2026

seceon

Defending India’s Energy Backbone at Scale

State of Cybersecurity for the Indian Oil and Gas Industry (2026 Edition)

How Autonomous, AI-Driven Security Protects Critical Energy Infrastructure

Executive Summary

By early 2026, India’s oil and gas sector has moved decisively beyond basic digital transformation into an era defined by Agentic AI, hyper-connected OT environments, and real-time operational intelligence. These advances have delivered measurable gains in efficiency, predictive maintenance, and asset utilization. However, they have also placed the sector firmly in the crosshairs of nation-state adversaries and highly organized ransomware groups.

Threat intelligence reports confirm a **935% surge in ransomware and targeted cyberattacks against global energy organizations**, with Indian energy infrastructure increasingly featured due to its geopolitical and economic importance. At the same time, India’s regulatory landscape has shifted from advisory to punitive. The **CERT-In 2025 Comprehensive Audit Guidelines** and the **Digital Personal Data Protection (DPDP) Act** now impose strict auditability, log retention, and incident reporting requirements, with financial penalties reaching **INR 250 crore per breach**.

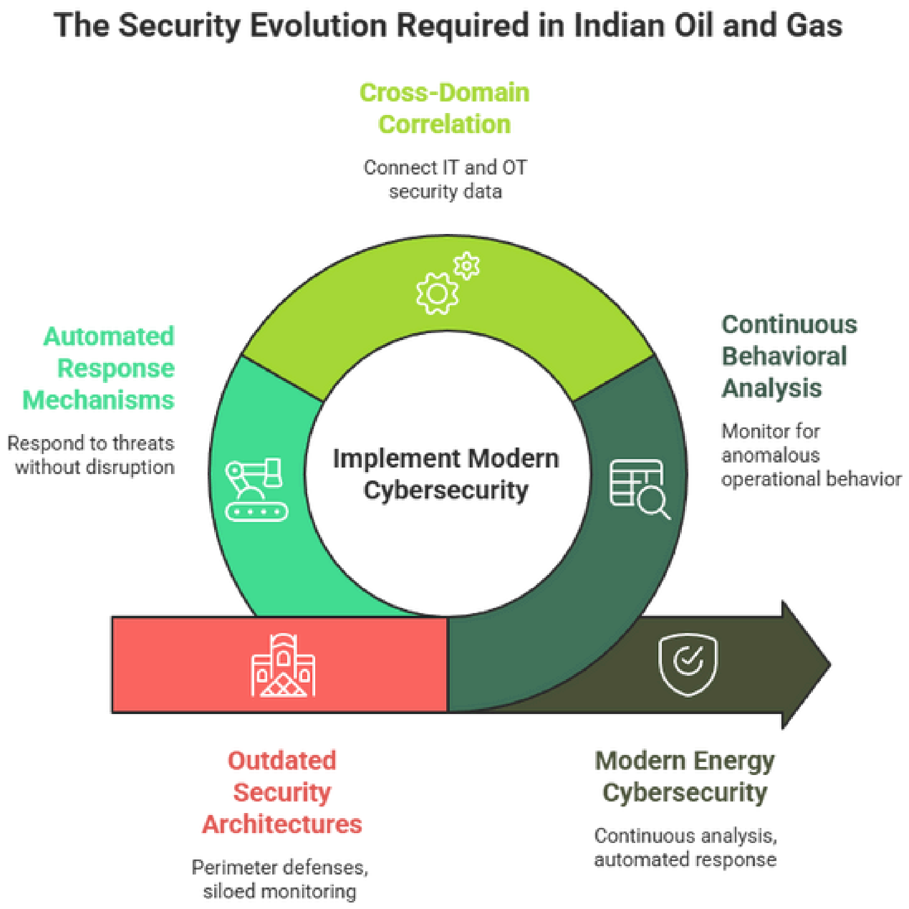
These converging pressures have exposed a critical reality: **human-led SOCs and fragmented security stacks cannot defend machine-speed infrastructure**. This whitepaper examines why legacy approaches fail in Indian oil and gas environments and how **Seceon’s AI-driven Open Threat Management (OTM) platform**, powered by **aiSecOT360**, enables autonomous, safety-aware defense for critical energy systems.

The Security Evolution Required in Indian Oil and Gas

India’s oil and gas organizations now operate deeply interconnected ecosystems that span refinery control systems, pipeline SCADA networks, cloud-hosted analytics platforms, and millions of edge-connected IoT and IIoT devices. Digital twins, predictive maintenance models, and real-time telemetry have become foundational to daily operations.

Security architectures, however, have not evolved at the same pace. Most enterprises continue to rely on perimeter defenses, siloed monitoring tools, and manual response processes that were never designed for converged IT/OT environments. These models struggle to distinguish legitimate operational behavior from malicious activity, particularly when attacks unfold slowly and deliberately.

Modern energy cybersecurity requires continuous behavioral analysis, cross-domain correlation, and automated response mechanisms that operate without disrupting safety-critical operations. Without these capabilities, attackers can remain embedded for months, mapping environments and staging attacks that can impact physical infrastructure.


The Security Evolution Required in Indian Oil and Gas
Cross-Domain Correlation
Connect IT and OT security data
Automated Response Mechanisms
Respond to threats without disruption
Continuous Behavioral Analysis
Monitor for anomalous operational behavior
Implement Modern Cybersecurity
Outdated Security Architectures
Perimeter defenses, siloed monitoring
Modern Energy Cybersecurity
Continuous analysis, automated response

National Impact and Strategic Significance

Cyberattacks on Indian oil and gas infrastructure represent far more than isolated security incidents. They pose a **systemic national risk**, capable of disrupting fuel supply chains, cascading into power and transportation sectors, and undermining public confidence during periods of geopolitical tension. With the energy sector projected to contribute nearly **20% of India’s GDP by the end of 2026**, its resilience is inseparable from national economic stability. A single prolonged outage or safety incident triggered by cyber sabotage could have consequences extending well beyond the affected organization.

To illustrate the scale and urgency of the challenge, the following table summarizes the most critical cybersecurity impact indicators across the Indian oil and gas sector.

Indian Oil and Gas Cyber Impact Summary

Metric	Observed Impact
Growth in Energy Sector Attacks	935% increase year-over-year
Expansion of Connected Assets	11+ million IT, OT, and IIoT endpoints
Average Breach Dwell Time (Traditional SOCs)	85–241 days
CERT-In Incident Reporting Window	6 hours
Maximum DPDP Act Penalty	INR 250 crore per breach
AI-Based Critical Threat Containment	Under 30 seconds

Threat Landscape and Adversary Methodology

Recent threat activity targeting Indian energy organizations reflects a shift toward **hybrid warfare models**. Advanced Persistent Threat (APT) groups such as **SideWinder**, along with China-linked actors including **Volt Typhoon**, increasingly focus on long-term pre-positioning rather than immediate disruption.

These actors exploit legacy OT protocols, insecure edge devices, and flat networks to establish stealthy footholds. In parallel, financially motivated groups leverage credential resale markets and vulnerabilities in managed file transfer platforms to gain initial access. Once inside, attackers move laterally across IT and OT boundaries, often without triggering alerts from traditional security tools.

The continued use of protocols such as **Modbus** and unsecured radio-based RTUs further amplifies risk, as these technologies were never designed with authentication or integrity verification in mind. To better understand how these attacks progress and where traditional defenses fail, the following table outlines a typical attack chain observed in energy-sector incidents.

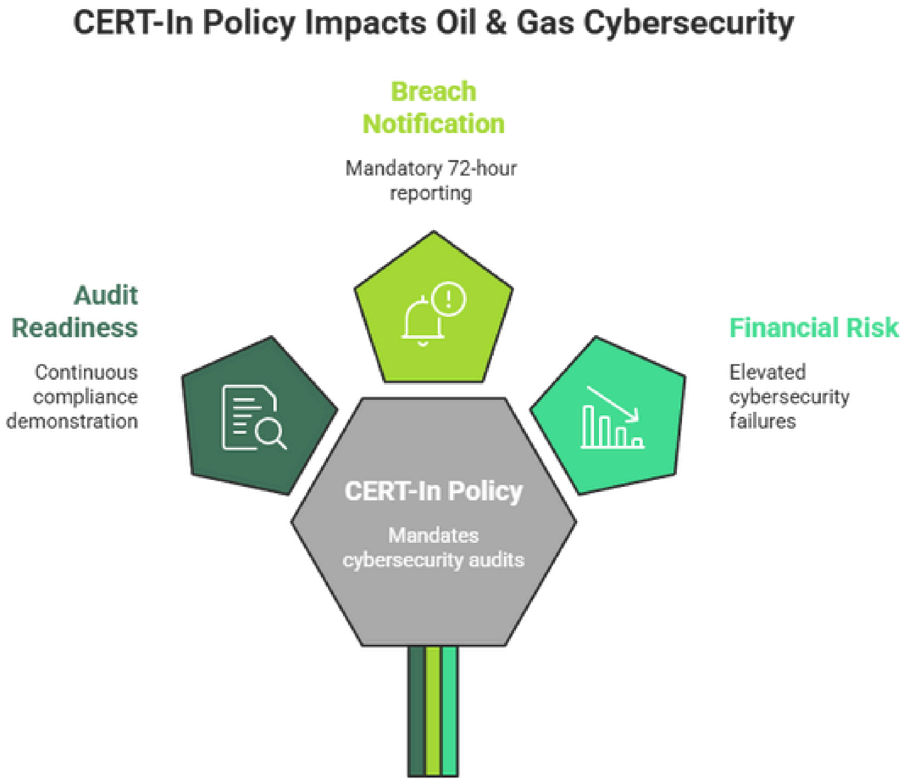
Energy Sector Attack Chain Overview

Attack Stage	Observed Technique	Why Traditional Security Fails	Seceon AI Countermeasure
Initial Access	Credential resale, phishing	No behavioral identity context	AI-driven anomaly detection
Persistence	Shared or unmanaged admin access	Lack of UEBA	Privilege deviation analysis
Lateral Movement	IT–OT traversal	Limited east–west visibility	Behavioral network analytics
Command Execution	Unsafe OT command injection	No protocol-level inspection	Deep industrial protocol inspection
Impact	Sabotage or ransomware	Manual response latency	Autonomous containment

Regulatory Imperative: From Compliance to Survival

India’s regulatory environment has fundamentally altered the cybersecurity risk equation for oil and gas operators. The **CERT-In 2025 Comprehensive Audit Policy** mandates annual third-party audits, real-time documentation of software and cryptographic components, and a strict six-hour incident reporting window. In parallel, the **DPDP Act** enforces mandatory breach notification within 72 hours and introduces penalties that elevate cybersecurity failures into board-level financial risks.

These mandates have rendered manual compliance models obsolete. Organizations must now demonstrate **continuous audit readiness**, not periodic compliance snapshots.


CERT-In Policy Impacts Oil & Gas Cybersecurity
Breach Notification
Mandatory 72-hour reporting
Audit Readiness
Continuous compliance demonstration
Financial Risk
Elevated cybersecurity failures
CERT-In Policy
Mandates cybersecurity audits

Seceon’s AI-Driven Security Blueprint for Energy Infrastructure

Seceon addresses these challenges through a **unified Open Threat Management (OTM) platform** that consolidates SIEM, XDR, UEBA, NDR, and SOAR into a single AI-driven analytics and response fabric. Unlike traditional SOC platforms, Seceon’s architecture is designed to understand behavioral context across IT, OT, cloud, and identity systems. This enables the detection of subtle deviations that signal early-stage compromise, even when attackers use valid credentials or low-noise techniques.

At the core of this approach is **aiSecOT360**, a purpose-built module for securing legacy SCADA and PLC environments without compromising safety or air-gap integrity.

aiSecOT360: Autonomous Security Without Operational Risk

aiSecOT360 bridges the IT/OT divide through a dual-stage Collection and Control Engine that preserves unidirectional data flow from OT to IT systems. This design ensures that security monitoring never introduces pathways for external compromise.

The platform supports deep inspection of more than 70 industrial protocols, allowing it to identify unsafe commands, anomalous control sequences, and lateral movement attempts in near real time. Safety interlocks maintain human oversight for critical remediation actions, ensuring automation never triggers unintended shutdowns or safety incidents.

For Indian PSUs, Seceon’s sovereign deployment model enables full on-premises or in-country hosting, ensuring compliance with CERT-In and DPDP localization requirements.

To quantify the operational difference between legacy SOC models and autonomous AI-driven security, the table below highlights key performance outcomes.

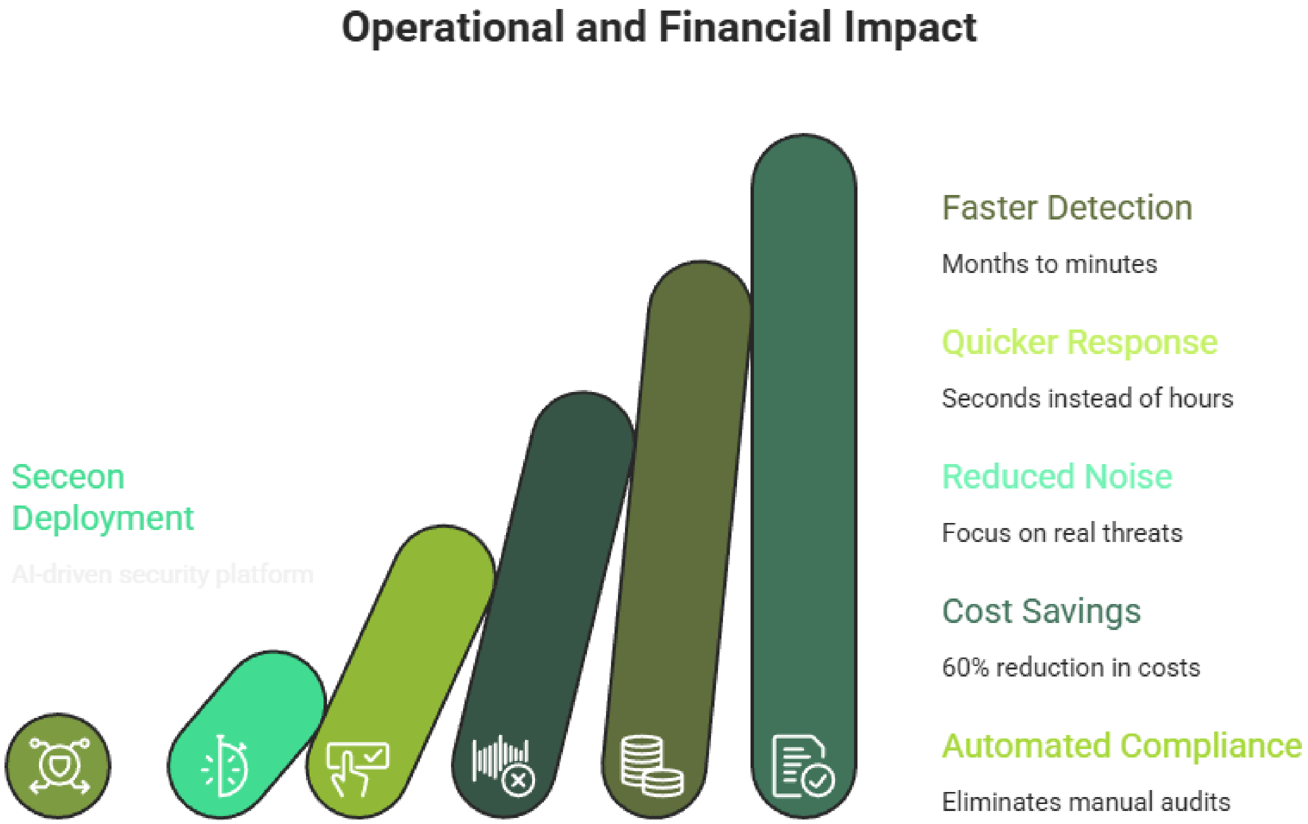
Detection and Response Performance Comparison

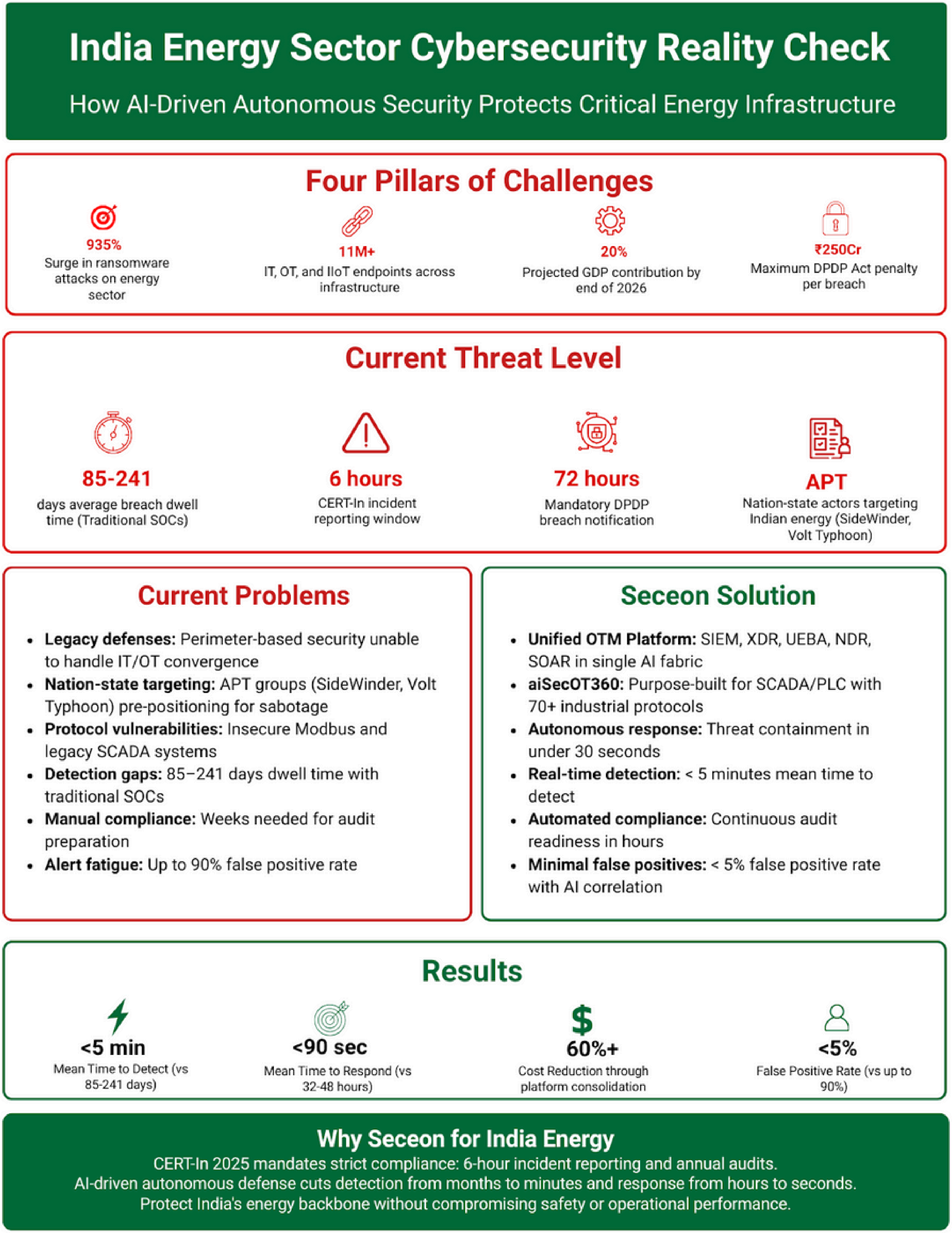
Metric	Traditional Energy SOC	With Seceon OTM
Mean Time to Detect	85–241 days	< 5 minutes
Mean Time to Respond	32–48 hours	< 90 seconds
False Positive Rate	Up to 90%	< 5%
Automated Response Coverage	< 20%	~70%
Audit Readiness	Weeks	Hours

Operational and Financial Impact

Organizations deploying Seceon in energy environments report significant improvements across both security and operational metrics. Detection times are reduced from months to minutes, while response actions execute in seconds rather than hours. Alert noise drops dramatically due to AI-driven correlation, allowing security teams to focus on true threats instead of false positives.

From a financial perspective, platform consolidation reduces tooling and operational costs by more than 60%, while automated compliance reporting eliminates weeks of manual audit preparation.





India Energy Sector Cybersecurity Reality Check

How AI-Driven Autonomous Security Protects Critical Energy Infrastructure

Four Pillars of Challenges

935%
Surge in ransomware attacks on energy sector

11M+
IT, OT, and IIoT endpoints across infrastructure

20%
Projected GDP contribution by end of 2026

₹250Cr
Maximum DPDP Act penalty per breach

Current Threat Level

85-241
days average breach dwell time (Traditional SOCs)

6 hours
CERT-In incident reporting window

72 hours
Mandatory DPDP breach notification

APT
Nation-state actors targeting Indian energy (SideWinder, Volt Typhoon)

Current Problems

- **Legacy defenses:** Perimeter-based security unable to handle IT/OT convergence
- **Nation-state targeting:** APT groups (SideWinder, Volt Typhoon) pre-positioning for sabotage
- **Protocol vulnerabilities:** Insecure Modbus and legacy SCADA systems
- **Detection gaps:** 85–241 days dwell time with traditional SOCs
- **Manual compliance:** Weeks needed for audit preparation
- **Alert fatigue:** Up to 90% false positive rate

Seceon Solution

- **Unified OTM Platform:** SIEM, XDR, UEBA, NDR, SOAR in single AI fabric
- **aiSecOT360:** Purpose-built for SCADA/PLC with 70+ industrial protocols
- **Autonomous response:** Threat containment in under 30 seconds
- **Real-time detection:** < 5 minutes mean time to detect
- **Automated compliance:** Continuous audit readiness in hours
- **Minimal false positives:** < 5% false positive rate with AI correlation

Results

<5 min
Mean Time to Detect (vs 85-241 days)

<90 sec
Mean Time to Respond (vs 32-48 hours)

60%+
Cost Reduction through platform consolidation

<5%
False Positive Rate (vs up to 90%)

Why Seceon for India Energy

CERT-In 2025 mandates strict compliance: 6-hour incident reporting and annual audits.
AI-driven autonomous defense cuts detection from months to minutes and response from hours to seconds.
Protect India's energy backbone without compromising safety or operational performance.

Essential Actions for Indian Energy Leaders

To remain resilient in the face of escalating threats and regulatory pressure, Indian oil and gas leaders must prioritize unified visibility across IT and OT environments, transition to continuous compliance automation, and adopt autonomous response capabilities that operate at machine speed. Cybersecurity can no longer function as a reactive control; it must become an integral component of operational safety and national resilience.

Conclusion

The cybersecurity challenges facing India’s oil and gas sector in 2026 are unprecedented in scale and complexity. Fragmented tools, manual processes, and legacy defenses are no longer sufficient to protect hyper-connected, geopolitically targeted infrastructure.

A **unified, AI-driven, autonomous security model** is now a strategic necessity. Seceon enables energy organizations to secure critical operations, meet stringent regulatory requirements, and protect India’s energy backbone without compromising safety or performance.

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:

- India Cyber Threat Report 2025 – DSCI https://www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf
- Zscaler: Ransomware Attacks on Oil and Gas Surge 935% https://industrialcyber.co/reports/zscaler-warns-that-ransomware-attacks-on-oil-and-gas-surge-935-as-critical-sectors-targeted/
- CERT-In 2025 Comprehensive Audit Guidelines https://lawrbit.com/article/comprehensive-cyber-security-audit-policy-guidelines/
- India DPDP Rules 2025 – Deloitte https://www.deloitte.com/in/en/services/consulting/about/indias-dpdp-rules-2025-leading-digital-privacy-compliance.html
- MITRE ATT&CK for ICS https://attack.mitre.org

References and Citations:

This whitepaper is based on research and data from:

- China-Linked APT Activity – Volt Typhoon (NJCCIC) https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/volt-typhoon
- Cybersecurity in Oil and Gas – SLB https://www.slb.com/insights/cybersecurity-the-next-frontier-of-safety-in-oil-and-gas
- SCADA and Pipeline Security – Yokogawa https://www.yokogawa.com/in/library/resources/media-publications/cyber-security-for-pipelines-other-scada-systems/
- AI in Oil and Gas Security – Security Industry Association https://www.securityindustry.org/2025/12/16/smart-tech-for-the-oil-and-gas-sectors-how-ai-can-help-manage-millions-of-devices/
- Seceon aiSecOT360 for OT Security https://aavextechnology.com/products/seceon/aisecot360/

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

Kamna Srivastava

AI/ML Cybersecurity Engineer, Seceon Inc.

Kamna specializes in leveraging artificial intelligence and machine learning to protect IT, OT, IoT, and cloud infrastructures. Her work focuses on strengthening enterprise security, ensuring compliance with industry standards, and delivering measurable ROI through Seceon’s OTM Platform.