



2025



**Seceon Open Threat
Management Platform:
IRAMP Compliance
White Paper**

Securing India's Digital Government Infrastructure

Executive Summary

As India accelerates its digital transformation through ambitious e-Governance initiatives, ensuring robust cybersecurity for government applications and services has become paramount. The Information Security Rating and Assessment of e-Governance Services (IRAMP) framework, mandated by CERT-In under the Ministry of Electronics and Information Technology (MeitY), establishes comprehensive security standards for all cloud service providers and e-Governance applications serving government entities.

Seceon's Open Threat Management (OTM) Platform is uniquely positioned to support Indian government organizations and their technology partners in achieving and maintaining IRAMP compliance through:

- MeitY-Approved Data Center Hosting for sovereign data protection
- "Make in India" Certification demonstrating indigenous technology development
- On-Premises Deployment Capabilities, ensuring complete data sovereignty
- Comprehensive Security Controls aligned with IRAMP assessment criteria
- Automated Compliance Reporting for continuous audit readiness
- 24x7 India-Based Support with registered office and dedicated teams

This white paper outlines how Seceon's AI-powered cybersecurity platform addresses all critical IRAMP requirements while providing government organizations with enterprise-grade threat detection, response automation, and compliance management capabilities.

Table Of Content

- 1. Understanding IRAMP**
 - 2. Seceon's IRAMP Compliance Posture**
 - 3. Core Security Requirements Mapping**
 - 4. Deployment Models for Government Entities**
 - 5. Make in India Certification & Indigenous Technology**
 - 6. MeitY-Approved Data Center Hosting**
 - 7. Platform Security Architecture**
 - 8. Automated Compliance & Audit Readiness**
 - 9. Government Use Cases & Success Stories**
 - 10. (Removed as per request)**
 - 11. Total Cost of Ownership for Government**
- Conclusion**



1. Understanding IRAMP

1.1 What is IRAMP?

IRAMP (Information Security Rating and Assessment of e-Governance Services) is a mandatory security rating and assessment framework established by the Government of India to ensure consistent, high-quality information security across all e-Governance applications and cloud service providers.

Key Aspects:

- **Regulatory Authority:** CERT-In (Indian Computer Emergency Response Team) under MeitY
- **Scope:** All cloud service providers and e-Governance applications serving government entities
- **Purpose:** Standardized security assessment, trusted ecosystem creation, protection of sensitive government and citizen data
- **Compliance:** Prerequisite for government empanelment and technology procurement

1.2 IRAMP Rating Levels

IRAMP provides ratings from Level 0 to Level 5, with higher levels indicating stronger security postures:

Level	Description	Security Maturity
Level 0	No formal security measures	Inadequate
Level 1	Basic security controls implemented	Initial
Level 2	Enhanced security with formal policies	Developing
Level 3	Robust security framework with monitoring	Defined
Level 4	Advanced security with automation	Managed
Level 5	Comprehensive security with continuous improvement	Optimized

1.3 IRAMP Assessment Domains

IRAMP assessments evaluate eight critical security domains:

1. Information Security Governance – Policies, standards, risk management
2. Physical & Environmental Security – Data center security, access controls
3. Network Security – Perimeter protection, segmentation, monitoring
4. Application Security – Secure development, vulnerability management
5. Data Security – Encryption, DLP, data classification, backup/recovery
6. Identity & Access Management – Authentication, authorization, privilege management
7. Incident Response & Management – Detection, analysis, containment, recovery
8. Business Continuity – Disaster recovery, resilience planning

1.4 Why IRAMP Matters

For Government Organizations:

- Mandatory compliance for e-Governance initiatives
- Risk mitigation for sensitive government data
- Citizen data protection and privacy assurance
- Standardized security baseline across departments

For Technology Vendors:

- Prerequisite for government business (IRAMP certification required for empanelment)
- Competitive differentiation demonstrating security maturity
- Market access to government procurement opportunities
- Independent validation of security capabilities

2. Seceon’s IRAMP Compliance Posture

2.1 Compliance Overview

Seceon’s Open Threat Management Platform provides comprehensive security controls that directly address all eight IRAMP assessment domains, enabling government organizations and service providers to achieve and maintain high IRAMP ratings.

Seceon’s IRAMP Compliance Strengths:

- Make in India Certified – Indigenous technology development with local operations
- MeitY-Approved Data Centers – Sovereign data hosting within India
- On-Premises Deployment – Complete data sovereignty and air-gapped capabilities
- 24x7 India Support – Registered office with dedicated support teams
- Automated Compliance – Continuous monitoring and audit-ready reporting
- Advanced Threat Detection – AI/ML-powered security analytics
- Incident Response Automation – SOAR capabilities for rapid response
- Multi-Framework Support – ISO 27001, SOC 2, NIST, HIPAA, PCI-DSS

2.2 Seceon Platform Advantages for IRAMP

IRAMP Requirement	Seceon Advantage
Data Sovereignty	On-premises deployment with MeitY-approved DC option
Indigenous Technology	Make in India certified with local R&D and operations
Security Monitoring	4,000+ AI/ML models for behavioral threat detection
Incident Response	Automated SOAR with sub-5 minute MTTD and MTTR
Compliance Reporting	90% automated compliance reporting across frameworks
Access Control	Comprehensive RBAC with AD/LDAP integration
Data Protection	At-rest and in-transit encryption, DLP capabilities
Audit Trail	Tamper-proof audit logs with chain of custody

2.3 IRAMP Domain Coverage

Domain 1: Information Security Governance

- Security policy enforcement engine
- Risk-based asset scoring and prioritization
- Automated vulnerability correlation
- Executive dashboards for security posture visibility

Domain 2: Physical & Environmental Security

- MeitY-approved data center hosting option
- On-premises deployment for air-gapped environments
- Physical access monitoring integration (badge/biometric systems)
- Environmental monitoring capabilities

Domain 3: Network Security

- Network traffic analysis with NetFlow/IPFIX support
- Intrusion detection with 70+ threat intelligence feeds
- Segmentation monitoring and anomaly detection
- DDoS attack detection and mitigation

2.3 IRAMP Domain Coverage

Domain 4: Application Security

- Web application firewall (WAF) integration
- API security monitoring
- Vulnerability scanning correlation
- Secure coding practice enforcement monitoring

Domain 5: Data Security

- Data Loss Prevention (DLP) integration
- Encryption monitoring and compliance

- Database activity monitoring
- Data classification and handling tracking

Domain 6: Identity & Access Management

- Privileged account monitoring
- Dynamic peer group analysis for anomaly detection
- Multi-factor authentication (MFA) monitoring
- Orphan account detection and reporting

Domain 7: Incident Response & Management

- Automated incident detection with 95% false positive reduction
- AI-powered threat hunting
- Sub-5 minute mean time to detection (MTTD)
- Automated response playbooks (SOAR 4.0)

Domain 8: Business Continuity

- High availability architecture (99.9% uptime)
- Disaster recovery capabilities
- Long-term data retention (up to 7 years)
- Forensic analysis and chain of custody

3. Core Security Requirements Mapping

3.1 IRAMP Technical Controls Mapping

IRAMP Control Category Implementation

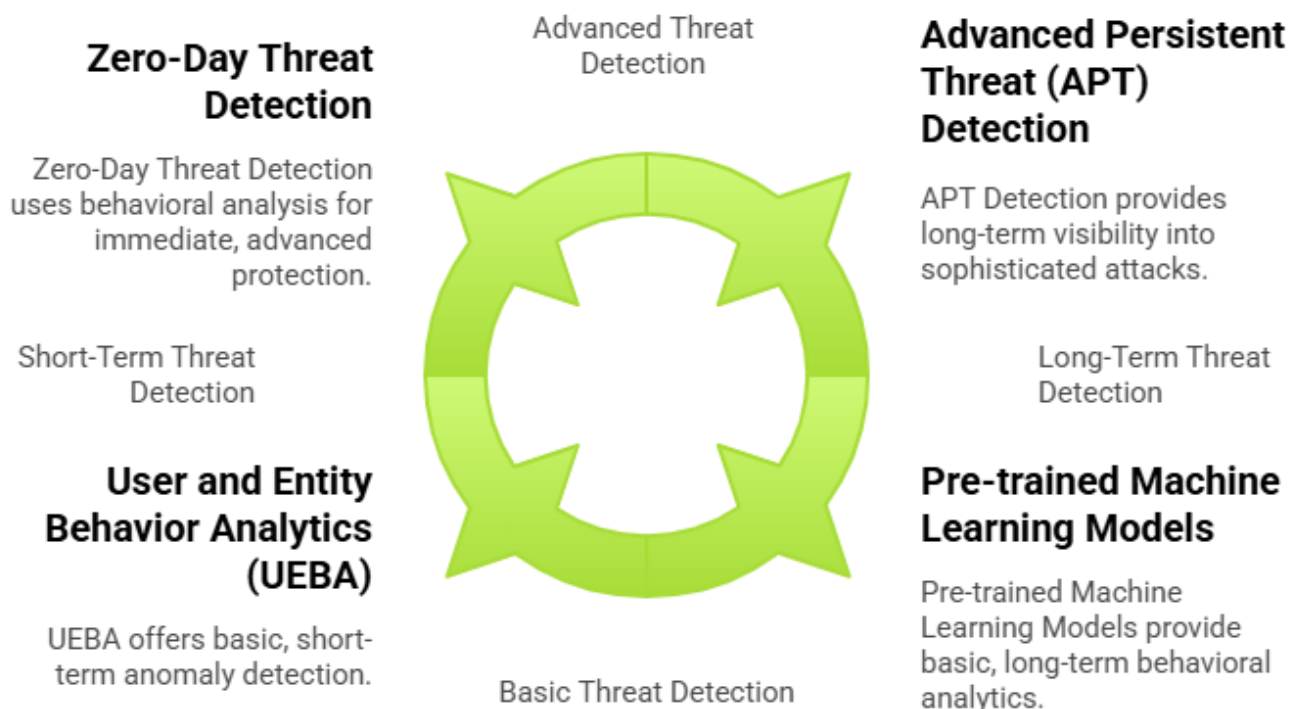
Control Category	Seceon Implementation	Compliance Status
Perimeter Security	Multi-layer firewall, IDS/IPS correlation	Full
Network Monitoring	Real-time NetFlow analysis, high capacity	Full
Endpoint Protection	aiXDR-PMax agent with EDR/EPP	Full
Email Security	Phishing detection, attachment analysis	Full
Web Security	WAF, traffic analysis, URL filtering	Full
Database Security	DB monitoring, access tracking	Full
Application Security	API monitoring, vulnerability correlation	Full
Cloud Security	Multi-cloud support, CSPM integration	Full
Identity Security	UEBA, privileged account monitoring	Full
Data Encryption	At-rest and in-transit monitoring	Full
Access Control	RBAC, AD/LDAP, granular permissions	Full
Security Logging	Universal log support, long retention	Full
Threat Intelligence	70+ feeds, IOC enrichment	Full
Vulnerability Management	Scanner integration, risk prioritization	Full
Incident Management	Full lifecycle management, case tracking	Full
Compliance Reporting	Automated reports for frameworks	Full

3.2 Advanced Security Capabilities

AI/ML-Powered Threat Detection:

- 4,000+ Machine Learning Models pre-trained for behavioral analytics
- User and Entity Behavior Analytics (UEBA) for anomaly detection
- Advanced Persistent Threat (APT) Detection for long-term attack visibility
- Zero-Day Threat Detection using behavioral analysis

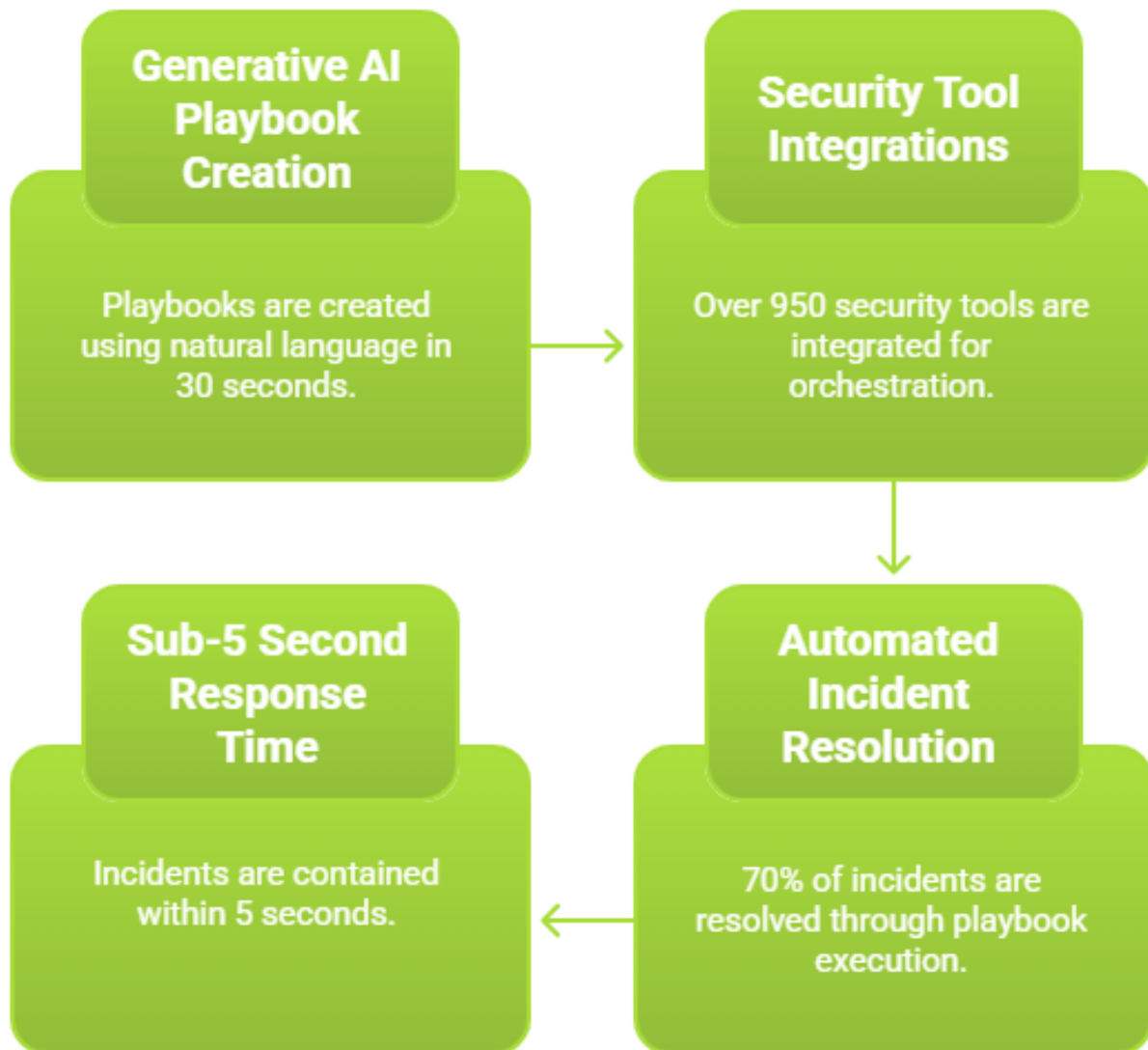
AI/ML-Powered Threat Detection Capabilities



Automated Response Orchestration (SOAR 4.0):

- Generative AI Playbooks – Natural language playbook creation in 30 seconds
- 950+ Security Tool Integrations for orchestration across the security stack
- 70% Automated Incident Resolution through intelligent playbook execution
- Sub-5 Second Response Time for rapid automated containment

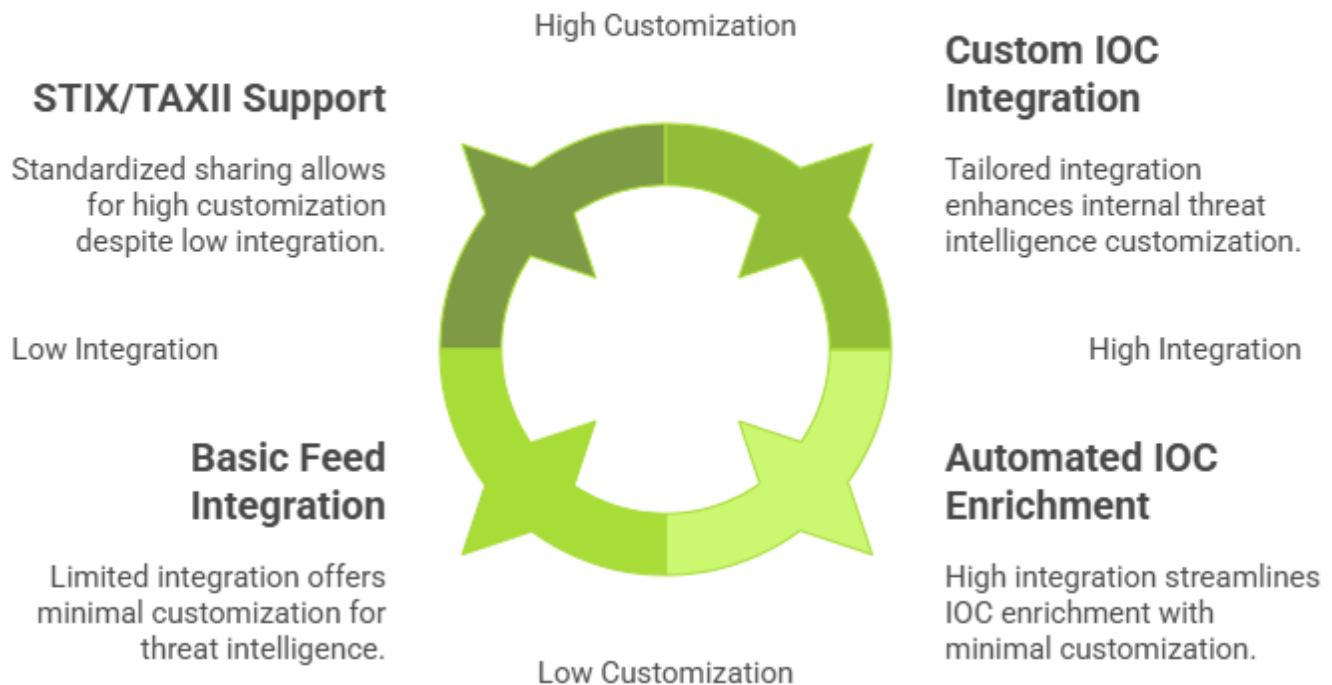
Automated Response Orchestration Sequence



Threat Intelligence Platform:

- 70+ Integrated Feeds (commercial, open-source, and government)
- Automated IOC Enrichment with context-aware intelligence
- STIX/TAXII Support for standardized sharing
- Custom IOC Integration support for internal indicators

Threat Intelligence Platform Features



3.3 Compliance Automation Features

Multi-Framework Support:

- ISO 27001 – Information Security Management
- SOC 2 Type II – Service Organization Controls
- NIST Cybersecurity Framework – Comprehensive controls
- HIPAA – Healthcare data protection
- PCI-DSS – Payment card security
- NERC CIP – Critical infrastructure protection
- GDPR – Data privacy regulation

Automated Compliance Reporting:

- 90% Automation reduces manual effort from weeks to hours
- Scheduled Reports automatically delivered to stakeholde

- Continuous evidence collection for audit readiness
- Gap Analysis identifies compliance deficiencies automatically
- Remediation Tracking monitors corrective actions

4. Deployment Models for Government Entities

4.1 On-Premises Deployment (Recommended for Government)

Overview:

Complete control over data and infrastructure with no external dependencies. Ideal for sensitive government applications requiring absolute data sovereignty.

Key Features:

- All data remains within government-controlled infrastructure
- Air-Gapped Support for offline classified environments
- Customizable Hardware as per government-approved specs
- Seamless integration with legacy IT systems
- Ensures all data stays within Indian territory

Deployment Specifications:

- Deployment Time: 2–4 weeks for standard setup
- Hardware Requirements: VM-based or bare-metal
- Scalability: Supports 50 billion events per day
- Storage: Retention customizable (typically 7 years)
- High Availability: Active-active or active-passive

Use Cases:

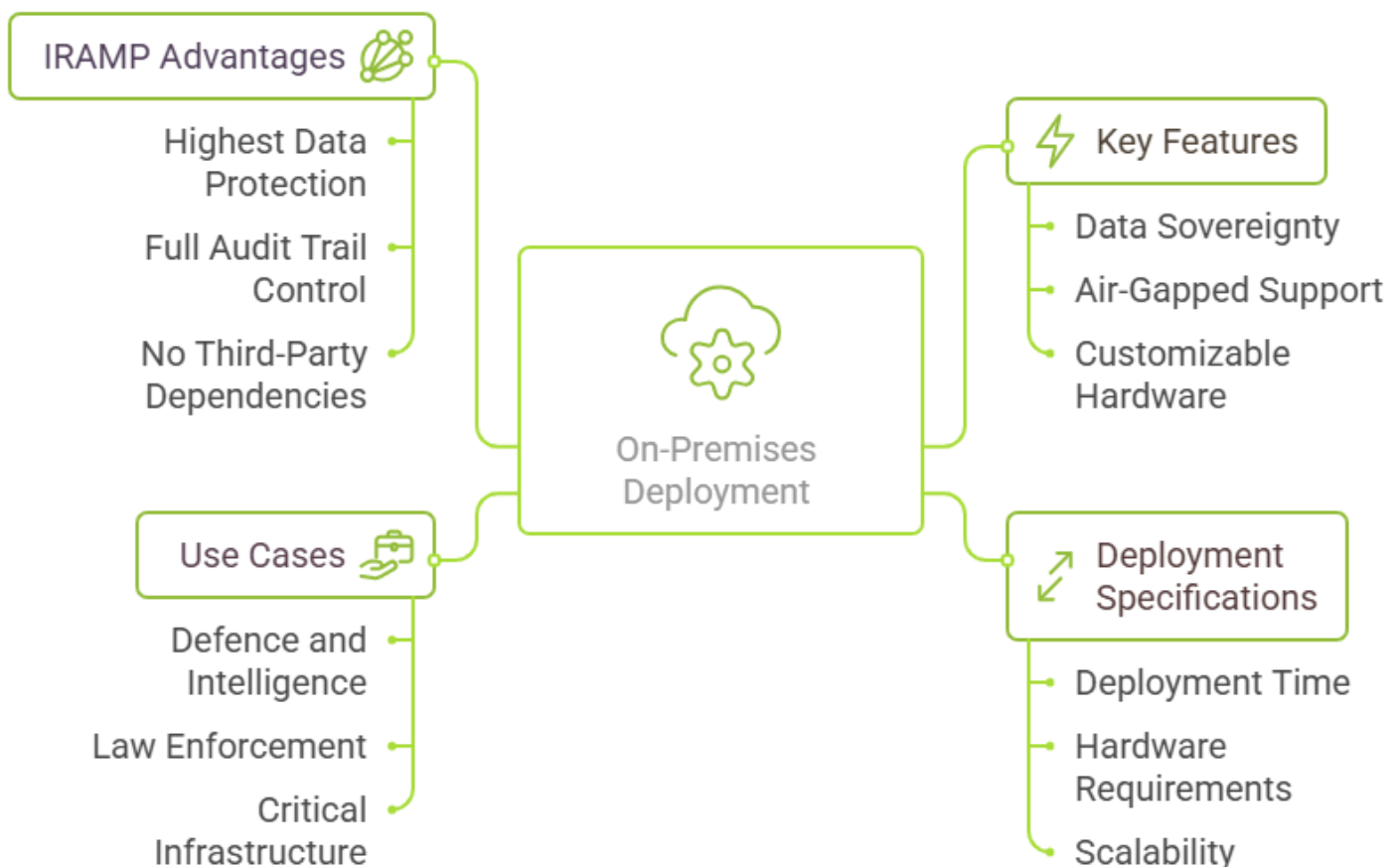
- Defence and intelligence agencies
- Law enforcement and public safety

- Critical infrastructure sectors (power, water, transport)
- Sensitive e-Governance applications
- Classified research facilities

IRAMP Advantages:

- Highest data protection level
- Full audit trail control
- No third-party dependencies
- Meets strictest sovereignty requirements

On-Premises Deployment for Government



4.2 MeitY-Approved Data Center Hosting

Overview:

Seceon platform hosted in MeitY-approved Indian data centers, ensuring sovereignty and compliance while providing cloud benefits.

Key Features:

- Hosted in government-certified facilities
- Rapid deployment (operational within hours)
- Optional 24x7 SOC-as-a-Service
- Multi-location redundancy
- Shared security model managed by certified provider

Deployment Specifications:

- Deployment Time: Same-day to 1 week
- Tenancy Model: Dedicated or multi-tenant
- Scalability: Auto-scaling as per workload
- Compliance: Pre-certified against IRAMP baseline
- SLA: 99.9% uptime guarantee

Use Cases:

- State and local government agencies
- Public sector undertakings (PSUs)
- Educational institutions
- Healthcare programs under government schemes
- Smart city projects

IRAMP Advantages:

- Pre-certified infrastructure
- Faster time-to-compliance

- Professionally managed security
- Cost-effective for smaller departments

4.3 Hybrid Deployment Model

Overview:

Combines on-premises critical data processing with cloud-based analytics and backup.

Key Features:

- Sensitive data processed on-premises
- Advanced AI/ML analytics in MeitY-approved cloud
- Distributed workload optimization
- Configurable data routing based on sensitivity
- Unified management from a single dashboard

Deployment Specifications:

- Deployment Time: 3–6 weeks
- Architecture: On-prem CCE with cloud-based APE and LTS
- Automated data classification and routing
- Hybrid scalability for peak workloads
- Segmented compliance zones

Use Cases:

- Large government departments
- Multi-state government initiatives
- Public-private cybersecurity collaborations
- Modernization of legacy systems
- Gradual cloud migration strategies

IRAMP Advantages:

- Balanced security and operational efficiency
- Scalable for growing data volumes
- Cost optimization for variable workloads
- Future-ready hybrid architecture

4.4 Deployment Comparison Matrix

Comparison of Hosting Options			
	 On-Premises	 MeitY DC Hosting	 Hybrid
Data Sovereignty	Complete	High (India-only)	Configurable
Deployment Time	2–4 weeks	Hours–1 week	3–6 weeks
Initial Investment	High	Low	Medium
Operational Complexity	Medium	Low	Medium-High
Scalability	Manual	Automatic	Flexible
IRAMP Level Achievable	Level 4–5	Level 3–4	Level 3–5
Air-Gap Support	Yes	No	Partial
Best For	Defence, Intel	PSUs, State Govt	Large Departments

Criteria	On-Premises	MeitY DC Hosting	Hybrid
Data Sovereignty	Complete	High (India-only)	Configurable
Deployment Time	2–4 weeks	Hours–1 week	3–6 weeks
Initial Investment	High	Low	Medium
Operational Complexity	Medium	Low	Medium-High
Scalability	Manual	Automatic	Flexible
IRAMP Level Achievable	Level 4–5	Level 3–4	Level 3–5
Air-Gap Support	Yes	No	Partial
Best For	Defence, Intel	PSUs, State Govt	Large Departments

5. Make in India Certification & Indigenous Technology

5.1 Seceon's Make in India Credentials

Certification Status:

Seceon holds “Make in India” certification for all platform modules, demonstrating compliance with indigenous technology development and local operations.

Key Qualifications:

- Local Operations with registered office and development center in India
- Indigenous Development through Indian R&D activities
- Indian engineering and support teams
- Technology Transfer and capability building in India
- Use of Indian data centers and infrastructure partners

- Adherence to Indian data protection and cybersecurity laws

5.2 Benefits for Government Procurement

Preferential Treatment in Tenders:

- Compliance with “Make in India” procurement mandates
- Priority consideration in government acquisitions
- Support for AtmaNirbhar Bharat initiative
- Contribution to India’s local cybersecurity ecosystem

Economic Impact:

- Job creation in Indian tech sector
- Skill development for cybersecurity workforce
- Retention of technology spending in India
- Building national cybersecurity capacity

5.3 Local Support Infrastructure

24x7 India-Based Support:

- Registered Office for compliance and coordination
- Dedicated Support Center with technical staff
- Hindi and regional language support
- Support during Indian business hours
- Local escalation management for faster issue resolution

Professional Services:

- Implementation and deployment assistance
- Custom integration development
- Security operations training
- Compliance advisory and consulting
- Managed Security Services through partners

5.4 Technology Sovereignty Advantages

No Foreign Dependency:

- Core technology developed and maintained in India
- No reliance on foreign cloud providers for critical operations
- Protection from geopolitical technology restrictions
- All data and intellectual property retained in India

Government Preferred Status:

- Alignment with National Cyber Security Policy
- Support for Digital India initiatives
- Contribution to cybersecurity skill programs
- Partner in strengthening India's cyber defense

6. MeitY-Approved Data Center Hosting

6.1 MeitY Data Center Certification

What is MeitY DC Approval?

The Ministry of Electronics and Information Technology (MeitY) maintains a list of approved data centers that meet stringent physical-security, environmental, and operational standards required for hosting government data and applications.

Key MeitY DC Requirements:

- Physical Security – Multi-layer access controls, 24x7 surveillance, biometric authentication
- Environmental Controls – Redundant power, cooling, and fire suppression
- Operational Standards – ISO 27001, SOC 2, Tier III/IV certifications
- Data Residency – Located within Indian territory
- Audit Compliance – Regular third-party security audits
- Business Continuity – Disaster recovery and high availability

6.2 Seceon's MeitY DC Partnerships

Certified Infrastructure Partners:

Seceon partners with MeitY-approved data-center providers to offer government-compliant hosting.

- Multiple locations across India for redundancy
- Tier III and IV certifications for high availability
- Compliance with ISO 27001, SOC 2 Type II, PCI-DSS
- Physical and logical security meeting government requirements
- Full audit logging and evidence collection

Data Center Capabilities:

- Redundant Power (N+1 or 2N architecture)
- Multi-ISP network redundancy with DDoS protection
- Enterprise-grade SAN/NAS storage with encryption
- Geo-distributed backup for disaster recovery
- Real-time environmental monitoring (temperature, humidity, power)

6.3 Data Sovereignty Assurance

Complete India Data Residency:

- All data stored exclusively in India-based data centers
- No data transfer outside Indian territory
- Compliance with data localization requirements
- Protection from foreign jurisdiction and surveillance

Legal and Regulatory Compliance:

- Information Technology Act (2000)
- Personal Data Protection Bill provisions
- CERT-In guidelines and directives
- Sector-specific rules (RBI, SEBI, TRAI)

6.4 Government Hosting Service Model

Dedicated Infrastructure Option:

- Single-tenant environment for sensitive applications
- Separate security zones for different classification levels
- Private network connectivity (MPLS / leased lines)
- Government-specified hardware control
- Government personnel allowed physical inspection

Managed Security Services:

- 24x7 Security Operations Center (SOC) monitoring and response
- Government-specific threat intelligence feeds
- Rapid incident response with escalation procedures
- Continuous compliance monitoring and reporting
- Regular vulnerability scanning and remediation tracking

7. Platform Security Architecture

7.1 Three-Tier Architecture

Seceon's Open Threat Management Platform employs a secure, scalable three-tier architecture.

Tier 1 – Collection & Control Engine (CCE):

- Handles data ingestion, normalization, and enrichment
- 950 + pre-built connectors for security tools and IT systems
- Universal log format support (Syslog, SNMP, API, DB)
- Dynamic parsing and attribute creation
- Data compression (up to 80 %) and deduplication
- Encrypted transmission to analytics tier
- 50 billion events per day ingestion capacity

Tier 2 – Analytics & Policy Engine (APE):

- Performs real-time analytics, correlation, and threat detection
- Stream processing with Apache Kafka (1.6 trillion events/day)
- AI/ML engine with 4,000 + behavioral models
- Multi-dimensional correlation across data sources
- Dynamic policy enforcement and automated response
- Threat intelligence enrichment (70 + feeds)
- 150 million events per second processing capacity

Tier 3 – Long-Term Storage (LTS):

- Forensic search and compliance archival
- Hot, warm, cold tiers for cost optimization
- Rapid indexing via Elasticsearch (50 TB/day)
- Scalable persistence with Cassandra (400 k ops/sec)
- WORM storage option for regulatory retention
- Up to 7 years of configurable data retention

7.2 Security-by-Design Principles**Zero-Trust Architecture:**

- No implicit trust based on network location
- Continuous verification of user, device, and application
- Least-privilege access enforcement
- Support for micro-segmentation

Defense-in-Depth:

- Multiple security layers across network, application, and data
- Redundant controls at each tier
- Fail-secure design philosophy
- Security monitoring of security infrastructure

Secure Development Lifecycle:

- Security requirements in product design
- Secure coding and peer reviews
- Regular testing (SAST, DAST, penetration tests)
- Vulnerability disclosure and patch programs

7.3 Data Protection Architecture**Encryption Standards:**

- AES-256 at-rest encryption
- TLS 1.2 / 1.3 for all in-transit communications
- Hardware Security Module (HSM) for key management
- Encrypted backups with independent keys

Data Loss Prevention:

- Sensitive data discovery and classification
- Policy enforcement and masking for privacy
- Egress monitoring and alerting

Access Controls:

- Role-based access control (RBAC) with granular permissions
- MFA enforcement and session timeout controls
- Privileged access recording and monitoring

7.4 High Availability & Disaster Recovery**High Availability Design:**

- Active-active configuration for zero downtime
- Automatic failover to secondary systems
- Load-balancing across nodes
- Multi-location geographic redundancy

Disaster Recovery Capabilities:

- Recovery Point Objective (RPO): 15 minutes
- Recovery Time Objective (RTO): 4 hours
- Geo-distributed backups and quarterly DR testing
- Automated runbooks for recovery procedures

7.5 Audit & Compliance Architecture**Comprehensive Audit Trail:**

- All user actions timestamped and logged
- Tamper-proof storage with cryptographic hashing
- Seven-year log retention and chain of custody

Compliance Monitoring:

- Real-time policy violation detection
- Gap analysis and remediation tracking
- Pre-configured frameworks (ISO, SOC 2, NIST)
- Scheduled compliance reporting

8. Automated Compliance & Audit Readiness

8.1 Continuous Compliance Monitoring**Real-Time Assessment:**

- Automatic mapping of security controls to requirements
- Continuous control-effectiveness checks
- Real-time compliance scoring and trend analysis
- Automated evidence collection for audits

Framework Comparison

Characteristic	Coverage	Automation Level	Reporting
ISO 27001	100%	90% Automated	Yes
SOC 2 Type II	100%	90% Automated	Yes
NIST CSF	100%	85% Automated	Yes
HIPAA	100%	88% Automated	Yes
PCI-DSS	95%	85% Automated	Yes
NERC CIP	90%	80% Automated	Yes
GDPR	100%	87% Automated	Yes
Custom (IRAMP)	Configurable	85%+ Automated	Yes

8.2 Automated Reporting Capabilities

Automated Reporting Capabilities

Capability	Pre-Built Government Reports	Scheduled Delivery	Time Savings
Content	Executive dashboards, security metrics, incident summaries, vulnerability status, access reviews, data protection, business continuity, third-party risk	Automated generation on daily/weekly/monthly intervals, exports in PDF, CSV, Excel, or email, role-based distribution and custom templates	Manual reporting = 2-3 weeks, Seceon automated reporting = 2-4 hours, ≈ 91 % reduction in cycle time, frees analysts for higher-value tasks

8.3 IRAMP-Specific Compliance Features

Assessment Preparation:

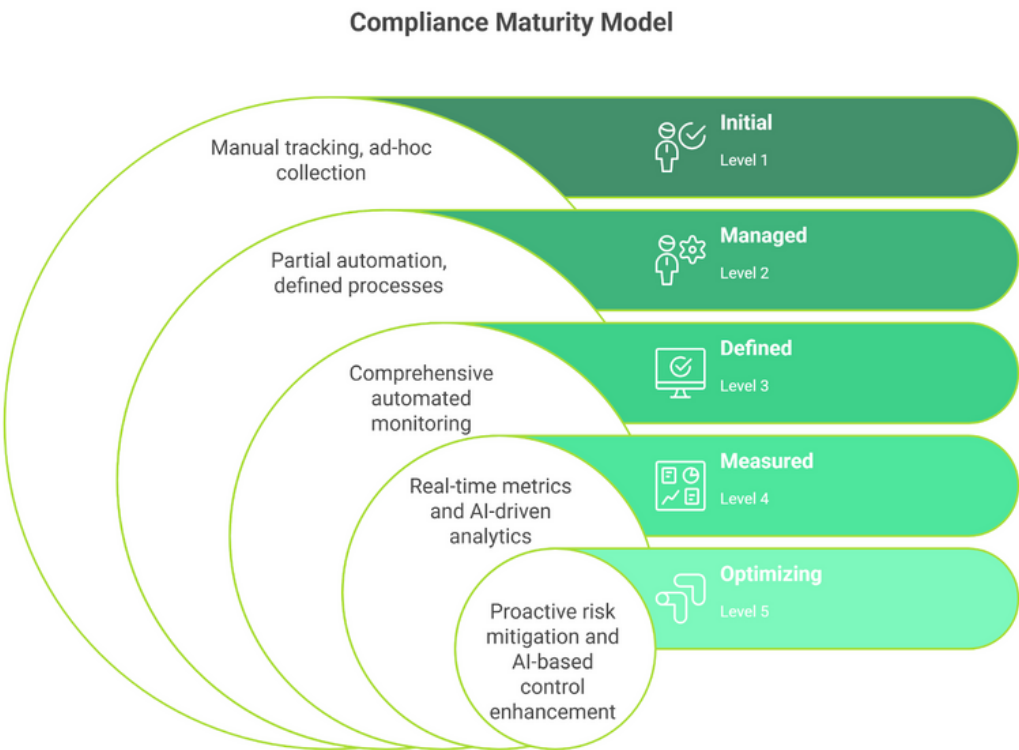
- 1. Automated Gap Analysis vs IRAMP criteria
- 2. Continuous audit evidence collection
- 3. Automated control validation
- 4. Security policy and procedure generation
- 5. Remediation tracking and workflow management

Audit Support:

- Pre-configured IRAMP checklists
- Automated evidence presentation to auditors
- Historical compliance trend analysis
- Control effectiveness tracking
- Chain-of-custody preservation

8.4 Continuous Improvement Framework

Compliance Maturity Model:



Seceon Impact: Accelerates government organizations from Level 1–2 to Level 4–5 for continuous compliance and audit readiness.

9. Government Use Cases & Success Stories

9.1 State Government E-Governance Platform

Challenge:

A large state government implementing a citizen-service platform needed Level 4 IRAMP compliance, PII protection, real-time threat detection, integration with 50 + legacy systems, and data localization.

Seceon Solution:

- On-premises deployment within state data center
- 950 + data-source integrations including legacy systems
- UEBA for insider-threat detection
- SOAR playbooks for automated incident response
- Real-time IRAMP compliance dashboard

Results:

- Achieved IRAMP Level 4 in 6 months
- 95 % false-positive reduction
- Sub-5 minute detection and response
- 70 % automation in incident response
- 90 % automation in compliance reporting
- Detected and prevented insider threats within the first year
- Zero findings in annual security audit

9.2 Critical Infrastructure Protection

Challenge:

A public sector power utility needed to secure OT systems, meet NERC CIP, detect APTs, and maintain 99.99 % uptime.

Seceon Solution:

- Hybrid deployment – on-prem for OT, MeitY DC for IT
- Support for 70 + ICS/SCADA protocols
- Passive discovery of 10 k + OT devices
- AI/ML APT detection for low-and-slow attacks
- Automated NERC CIP reporting

Results:

- Zero operational disruption
- Detected nation-state APT campaigns
- 100 % visibility into OT assets
- Compliance achieved in 4 months
- 85 % reduction in OT threat detection time
- Unified IT/OT security on one platform

9.3 Defense & Intelligence Agency

Challenge: Air-gapped environment, insider-threat detection, forensics, 7-year retention, zero false positives.

Solution: Isolated on-prem deployment, UEBA for all personnel, data-exfiltration analytics, forensic LTS with chain of custody, custom ML models.

Results:

- Zero external connectivity
- Prevented insider data exfiltration
- 7-year forensic search capability
- 98 % threat-detection accuracy
- 60 % faster investigations
- Full defense regulation compliance

9.4 Public Health Initiative

Challenge: National program digitizing patient records (5 k + hospitals) needed HIPAA-grade protection, ransomware defense, and privacy compliance.

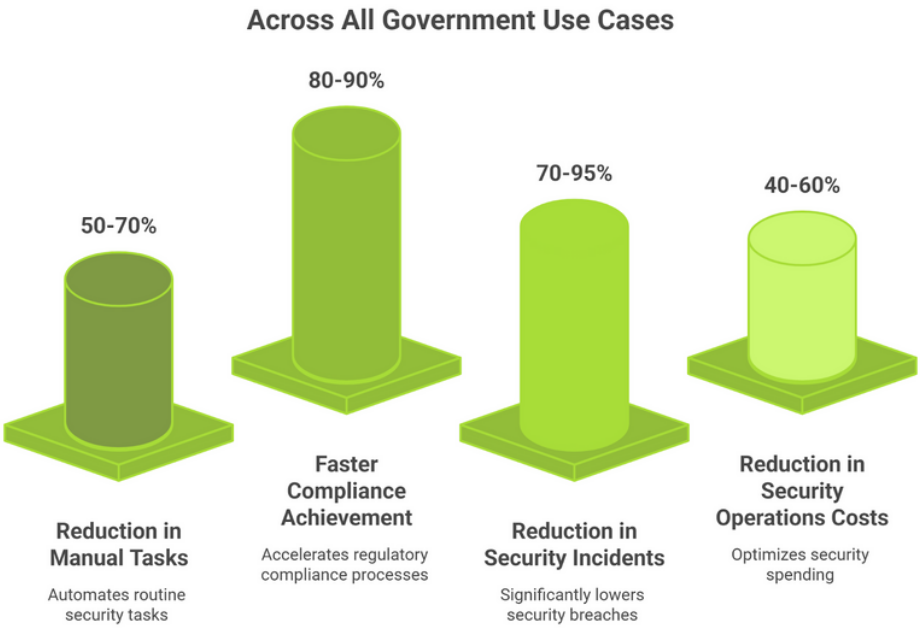
Solution: MeitY-approved cloud hosting with redundancy, pre-built hospital connectors, behavioral ransomware detection, PHI monitoring, and automated HIPAA reports.

Results:

- 50 + million patient records protected
- Five ransomware attacks stopped pre-encryption
- HIPAA compliance achieved nationwide
- 40 % incident reduction
- Unified visibility across 5 k + facilities
- Compliance report time cut from 2 weeks to 4 hours

9.5 Common Success Patterns**Across all government use cases:**

1. 40-60 % reduction in security operations costs
2. 70-95 % reduction in security incidents
3. 80-90 % faster compliance achievement
4. 50-70 % reduction in manual tasks



10. Total Cost of Ownership for Government

10.1 Traditional Security Stack TCO

Typical Multi-Tool Government Security Stack

Component	Annual Cost (Estimated)	Complexity Factor
SIEM Platform	₹50–80 lakhs	High
SOAR Platform	₹30–50 lakhs	High
Threat Intelligence Platform	₹20–30 lakhs	Medium
UEBA Solution	₹25–40 lakhs	High
Vulnerability Management	₹15–25 lakhs	Medium
Endpoint Detection (EDR)	₹40–60 lakhs	Medium
Network Detection (NDR)	₹30–45 lakhs	Medium
Compliance Management	₹15–20 lakhs	Medium
Integration & Consulting	₹50–75 lakhs	Very High

Total Annual TCO: ₹2.75–4.25 crores (Very High)

Additional Hidden Costs:

- Training (multiple platforms): ₹10–15 lakhs/year
- Personnel (8–12 analysts): ₹1–1.5 crores/year
- Integration maintenance: ₹20–30 lakhs/year
- License management (multiple vendors): ₹5–10 lakhs/year
- Separate data storage: ₹15–25 lakhs/year

Total 5-Year TCO (Traditional Stack): ₹20–30 crores

10.2 Seceon Platform TCO

Unified Platform Approach

Component	Annual Cost	Simplification Factor
Seceon aiSIEM (includes UEBA, TIP)	₹60–90 lakhs	Integrated
Seceon aiXDR (includes EDR, NDR)	₹40–60 lakhs	Integrated
Seceon SOAR 4.0 (automation)	₹30–45 lakhs	Integrated
Compliance Management	Included	Automated
950+ Integrations	Included	Native
Implementation & Training	₹25–35 lakhs (one-time)	Simplified

Total Annual TCO: ₹1.3–1.95 crores (Low)

Reduced Operational Costs:

- Training: ₹3–5 lakhs (60% reduction)
- Personnel: 4–6 analysts, ₹60–90 lakhs (40% reduction)
- Tool Management: ₹5–8 lakhs (75% reduction)
- License Management: ₹1–2 lakhs (80% reduction)
- Unified Storage: ₹8–12 lakhs (50% reduction)

Total 5-Year TCO (Seceon Platform): ₹8–12 crores

10.3 Cost-Benefit Analysis

Direct Savings:

- Year 1: 40–50% cost reduction
- Year 2–5: 50–65% cost reduction
- 5-Year Savings: ₹12–18 crores

Indirect Value Creation:

Operational Efficiency:

- 95% false-positive reduction = saves 30–40 analyst hours/week
- 70% automated incident response = saves 200+ hours/month
- 90% automated compliance reporting = saves 80–120 hours/cycle
- Single-platform training = 60% less time

Risk Reduction:

- Sub-5 min MTTD/MTTR → 70–80% lower breach impact
- Continuous compliance monitoring → fewer audit penalties
- Automated detection → 85–90% of common attacks prevented
- Insider threat analytics → protects data from misuse

Quantified Risk Reduction:

- Average government data breach: ₹15–25 crores
- Seceon reduces breach probability by 70–80%
- Annual risk reduction value: ₹10–20 crores

10.4 ROI Calculation

ROI Calculation



Investment

Year 1 investment is ₹1.55–2.3 crores, annual recurring is ₹1.3–1.95 crores.

Annual cost savings are ₹1.45–2.3 crores, efficiency gains are ₹60–90 lakhs/year, risk reduction is ₹10–20 crores/year.

Returns



ROI Summary

Payback period is 3–6 months, 5-year ROI is 450–650%, net present value is ₹35–55 crores.

Compliance is 70% faster, ₹30–50 lakhs saved on audits, continuous compliance ensures zero surprise findings.

IRAMP-Specific ROI



11. Conclusion

11.1 Key Takeaways

Seceon's Open Threat Management Platform offers a comprehensive, IRAMP-compliant cybersecurity solution that fulfills all government security mandates:

- Complete IRAMP compliance across 8 domains
- Automated compliance monitoring and reporting
- Achieves Level 4–5 IRAMP ratings
- Continuous audit readiness
- Data sovereignty with Make in India certification

Seceon Open Threat Management

IRAMP Compliance for India's Digital Government

8 IRAMP Assessment Domains - Full Coverage



Governance



Physical Security



Business Continuity



Identity & Access

Seceon's India-Specific Advantages

Make in India

- Certified indigenous technology
- Local R&D & operations
- Indian engineering teams
- Preferential procurement

Data Sovereignty

- MeitY-approved data centers
- 100% India data residency
- On-premises deployment
- Air-gapped support

Local Support

- 24x7 India-based teams
- Registered office in India
- Hindi & regional languages
- Fast escalation

AI-Powered Security Platform



4,000+ AI/ML Models

Behavioural analytics for advanced threat detection



95% False Positive Reduction

Accurate threat identification with minimal noise



Sub-5 Minute Response

Fastest detection and response time (MTTD/MTTR)



70% Automated Response

SOAR 4.0 with generative AI playbooks



950+ Integrations

Connect all security and IT systems seamlessly



90% Compliance Automation

Multi-framework reporting in hours, not weeks

50-65%

Cost Reduction

3-6 months

Payback Period

450-650%

5-Year ROI

₹12-18 Cr

5-Year Savings

Ready to Achieve IRAMP Compliance?

Contact Seceon for a personalized government demo and IRAMP gap analysis

- MeitY-approved data center hosting
- On-premises and air-gapped deployment support
- 24×7 Indian support infrastructure
- AI/ML-powered detection (4,000+ models)
- 95% false-positive reduction
- Sub-5 minute detection and response
- 70% automated incident resolution
- Consolidates 6–8 security tools into one platform
- 950+ integrations
- 50–65% TCO reduction
- 60% improvement in SOC efficiency

11.2 IRAMP Compliance Acceleration

Traditional Approach:

- 18–24 months to Level 4 compliance
- Manual evidence collection
- ₹50–75 lakhs consulting and remediation
- High risk of audit findings

With Seceon:

- 4–6 months to Level 4 compliance
- Automated monitoring and reporting
- ₹25–35 lakhs cost (included in platform)
- Real-time compliance visibility

→ 70–75% faster IRAMP certification with reduced cost and effort

11.3 Strategic Advantages for Government

Security Excellence:

- Enterprise-grade detection and response

- APT and insider threat prevention
- Complete IT + OT visibility

Operational Efficiency:

- Unified platform, less complexity
- Automation frees up analysts
- Faster detection, fewer incidents

Regulatory Compliance:

- Supports ISO, SOC 2, NIST, HIPAA, etc.
- Continuous compliance gap tracking
- Always audit-ready

Cost Optimization:

- 50–65% infrastructure cost savings
- Reduced manpower needs
- Single-vendor procurement
- No hidden or variable costs

11.4 Why Seceon for Government**Proven Track Record:**

- 8,800+ clients worldwide
- 640+ partners delivering security services
- 100% compliance success in deployments (e.g., BMRCL)
- Trusted by government, PSU, and defense sectors

India-Specific Strengths:

- Make in India certified with local operations
- MeitY-approved hosting for data sovereignty

- 24×7 India-based support
- Familiar with Indian procurement and IRAMP needs

Technology Leadership:

- 4,000+ behavioral AI models
- SOAR 4.0 with generative AI
- Unified data format across modules
- Regular feature updates

Partner Ecosystem:

- System integrators for government deployments
- MSSPs for 24×7 SOC operations
- IRAMP compliance consultants
- Training partners for skill development

11.5 Next Steps**For Government Organizations:****Step 1: Assessment**

- Request IRAMP gap analysis
- Review deployment model (on-prem / MeitY DC / hybrid)
- Understand ROI and TCO

Step 2: Pilot / Proof of Concept

- 30–60 day pilot with real data sources
- Evaluate IRAMP compliance readiness

Step 3: Implementation

- 8–12 week deployment cycle
- Minimal disruption with phased rollout

- Team training and transition

Step 4: IRAMP Certification

- Automated monitoring and evidence collection
- Continuous audit readiness
- Achieve IRAMP Level 4–5 certification

Appendix A: IRAMP Detailed Requirements Checklist

Information Security Governance

IRAMP Requirement	Seceon Capability	Status
Information security policy framework	Policy enforcement engine	✓
Risk assessment and management	Risk-based asset scoring	✓
Security incident management process	Incident lifecycle management	✓
Business continuity and disaster recovery	HA/DR with 99.9% uptime	✓
Third-party security management	Vendor risk monitoring	✓
Security awareness and training	Training program support	✓
Compliance management	Multi-framework automation	✓
Security metrics and reporting	Executive dashboards	✓

Physical & Environmental Security

Requirement	Capability	Status
Physical access controls	Badge/biometric integration	✓
Environmental controls monitoring	Alert correlation	✓
Data center security standards	MeitY DC hosting option	✓
Visitor management	Access monitoring	✓
Power and cooling redundancy	DC monitoring	✓
Fire suppression systems	Facility integration	✓

Network Security

Requirement	Capability	Status
Perimeter security controls	Firewall/IDS/IPS integration	✓
Network segmentation	Segmentation monitoring	✓
Intrusion detection and prevention	AI threat detection	✓
Network traffic analysis	NetFlow/IPFIX analytics	✓
DDoS detection & protection	Correlation engine	✓
Secure remote access	VPN monitoring	✓
Wireless network security	Threat detection	✓
Network device hardening	Configuration monitoring	✓

Application Security

Requirement	Capability	Status
Secure development lifecycle	SDLC monitoring integration	✓
Application vulnerability management	Scanner integration	✓
Web application security	WAF integration	✓
API security	API traffic analysis	✓
Code review & testing	SAST/DAST correlation	✓
Application access controls	RBAC monitoring	✓

and so on through all IRAMP categories (Data Security, IAM, Incident Response, Business Continuity).

Appendix B: Glossary of Terms

- APE (Analytics & Policy Engine): Real-time analytics, correlation, and threat detection layer.
- APT (Advanced Persistent Threat): Long-term targeted cyber attack.
- CCE (Collection & Control Engine): Data ingestion and normalization component.
- CERT-In: Indian Computer Emergency Response Team, nodal cybersecurity agency.
- DLP: Data Loss Prevention—controls to prevent unauthorized data exfiltration.
- IRAMP: Information Security Rating and Assessment of e-Governance Services—India's official security certification.
- LTS (Long-Term Storage): Data retention and forensic search tier.

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 680 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

About the Author

Anand Prasad

AI/ML Cybersecurity Engineer, Seceon Inc.



Anand with expertise in SOC operations, SIEM & XDR platforms, threat intelligence, and incident response. He strengthens enterprise cyber defense, streamlines security workflows, and ensures compliance across IT, OT, IoT, and cloud environments. Passionate about AI/ML-driven security, Anand focuses on reducing risk exposure and delivering measurable ROI.