SEBI Red Alert Response Brief

Mapping SEBI Directives to Seceon OTM Capabilities

India's Securities and Exchange Board (SEBI) has issued a nationwide infosec red alert for 19 classes of regulated entities following the emergence of AI-driven vulnerability detection tools capable of identifying and exploiting weaknesses at machine speed. As financial institutions reassess their cybersecurity posture against rapidly evolving AI-accelerated threats, Seceon OTM provides a unified platform built to help organizations detect, respond to, and contain threats in real time. This brief maps key SEBI directives directly to Seceon OTM platform capabilities and demonstrates how organizations can strengthen cyber resilience while simplifying modern security operations.

Threat Context & Global Regulatory Action

Anthropic's Mythos AI bug-finding tool has triggered simultaneous regulatory action across five major global financial regulators. AI-driven vulnerability scanners can now identify and exploit weaknesses at machine speed, rendering traditional security postures obsolete overnight. SEBI has put 19 classes of regulated entities, from stock exchanges and mutual funds to merchant bankers and KYC agencies, on immediate alert.

India (SEBI)	USA (Treasury)	Singapore (MAS)	Australia (APRA)	Hong Kong (HKMA)
Red alert issued. 19 entity classes directed to act immediately.	US Treasury convened emergency meeting with the nation's banks.	Regulatory action initiated the same week. MAS issued formal guidance.	APRA issued a strongly worded mandate for AI risk strategies.	HKMA is working on new infosec guidance for AI-accelerated threats.

Seceon OTM Platform Performance

150M	≥70%	<60s	800+	70+
Events per sec processed by aiSIEM	Autonomous L1 alert resolution via SeraAI	Threat containment via aiSOAR 4.0	Data source connectors for telemetry	Global threat intelligence feeds

SEBI Directives Mapped to Seceon OTM Platform Capabilities

SEBI Directive 1

"Ensure patches are up to date and conduct audits of potential vulnerabilities."

Seceon OTM Response

Continuous Risk-Based Vulnerability Management

aiSIEM ingests telemetry from more than 800 connectors, instantly identifying unpatched systems that are being actively probed, not just cataloged. The VM/RBVM module (Beta Q2 2026) delivers continuous, risk-prioritized scanning designed to keep pace with AI-driven reconnaissance. Dynamic Threat Models continuously self-adjust, eliminating weeks of manual tuning and improving real-time threat visibility.

aiSIEM	VM/RBVM (Beta)	NDR	Dynamic Threat Models

SEBI Directive 2

"Conduct inventories of APIs and secure them."

Seceon OTM Response

API Behavior Baselining & Anomaly Detection

NDR performs deep packet inspection across all network traffic, including API calls. UEBA establishes behavioral baselines for every API endpoint and user, triggering alerts the moment those baselines are violated, whether by an external attacker or a compromised insider account.

NDR	UEBA	aiXDR-PMax	Deep Packet Inspection

SEBI Directive 3

"Run a serious SOC and take its advice through AI-augmented SOC transformation."

Seceon OTM Response

≥70% Autonomous L1 Resolution with SeraAI + aiSOAR 4.0

SeraAI, Seceon's AI Security Co-Pilot, resolves the majority of routine alerts without analyst intervention. aiSOAR 4.0 provides more than 500 automated playbooks with sub-60-second threat containment capabilities. This enables analysts to focus exclusively on high-fidelity, high-priority threats, even amid AI-accelerated attack volumes.

SeraAI	aiSOAR 4.0	aiMSSP	500+ Playbooks

SEBI Directive 4

"Harden systems by adopting zero-trust networking and running only essential services."

Seceon OTM Response

Continuously Enforced Zero Trust + Identity Threat Protection

The ZTA/ZTNA module (Q3 2026) operationalizes zero trust through continuously enforced policies integrated across identity, network, and endpoint telemetry. aiITDR and aiIDGuard help protect against credential theft, privilege escalation, and lateral movement techniques commonly used by AI-driven attackers following initial compromise.

ZTA/ZTNA	aiITDR	aiIDGuard	Zero Trust Policy

SEBI Directive 5
“Recalibrate risks for AI-accelerated threats and use AI as part of your infosec strategy.”
Seceon OTM Response
AI Fighting AI with Dynamic Threat Models + AI TRiSM (ADMP)
ADMP (AI Defense & Monitoring Platform), aligned with Gartner’s AI TRiSM framework, is designed to monitor AI systems for misuse, model poisoning, and adversarial manipulation. TI360 aggregates more than 70 global threat intelligence feeds to provide real-time contextual enrichment for every alert, enabling faster and more informed threat detection and response.

ADMP / AI TRiSM	TI360	Dynamic Models	SeraAI

SEBI Directive 6
“Review cybersecurity at third-party software vendors and ensure supply chain integrity.”
Seceon OTM Response
Cloud Posture Management + File Integrity Monitoring
CSPM/CDR monitors cloud environments across AWS, Azure, and GCP for misconfigurations and anomalous activity introduced through third-party integrations. FIM continuously monitors critical system files for unauthorized changes, while CMX360 automates compliance reporting for SEBI, RBI, and the DPDP Act to support ongoing regulatory readiness.

CSPM/CDR	FIM	CMX360	GRC Compliance

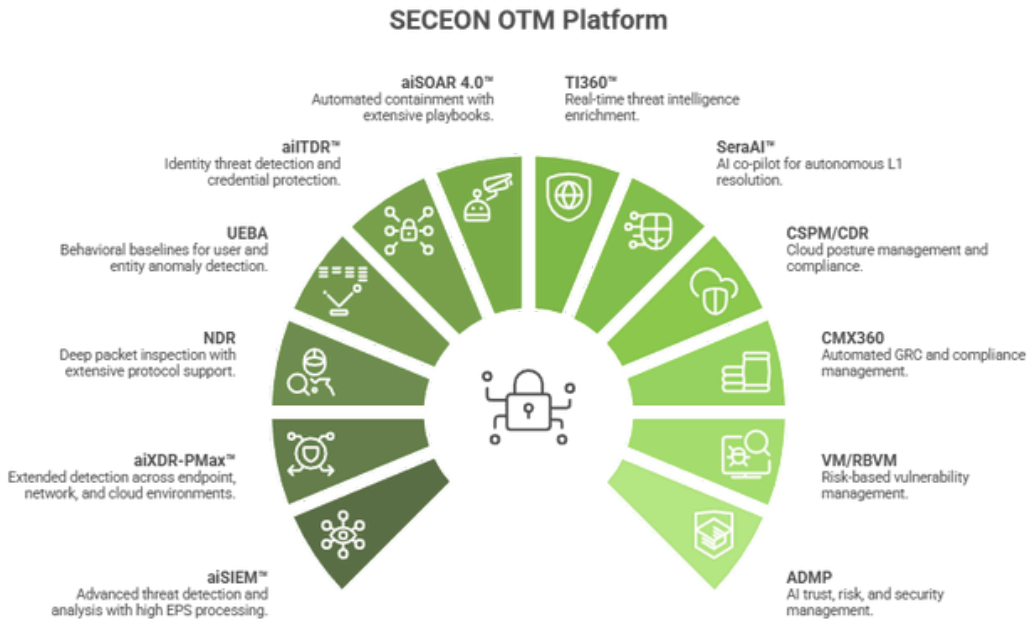
Complete SEBI Directive Compliance Matrix

SEBI Directive	Seceon Module	Capability	✓
Patch & Vulnerability Audit	VM/RBVM + aiSIEM	Continuous risk-based scanning and real-time active probe detection	✓
API Inventory & Security	NDR + UEBA	API behavior baselining, anomaly detection, and deep packet inspection	✓
AI-Augmented SOC Transformation	SeraAI + aiSOAR 4.0	≥70% autonomous L1 resolution with sub-60-second containment	✓
Zero Trust Architecture Adoption	ZTA/ZTNA + aiITDR	Continuously enforced identity-aware access control	✓

SEBI Directive	Seceon Module	Capability	✓
AI Threat Recalibration	ADMP + TI360	AI TRiSM, dynamic threat models, and 70+ threat intelligence feeds	✓
Third-Party / Supply Chain Risk	CSPM/CDR + FIM	Cloud posture management and file integrity monitoring	✓
Incident Reporting & TI Sharing	TI360 + CMX360	Real-time IOC sharing and automated regulatory reporting	✓
Continuous Vulnerability Management (AI)	VM/RBVM + SeraAI	AI-prioritized CVE remediation and autonomous triage	✓

Seceon OTM: A 25-Module Unified Security Platform

aiSIEM™ LIVE Dynamic threat models, 150M EPS processing	**aiXDR-PMax™ LIVE** Extended detection across endpoint, network, and cloud	**NDR LIVE** Deep packet inspection, 70+ protocol support	**UEBA LIVE** Behavioral baselines for users and entities
aiITDR™ LIVE Identity threat detection and credential protection	**aiSOAR 4.0™ LIVE** 500+ playbooks with sub-60s automated containment	**TI360™ LIVE** 70+ threat intel feeds with real-time enrichment	**SeraAI™ LIVE** AI co-pilot with ≥70% autonomous L1 resolution
CSPM/CDR LIVE Cloud posture management across AWS, Azure, and GCP	**CMX360 LIVE** Automated GRC, SEBI/RBI/DPDP compliance	**VM/RBVM BETA Q2** Risk-based vulnerability management	**ADMP LIVE** AI TRiSM for AI trust, risk, and security management



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, and aiXDR 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 850 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.



Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/

© 2026 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.