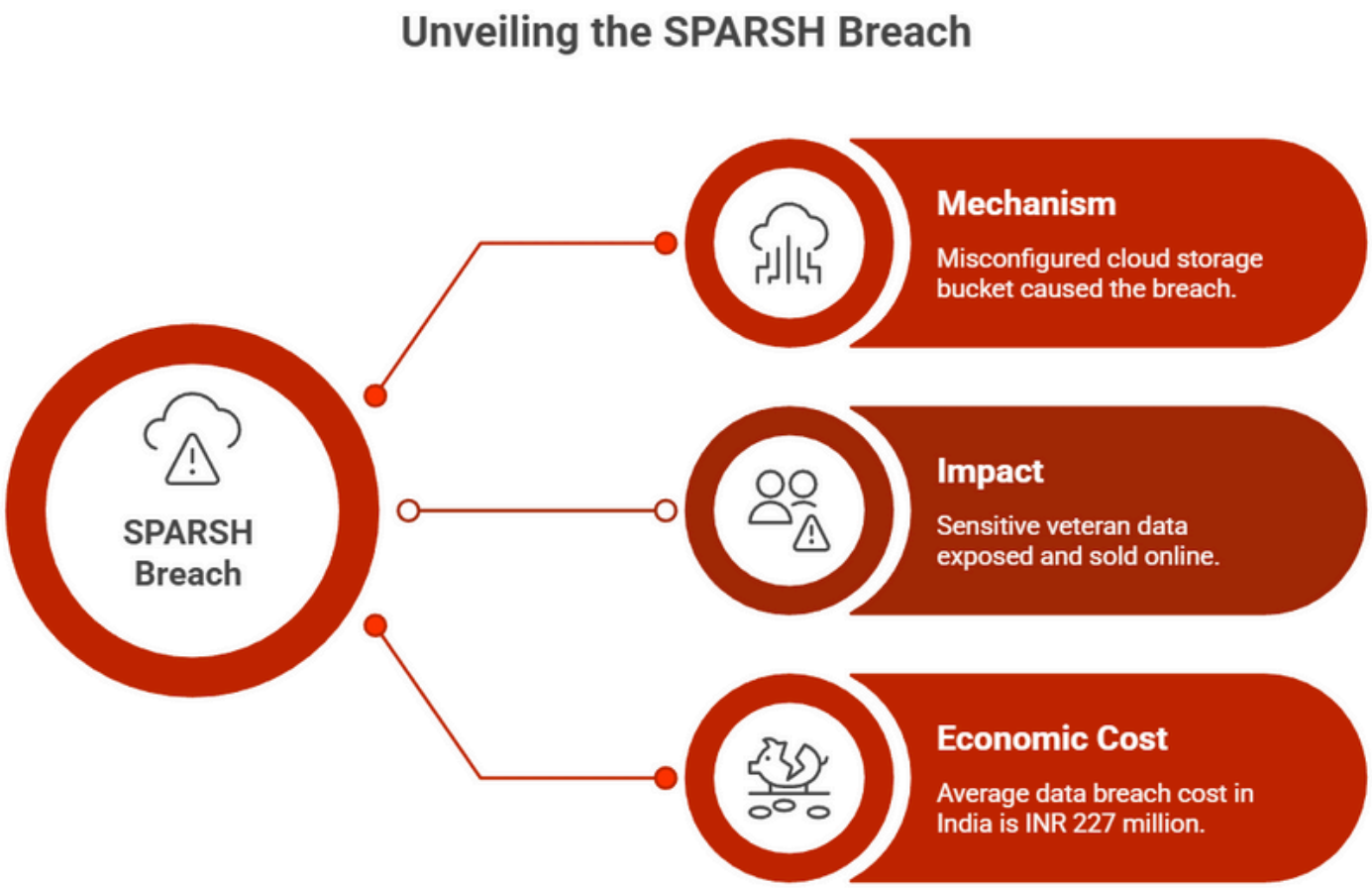
The Indian DIB is relentlessly targeted by state-sponsored actors seeking to steal intellectual property and military capabilities.

| APT Group | Affiliation | 2026 Tactical Focus | Strategic Target |
|---|---|---|---|
| APT36 (Transparent Tribe) | Pakistan-nexus. | Golang-based DeskRAT and Poseidon targeting BOSS and MayaOS Linux. | MoD officials, Army commands, classified drone blueprints. |
| SideCopy | Pakistan-allied. | Impersonating government domains and using custom RATs with layered obfuscation. | Critical defense manufacturing and infrastructure. |
| APT41 (Double Dragon) | China-nexus. | Supply chain weaponization and Chrome V8 zero-day exploits (CVE-2025-6554). | Telecom, aerospace manufacturing, and defense finance. |
| SideWinder | Regional. | ClickOnce-based infection chains generate new malware every five hours. | Maritime facilities, ports, and nuclear research agencies. |
| Mysterious Elephant | Regional. | Exfiltrating WhatsApp communications and Chrome tokens via ChromeStealer. | Foreign affairs and government leadership. |

## Technical Failure Case Study: The SPARSH Breach

The 2024 security breach of the **System for Pension Administration Raksha (SPARSH)** portal serves as a critical lesson in cloud security, demonstrating how basic configuration failures can lead to severe consequences.

The incident resulted from a **misconfigured cloud storage bucket**, rather than a sophisticated exploit, effectively a checkbox that was not enabled. As a result, **sensitive profiles of thousands of Army, Navy, and Air Force veterans** were exposed, with credentials and pension numbers later sold on Russian marketplaces for **$9.00**. The breach underscores the broader **economic impact of public cloud failures in India**, where the average cost per incident has reached **INR 227 million**.




## Regulatory and Compliance Mandates 2025-2026

Cybersecurity compliance is now legally binding and enforceable through the National Critical Information Infrastructure Protection Centre (NCIIPC) and CERT-In.

### Security Manual for Licensed Defence Industries (SMLDI) 2025

The MoD's revised manual introduces stringent operational requirements:

- **Turnover Mandate:** Companies with a turnover exceeding **INR 250 crore** must appoint a dedicated, full-time CISO.
- **Physical-Digital Synergy:** Biometric access control is now the mandatory baseline for all sensitive storage and production areas.
- **Air-Gap Requirement:** All official work related to highly classified products (Category A) must be conducted on air-gapped networks isolated from the internet.

### CERT-In 2025 Comprehensive Audit Policy

Issued on July 25, 2025, these rules apply to all entities operating within the digital ecosystem and introduce strict operational obligations. The **Six-Hour Rule** mandates that all significant cybersecurity incidents, including unauthorized access or malware infections, must be reported within six hours of discovery. **180-Day Log Retention** requires ICT logs to be retained within Indian jurisdiction and synchronized with National Physical Laboratory time sources. In addition, the **Layered BOM** requirement obligates organizations to maintain real-time standards for Software (SBOM), Cryptographic (CBOM), Quantum (QBOM), Hardware (HBOM), and AI (AIBOM) components.

### DPDP Act Acceleration

As of January 2026, MeitY is actively considering compressing the implementation timeline for Significant Data Fiduciaries (SDFs) from **18 months to 12 months**, meaning full compliance is expected by **November 2026**.

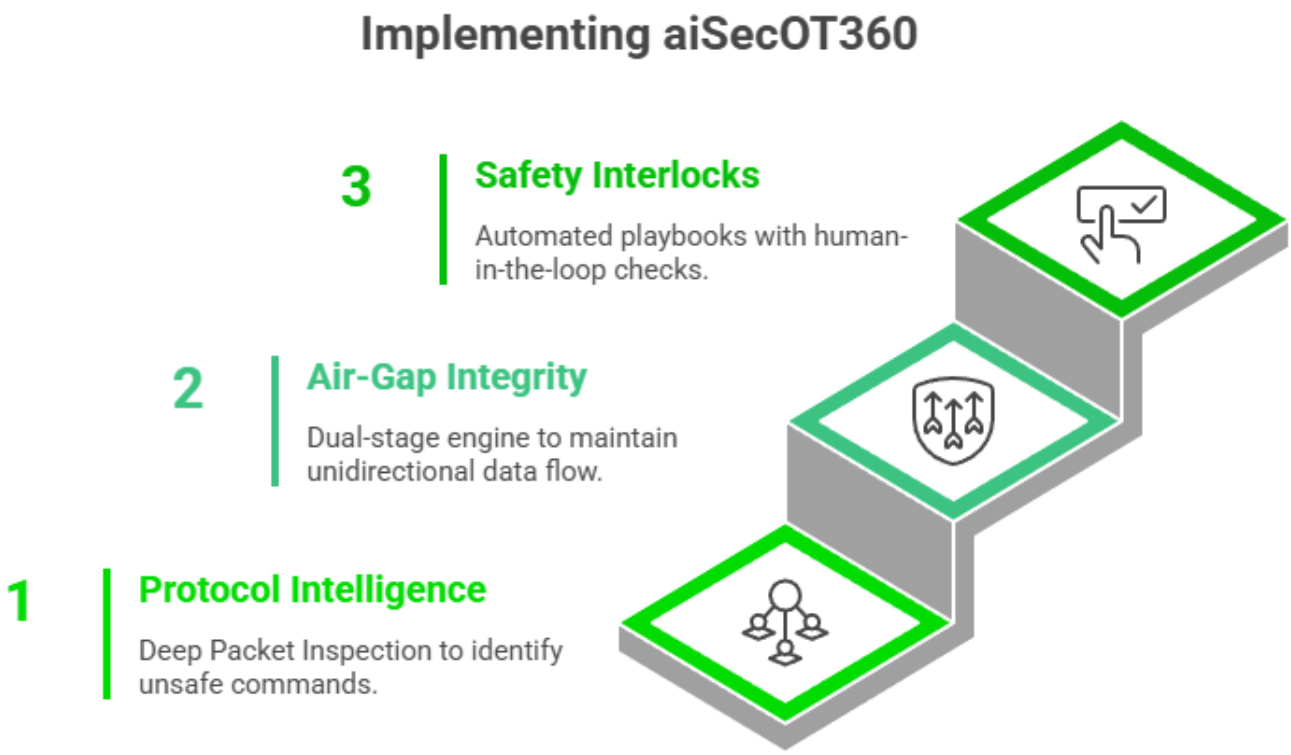
## The Seceon Platform: Autonomous Defense for India’s DIB

In an environment where attackers use AI to discover misconfigurations in minutes, traditional SIEM tools are failing. Seceon’s OTM platform provides an integrated, AI-driven fabric for mission-critical security.

**aiSecOT360: Jan 2026 Announcement**

Launched on **January 13, 2026**, the **aiSecOT360** module is purpose-built for the defense sector's OT environments:

- **Protocol Intelligence:** Deep Packet Inspection (DPI) for over **70 industrial protocols** (DNP3, Modbus, BACnet), identifying unsafe commands in sub-30 seconds.
- **Air-Gap Integrity:** A dual-stage Collection & Control Engine (CCE) maintains unidirectional data flow, allowing real-time monitoring without compromising physical isolation.
- **Safety Interlocks:** Automated response SOAR playbooks include human-in-the-loop interlocks to ensure no automated action disrupts critical manufacturing lines.

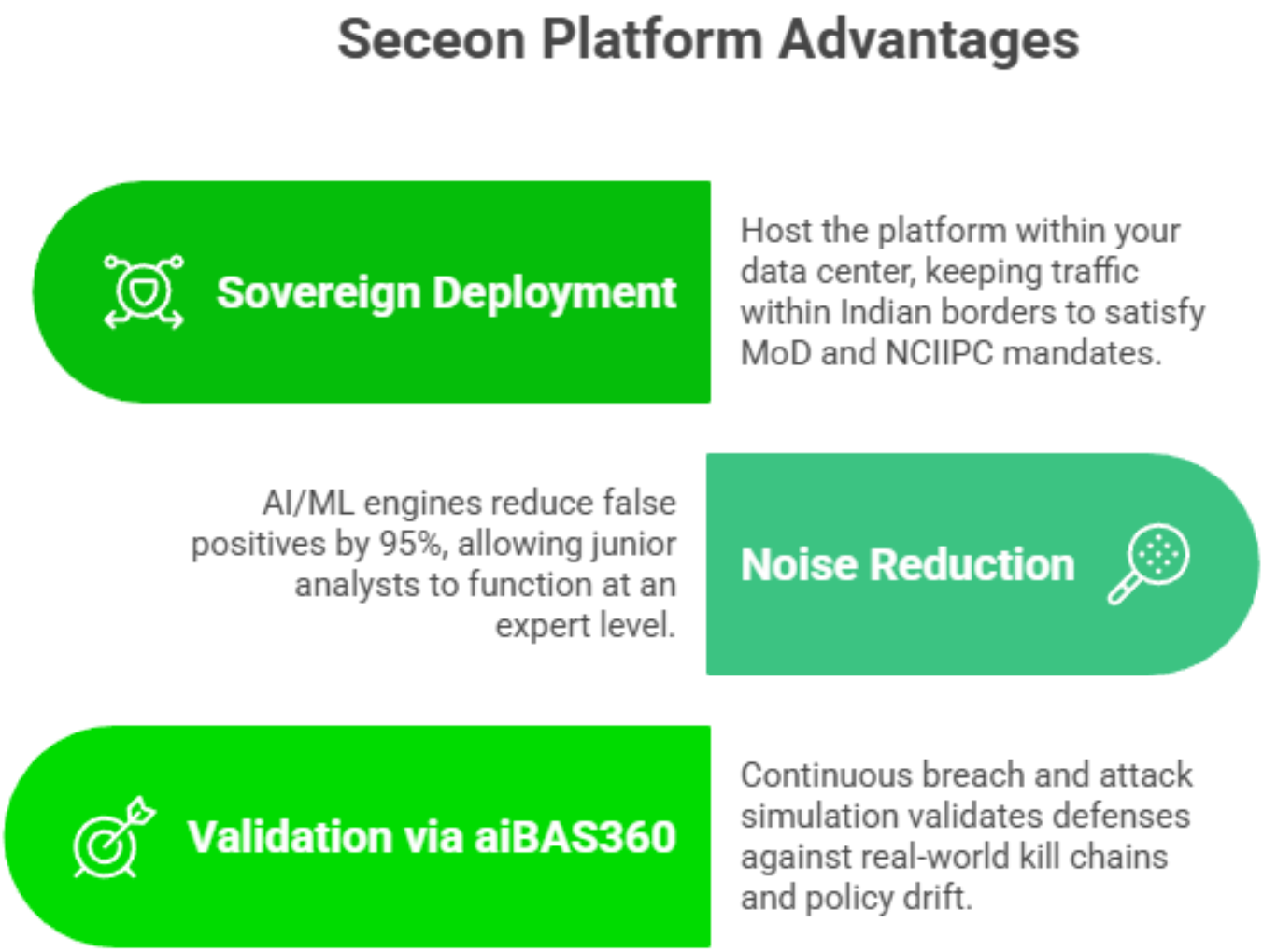



**Data Sovereignty and Tactical Advantages**

**Sovereign Deployment** enables Seceon to be hosted entirely within the client's own data center, ensuring that all traffic and logs remain within Indian borders to meet MoD and NCIIPC mandates.

**Noise Reduction** is achieved through advanced AI and ML engines that reduce false positives by up to 95 percent, allowing junior analysts to operate with expert-level effectiveness.

**Validation via aiBAS360** provides continuous breach and attack simulation, validating security controls against real-world kill chains and detecting policy drift before it can be exploited.



# Strategic Cybersecurity Architecture for the Indian Defence Industry

## Why Traditional Approaches Fail and How AI-Driven Security Succeeds

## Four Pillars of Challenges

**265M+ Attacks**
Detected across Indian networks in 2025-26

**Indigenization Exposure**
MayaOS and AI platforms expand attack surface

**85-Day Dwell Time**
Attackers persist inside OT networks

**INR 227M Cost**
Average public cloud breach impact

## Current Threat Level

**505 Alerts/Minute**
Sustained hostile activity at scale

**State-Backed APTs**
Pakistan and China-nexus groups active

**Hybrid Attacks**
DDoS, GPS spoofing, supply-chain abuse

**Residual Breaches**
Despite 99.99% attack prevention

## Current Problems

- **Fragmented security tools** across **IT, OT, and defense manufacturing**
- **Signature-based detection** unable to identify **zero-day and behavioral threats**
- **Manual response cycles** allowing attackers **extended dwell time**
- **Limited visibility** into legacy **SCADA and air-gapped environments**
- **High false positives** overwhelming understaffed SOC teams
- **Compliance complexity** across **SMLDI, CERT-In, DPDP, and NCIIPC mandates**

## Seceon Solution

- **Unified AI-driven platform** covering **IT, OT, cloud, endpoints, and identities**
- **Behavioral analytics** tailored for **users, devices, and industrial systems**
- **Automated response** with human-in-the-loop safety controls
- **Sovereign deployment** supporting fully **on-prem, air-gapped environments**
- **AI correlation** reducing **false positives by up to 95%**
- **Built-in compliance alignment** for **MoD, CERT-In, and NCIIPC requirements**

## Results

**<5 Minutes**
Mean time to detect

**95% Noise Reduction**
AI-driven alert accuracy

**Continuous Validation**
Live attack simulation

**Sovereign Control**
All data stays in India

## Why Seceon for Indian Defence

SMLDI and CERT-In mandates are tightening as cyber warfare intensifies. Defence organizations must modernize security architectures now. Unified, AI-driven, sovereign defense platforms enable faster detection, resilient operations, and compliance readiness across India's mission-critical defence ecosystem.

## Conclusion

The Indian Defence Industrial Base faces an increasingly complex cyber threat landscape driven by rapid digitization, indigenous technology adoption, and persistent state-sponsored attacks. Traditional, fragmented security models are no longer sufficient to protect mission-critical defense environments. A unified, AI-driven cybersecurity architecture that delivers continuous visibility, rapid response, and regulatory alignment is essential to maintaining operational resilience and safeguarding national security in the evolving landscape of modern warfare.

**About Seceon**

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats and breaches at scale. Seceon’s Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It’s all enriched and analyzed in real-time by applying threat intelligence, AI, and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 700 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,300 clients.

# References and Citations:

This whitepaper is based on research and data from:


- Indian Defense Sector Outlook 2026 - Why Analysts Stay Overweight - Swastika Investmart, accessed January 24, 2026, https://www.swastika.co.in/blog/indian-defense-sector-outlook-2026-why-analysts-stay-overweight
- Navigating India's Digital Personal Data Protection Act (DPDPA) Rules: A Compliance Guide - Securiti.ai, accessed January 24, 2026, https://securiti.ai/india-digital-personal-data-protection-act-dpdpa-rules/
- AI Roadmap for Indian Army Operations - Sanskriti IAS, accessed January 24, 2026, https://www.sanskritiias.com/current-affairs/ai-roadmap-for-indian-army-operations
- Seceon OTM + CGuard 2.0 = The Future of Unified Cyber Defense, accessed January 24, 2026, https://seceon.com/seceon-otm-cguard-2-0-the-future-of-unified-cyber-defense/
- Cyber Security Audit Checklist for Businesses in 2026 - Quick Heal, accessed January 24, 2026, https://www.quickheal.co.in/knowledge-centre/cyber-security-audit-checklist-for-businesses-in-2026/
- CERT-In: India's Frontline Defender against Cyber Threats - PIB, accessed January 24, 2026, https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=157049&ModuleId=3
- CERT-In Directions Compliance in 2025: A Practical Counsel's Guide - amlegals, accessed January 24, 2026, https://amlegals.com/cert-in-compliance-guide-2025/
- Strengthening cybersecurity: Lessons for Indian enterprises in 2026 - ET CISO, accessed January 24, 2026, https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/top-5-cybersecurity-mistakes-indian-enterprises-should-avoid-in-2026/126789272
- Seceon Breaks the OT Security Barrier: aiSecOT360 Delivers Holistic Protection Without Compromising Air-Gap Integrity, accessed January 24, 2026, https://seceon.com/seceon-breaks-the-ot-security-barrier-aisecot360-delivers-holistic-protection-without-compromising-air-gap-integrity/

## About the Author

# Madan Mohan Pandey

**Principal Cybersecurity Architect, Seceon Inc.**

Madan is a software professional with strong experience in network design, application development, and cybersecurity engineering. He has worked extensively with the TCP/IP stack, routing and switching, and AWS services such as EC2 and S3. He has built automated CI/CD pipelines using Jenkins and Git to enable continuous testing and daily product updates. Madan also brings solid knowledge of EDR, XDR, MDR, and threat intelligence, along with an understanding of threats like ransomware, trojans, zero-day malware, botnets, and DNS tunneling. His experience with firewalls, IDS, IPS, VPNs, SIEM platforms, and log and netflow analysis helps him identify anomalies and support accurate threat detection across modern environments.

## About the Author

# Aditya Kumar

**AI/ML Cybersecurity Engineer, Seceon Inc.**

Aditya brings deep expertise in applying artificial intelligence and machine learning to safeguard IT, OT, IoT, and cloud ecosystems against advanced and evolving cyber threats. At Seceon, he plays a key role in strengthening enterprise security resilience, ensuring alignment with global compliance frameworks, and delivering measurable ROI through the company's next generation aiSIEM and OTM platforms.