TRINETRA CYBER DEFENSE

VISION

Security Information & Event Management Platform

SOLUTION PROPOSAL

Next-Generation, Intelligence-Led Cyber Threat Detection

"See Everything. Miss Nothing. Respond in Seconds."

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

India's digital economy is growing at an unprecedented pace — and so is the threat landscape. Every day, thousands of cyberattacks target organisations of all sizes: ransomware cripples operations, data breaches expose customer records, and phishing campaigns drain accounts. Yet most businesses — from agile startups to established enterprises — continue to operate without the tools needed to detect, contain, and recover from these threats in time.

VISION, developed by Trinetra Cyber Defense, is India's next-generation Security Information and Event Management (SIEM) platform. Purpose-built for Indian organisations, it delivers enterprise-grade threat detection at a fraction of the cost of global alternatives such as Splunk or Microsoft Sentinel — with the added advantage of complete data sovereignty.

VISION does not merely collect security logs — it thinks, analyses, and acts. It continuously monitors every corner of your network, identifies suspicious behaviour in real time, and automatically triggers containment actions before damage can spread. Deployed on your own infrastructure, your sensitive data never leaves your control.

80–95%	**<60 sec**	**11+**	**100%**
proven across deployments	*from anomaly to alert*	*log source types natively*	*no foreign cloud dependency*
Reduction in Manual Security Effort	Threat Detection Time	Supported Format Adapters	On-Premise Data Sovereignty

Key Outcomes Delivered

- **Faster Threat Detection:** Identify intrusions and anomalies within seconds, not hours or days.
- **Automated Response:** Contain threats automatically — no manual intervention required.
- **Complete Visibility:** One unified dashboard for all devices, servers, applications, and users.
- **Reduced Security Costs:** Replace multiple expensive point-solutions with one unified platform.
- **Compliance Readiness:** Stay audit-ready with automatic reporting for ISO 27001 and CERT-In.
- **Data Sovereignty:** Your security data stays on your servers — fully within your control.

2. THE CHALLENGE — WHY CYBERSECURITY IS FAILING

India recorded over 1.5 million cybersecurity incidents in 2024 alone, with financial losses exceeding ■20,000 Crore. The majority affected organisations that had some security tools in place — yet were still breached. The reason: fragmented, slow, reactive security operations cannot keep pace with modern, automated cyberattacks.

1. Invisible Threats

Security logs from firewalls, servers, applications, and endpoints exist in isolation. Without a unified view, attackers move freely within networks for weeks undetected.

2. Alert Fatigue

Existing tools generate hundreds of alarms daily. Teams waste hours on false positives, missing genuine threats buried within the noise.

3. Slow Manual Response

When a breach is detected, manual escalation and containment takes hours or days. By then, data has been stolen or systems encrypted by ransomware.

4. Prohibitive Cost of Global Solutions

Enterprise SIEMs like Splunk cost several Crores per year, requiring dedicated certified engineers. This is out of reach for most Indian SMEs and startups.

5. Data Privacy & Sovereignty Risks

Cloud-only solutions send sensitive business data to overseas servers, creating regulatory, confidentiality, and national sovereignty concerns.

6. Compliance Burden Without Tools

CERT-In mandates, ISO 27001 requirements, and sectoral regulations demand detailed audit logs and incident reports — a massive burden without the right platform.

> The attacker's window of opportunity is measured in **minutes**. The average organisation's window of detection is measured in **weeks**. VISION closes this gap — permanently.

3. INTRODUCING VISION — THE SOLUTION

VISION is a unified cybersecurity operations platform that collects, analyses, and responds to threats across your entire digital environment — in real time. Designed specifically for Indian organisations: affordable, deployable on your own infrastructure, and built to meet Indian regulatory standards from the ground up.

Think of VISION as a round-the-clock Security Operations Centre running inside your own walls — one that never sleeps, never gets fatigued, and acts the moment a threat is confirmed. It brings threat detection, automated response, compliance management, and forensic investigation into one seamless, sovereign platform.

Our Design Philosophy

■ See Everything

VISION ingests logs and telemetry from every source — servers, firewalls, endpoints, cloud services, applications, and more. Nothing remains invisible.

■ Understand Everything

Intelligent analysis separates genuine threats from routine activity, delivering clear, prioritised alerts — not thousands of meaningless notifications.

■ Respond Instantly

Automated response playbooks isolate infected machines, block malicious connections, and notify your team the moment a threat is confirmed — in seconds, not hours.

■ Keep Control

All data stays on your servers. No foreign cloud. No third-party access. Full sovereignty over your most sensitive security information — always.

4. CORE CAPABILITIES

VISION is composed of ten specialised capability modules. Together they provide complete protection — from the moment a threat enters your environment to the final compliance report.

Unified Log Collection

VISION accepts security data from over 11 different source types — Windows and Linux servers, firewalls, routers, email gateways, web applications, and cloud services — with the widest format support in its class, requiring no expensive custom connectors.

Intelligent Threat Detection

Rather than relying solely on pre-set rules, VISION learns normal behaviour of your users and systems over time. Deviations — unusual logins, abnormal data transfers — are flagged immediately, catching sophisticated attacks that rule-based systems miss.

AI-Powered Alert Triage

VISION's autonomous triage engine examines every alert in context, assigns a priority score, and surfaces only the incidents that truly require human attention. Alert fatigue is eliminated. Your team focuses exclusively on what matters.

Automated Threat Response (SOAR)

When a confirmed threat is detected, VISION acts — not just notifies. Pre-configured response playbooks automatically isolate the affected system, block the attacker's connection, and generate a complete incident summary for your team.

Network Enforcement

VISION enforces security policies directly on your network infrastructure. When a device is identified as compromised, it is quarantined at the network level immediately — without any manual intervention.

Attack Pattern Recognition

VISION identifies coordinated attack campaigns spanning multiple systems or time periods, enabling detection of multi-stage Advanced Persistent Threats (APTs) that would otherwise appear as isolated, unrelated events.

Threat Intelligence Integration

VISION connects to global and national threat intelligence feeds, cross-referencing activity in your environment against known attacker infrastructure and active threat actor profiles.

GRC & Compliance Reporting

Built-in compliance modules automatically track adherence to ISO 27001, CERT-In guidelines, and sector-specific requirements. Audit-ready reports available on demand.

Offline / Air-Gap Operation

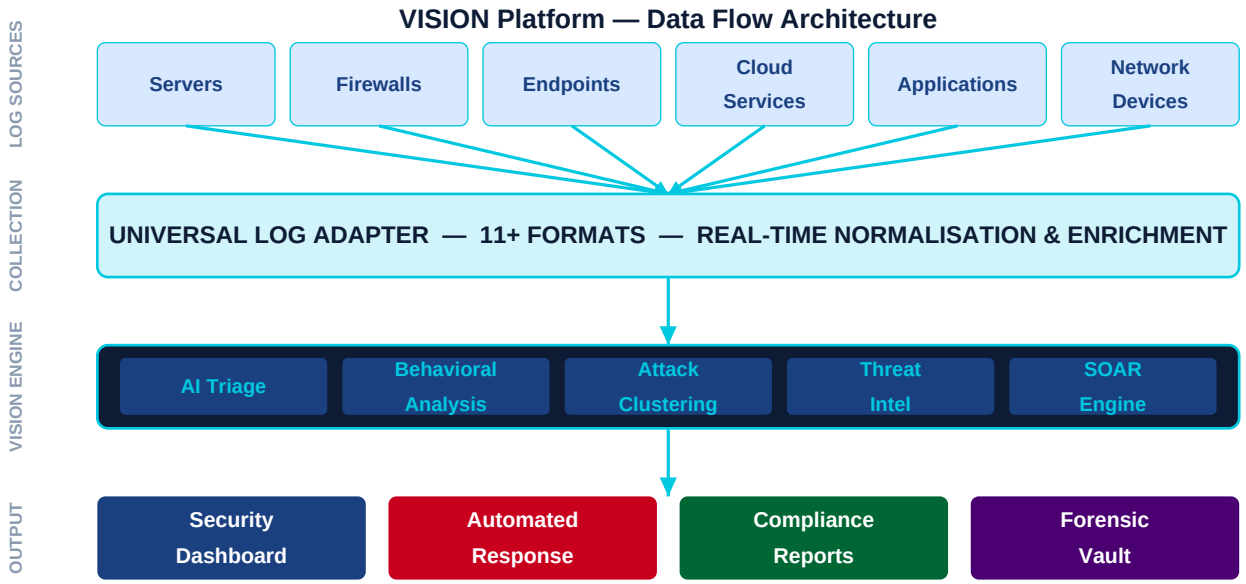
VISION operates in fully offline, air-gapped environments — a critical capability for defence establishments, power plants, and critical infrastructure where internet connectivity is restricted. Unique among all competing global SIEM platforms.

Institutional Security Memory

Every investigation, alert, and incident is preserved in VISION's central intelligence vault. New threats are instantly cross-referenced against historical activity, dramatically accelerating investigation and response.

5. HOW VISION WORKS — ARCHITECTURE & DATA FLOW

VISION operates as a continuous, always-on security intelligence engine. From the moment data enters the system to the final resolution of an incident, every step is automated, documented, and auditable. The diagram below illustrates the end-to-end data flow.



Step-by-Step Investigation Flow

Step 1	**Data Collection** Security logs from all connected devices — servers, firewalls, workstations, applications, and cloud services — are gathered automatically around the clock.
Step 2	**Normalisation & Enrichment** Raw log data is standardised across all formats and enriched with threat intelligence context before entering the analysis engine.
Step 3	**Intelligent Analysis** The analytics engine evaluates all data against behavioural baselines, known threat patterns, and live threat intelligence feeds. Suspicious activity is identified and correlated across sources.

Step 4	**Alert Triage & Prioritisation** AI-powered triage assigns a severity score to each anomaly. Only confirmed or high-probability threats are escalated to your security team.
Step 5	**Automated Response** For confirmed threats, response playbooks trigger automatically: isolating systems, blocking connections, and preserving forensic evidence — all within seconds.
Step 6	**Incident Documentation** A structured incident report captures the full timeline, affected systems, attacker activity, and all response actions — automatically.
Step 7	**Compliance Reporting** All security activity is logged in an immutable audit trail. ISO 27001 and CERT-In reports are available on demand at any time.

6. VISION IN ACTION — REAL-WORLD SCENARIOS

Scenario A: Ransomware Attack on a Mid-Sized Company

It is 11 PM on a Tuesday. The IT team has gone home. A ransomware payload — delivered via a phishing email clicked three hours earlier — begins encrypting critical files.

11:04 PM	VISION detects unusual file-access patterns: thousands of files modified in rapid succession. Behavioural analysis confirms this is not normal activity.
11:04 PM	VISION's automated response playbook triggers instantly. The infected server is isolated from the network. The ransomware cannot reach any other system.
11:05 PM	The IT Manager receives an SMS and email alert with a complete incident summary: account used, server affected, and containment action taken.
11:05 PM	VISION generates a forensic evidence report — preserving all logs, file-access records, and network connections for the subsequent investigation.
Result	Total damage: one isolated server. Recovery time: under 2 hours. Without VISION, the entire network would likely have been encrypted and inoperable by morning.

Scenario B: Insider Data Theft at a Growing Startup

A fast-growing SaaS startup suspects a departing employee may have exfiltrated customer data. HR raises the concern on a Friday afternoon. VISION enables an immediate investigation without any external forensic engagement.

Hour 1	The security team queries VISION's intelligence vault for the employee's account activity over 30 days. A complete timeline is generated within seconds.
Hour 1	VISION identifies: 14 days ago, 2,800 customer records were downloaded between 7–9 PM — outside normal working hours. The activity was flagged but unreviewed.
Hour 2	VISION displays the exact files accessed, the device used, the originating IP address, and identifies files were transferred to a personal cloud storage service.
Hour 3	A court-admissible incident report is generated with digital evidence hashes, timestamps, and chain-of-custody record — ready for the legal team.

Result	An investigation that would have taken weeks of manual analysis is completed in under 4 hours. Evidence is structured and ready for legal proceedings.

7. KEY BENEFITS & OUTCOMES

■ Dramatic Reduction in Manual Effort

VISION automates the most time-consuming security tasks: log collection, correlation, triage, and reporting. Security teams previously spending 80% of their time on administrative work can now focus entirely on strategic decisions and genuine incident response.

■ Real-Time Detection and Automated Containment

The average organisation takes 200+ days to detect a breach. With VISION, detection happens within seconds. Automated containment reduces response time from hours to under a minute.

■ Enterprise Security for Every Organisation

VISION allows a small security team to effectively monitor an entire enterprise environment. Startups and MSMEs gain the capabilities of a large Security Operations Centre at a fraction of the cost — democratising enterprise-grade security.

■ Stronger Legal & Compliance Position

Every incident, alert, and response action is documented automatically, providing the audit trail required for ISO 27001 certification, CERT-In compliance, and legal proceedings — without additional manual effort.

■ Reduced Risk of Catastrophic Loss

Ransomware, data breaches, and infrastructure attacks can cost organisations tens of Crores in damages, fines, and reputational harm. Early detection and automated containment dramatically reduces the blast radius of any security incident.

■ Improved Customer & Stakeholder Trust

A mature, certified security posture builds confidence with customers, investors, and regulators — a critical competitive advantage in today's data-sensitive environment.

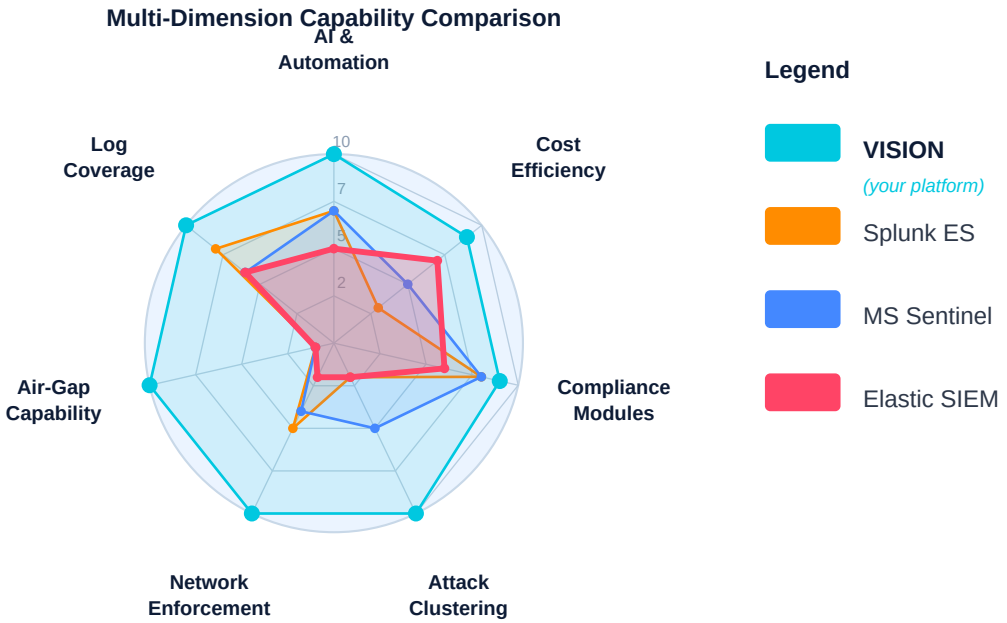
8. WHY VISION — COMPETITIVE ADVANTAGE

VISION has been independently benchmarked against the world's leading SIEM platforms. The results demonstrate superior or equivalent capability across every critical dimension — at a price accessible to Indian organisations.

Feature	VISION	Splunk ES	IBM QRadar	MS Sentinel	Elastic SIEM
AI-Autonomous Triage	**Full ✓**	Partial	Partial	Partial	Limited
Real-Time Behavioural Profiling	**Native ✓**	Add-on	Add-on	✓	Plugin
SOAR Auto-Response	**Native ✓**	✓	✓	✓	Limited
Firewall / Network Enforcement	**Native ✓**	Add-on	Add-on	Partial	✗
Log Source Support	**11 ✓**	9	8	7	6
Air-Gap / Offline AI	**Native ✓**	✗	✗	✗	✗
On-Premise Deployment	✓	✓	✓	Cloud Only	✓
Attack Clustering	**Native ✓**	✗	✗	Partial	✗
Open Source Core	✓	✗	✗	✗	✓
Zero-Config AI Pipeline	✓	✗	✗	Partial	✗
Threat Intel Integration	**Native ✓**	✓	✓	✓	✓
GRC / Compliance Modules	✓	✓	✓	✓	Partial

✓ = Full native support | Partial = Limited capability | ✗ = Not available

Visual Capability Comparison — Radar Chart



Scores are based on independent capability benchmarking across 7 key operational dimensions. VISION's Air-Gap / Offline AI capability and native Attack Clustering are unique differentiators not offered by any competing global platform.

9. DEPLOYMENT MODEL

VISION is engineered to fit your organisation's infrastructure. It integrates seamlessly into your existing environment without requiring you to replace or restructure anything.

On-Premise Deployment

VISION is installed entirely within your own data centre or server room. All security data is processed and stored on your infrastructure. No data ever leaves your premises. Recommended for banking, defence, government, and any organisation with strict data sovereignty requirements.

Hybrid Deployment

For organisations with a mix of on-premise infrastructure and cloud services, VISION's hybrid model monitors both environments from a single unified dashboard. Cloud service logs are securely ingested while all analysis and storage remain on your own servers.

Air-Gap / Offline Deployment

For critical infrastructure with no internet connectivity — power plants, manufacturing facilities, defence installations — VISION operates fully offline, including its AI intelligence engine. This capability is unique among all competing global SIEM platforms.

Data Sovereignty Guarantee: Under all deployment models, your raw security data, incident records, and compliance logs are stored exclusively on infrastructure under your direct control. Trinetra Cyber Defense personnel have no access to your data without explicit, documented authorisation.

10. TRAINING & IMPLEMENTATION

VISION is deployed and operational within **14 days** of contract signing. Our engineering team manages the entire technical installation so your staff can focus on operations from Day 1.

Week 1: Setup & Integration

Engineers install and configure VISION on your designated servers, connect all data sources, and conduct a baseline security assessment.

Week 2: Testing & Customisation

Validated with your real data. Alert thresholds and response playbooks customised to your specific environment and risk profile.

Week 2: Training Delivery

Role-specific training for three groups: First Responders, Security Analysts, and Leadership. Practical, scenario-based, and conducted on-site.

Day 14: Go-Live

VISION goes live. Your team is fully operational, with a dedicated on-boarding engineer available throughout the first 30 days.

Training Curriculum

Module	Audience	Focus Areas
Module A — First Responder	IT Staff & Help Desk	Alert review, basic investigation, escalation procedures
Module B — Security Analyst	Security / Technical Team	Advanced investigation, threat hunting, playbook management
Module C — Leadership	CISOs, Directors, Senior Management	Executive dashboards, compliance reporting, strategic oversight

11. CLIENT PREREQUISITES — SUCCESS READINESS CHECKLIST

To ensure VISION's 14-day deployment guarantee is met without delays, the following prerequisites must be confirmed by the client before the deployment engagement begins. Our team will conduct a readiness review during the initial kick-off call.

> **Note:** Items marked in this checklist are the client's responsibility. Trinetra Cyber Defense will provide guidance on any item during the pre-deployment readiness review — typically conducted 5 business days before the start date.

A. Infrastructure & Hardware

- ■ Dedicated server provisioned and accessible (see server specifications in proposal)
- ■ Server rack space, adequate cooling, and UPS / power backup in place
- ■ Intranet connectivity confirmed between deployment server and investigator workstations
- ■ Operating system licensing secured (Windows Server / Linux RHEL)
- ■ At least one static IP address assigned to the VISION server on the internal network

B. Network & Access

- ■ Network firewall rules documentation prepared (outbound/inbound ports for log ingestion)
- ■ IT / Security point of contact nominated as the VISION System Administrator
- ■ Admin-level access credentials prepared for initial configuration
- ■ Log forwarding enabled or schedulable on key devices (firewalls, Active Directory, etc.)
- ■ Inventory of all log sources prepared (device type, IP, OS, log format)

C. Organisational Readiness

- ■ Security team of 2–5 users nominated and available for Day 1 training
- ■ Executive sponsor confirmed for the project and available for kick-off call
- ■ Schedule cleared for two-day on-site training (to be agreed with Trinetra team)
- ■ Internal incident response procedure (basic) documented or available for review
- ■ Data retention and security policy agreed with management before go-live

D. Compliance & Legal

- ■ Non-Disclosure Agreement (NDA) with Trinetra Cyber Defense executed
- ■ ISO 27001 scope defined (if the deployment is for certification purposes)

- CERT-In compliance obligations and reporting obligations reviewed internally
- Legal team informed of court-admissible report format requirements (if applicable)

What happens if prerequisites are not met? If any infrastructure prerequisite is outstanding at the start of deployment, the 14-day go-live timeline will be extended by the equivalent number of working days. Trinetra Cyber Defense will notify the client immediately upon identification of any readiness gap.

12. SUPPORT & MAINTENANCE

VISION is a mission-critical platform. Our support framework ensures your security operations are never interrupted — with guaranteed response times and continuous platform improvement throughout the subscription period.

- **Helpdesk Support:** Email and ticketing support for operational queries, user issues, and configuration assistance — available during business hours with extended coverage for critical issues.
- **Remote Technical Support:** Remote support for software issues, integration problems, and performance tuning, with a guaranteed response within 2 hours for high-priority matters.
- **Critical Incident Response:** For system-down scenarios, our engineering team responds within 1 hour and resolves within 4 hours — guaranteed in writing.
- **Continuous Platform Updates:** VISION receives regular updates: new threat detection rules, improved AI models, compatibility with new log sources, and security patches. All included in the subscription.
- **Quarterly Business Reviews:** Every quarter, our team reviews your VISION deployment — covering system health, threat trends, optimisation recommendations, and roadmap updates.

Service Level Commitments

Priority	Situation	Response	Resolution
Critical	System completely unavailable	< 1 Hour	< 4 Hours
High	Core detection or response feature down	< 2 Hours	< 8 Hours
Medium	Non-critical functionality or UI issue	< 4 Hours	< 2 Business Days
Low	Feature request or cosmetic issue	< 1 Business Day	Next Release

13. COMPLIANCE & DATA TRUST

Organisations deploying VISION gain not just security capabilities, but a structured foundation for regulatory compliance, legal defensibility, and auditor confidence.

■ ISO 27001 Compliance Support

VISION's built-in GRC module maps security controls directly to ISO 27001 requirements. All required evidence — access logs, incident records, configuration change records — is automatically captured, enabling organisations to achieve and maintain certification with significantly reduced manual effort.

■ CERT-In Compliance (2022 Directions)

VISION supports compliance with CERT-In's mandatory cyber incident reporting and log retention directions. All security events are logged with required metadata, and incident reports can be generated in the prescribed format on demand.

■ Immutable Audit Trail

Every action within VISION — every search, every alert reviewed, every response triggered — is recorded in a tamper-proof audit log that cannot be modified or deleted, providing an irrefutable evidence trail for legal or disciplinary proceedings.

■ Court-Ready Incident Reports

VISION generates structured incident reports containing timestamps, digital evidence hashes, chain-of-custody documentation, and a clear incident timeline — accepted as electronic records under the Information Technology Act.

■ Data Privacy (DPDP Act 2023)

VISION's architecture complies with India's Digital Personal Data Protection Act. Data is processed only for defined security purposes, retention policies are configurable, and all access is strictly role-based and audited.

14. COMMERCIAL SUMMARY & PRICE BREAKDOWN

VISION is offered as a subscription-based service — transparent, predictable, and scalable. Unlike traditional enterprise security tools requiring large upfront capital and expensive specialist staff, VISION is priced to deliver enterprise-grade security within the budget of Indian startups, MSMEs, and growing organisations.

Plan Overview

Plan	Coverage	Annual (+ GST)	3-Year / yr (+ GST)	Best For
Starter	Up to 1 Network / 10 Servers	**■50,00,000**	■42,50,000	Startups & Small Offices
Professional	Up to 3 Networks / 50 Servers	**■75,00,000**	■63,75,000	MSMEs & Mid-Market
Enterprise	Unlimited Networks / Servers	**■1,00,00,000**	■85,00,000	Large Orgs & Critical Infra

Detailed Price Breakdown — What You Are Paying For

The following breakdown shows exactly how the subscription fee is allocated across each component — ensuring full transparency and allowing leadership to assess value against individual cost centres.

Component	Starter (■ Lakh)	Professional (■ Lakh)	Enterprise (■ Lakh)	Notes
Core SIEM Platform License	31.00	48.00	68.00	Annual software subscription for core detection & response modules
AI Intelligence Module	Included	Included	Included	Autonomous triage, behavioral profiling, attack clustering
Deployment & Configuration	6.50	8.50	12.00	On-site installation, integration, and firewall configuration

On-Site Training (2 days)	3.00	4.00	5.00	Role-specific training for up to 20 users across 3 modules
GRC & Compliance Module	4.00	6.50	8.00	ISO 27001, CERT-In, DPDP Act automated reporting
Annual Maintenance & Support	5.50	8.00	7.00	Updates, helpdesk, SLA-backed technical support
Subtotal (Pre-GST)	**50.00**	**75.00**	**1,00.00**	
GST @ 18%	**9.00**	**13.50**	**18.00**	Applicable as per GoI norms
Total (Incl. GST)	**59.00**	**88.50**	**1,18.00**	Annual payable amount

All amounts are in Indian Rupees (INR). GST charged as applicable. 3-year subscriptions save 15% on the software license component. Custom pricing available for government, defence, and multi-site deployments.

Included in Every Subscription

✓ Full access to all VISION platform modules (Modules 1–10)
✓ On-premise or hybrid deployment and end-to-end configuration
✓ 14-day rapid deployment and go-live guarantee
✓ Role-based training for up to 20 users across 3 modules
✓ Continuous platform updates and new threat detection rules
✓ Email and ticketing helpdesk support (business hours)
✓ ISO 27001 and CERT-In compliance reporting modules
✓ Immutable audit trail and court-ready incident report generation

15. CONCLUSION

The question for any organisation today is not whether a cyberattack will happen — it is when. The difference between a minor disruption and a catastrophic breach lies entirely in how quickly a threat is detected and contained.

VISION gives your organisation the capability to see threats in real time, respond in seconds, and build a defensible, compliant security posture — without the complexity, cost, or data sovereignty compromises of global enterprise platforms.

For Indian startups, MSMEs, and critical infrastructure organisations, VISION is a strategic investment in resilience. It is not merely a security tool — it is a force multiplier that empowers your team to operate with confidence in an increasingly hostile digital environment. Every organisation that deploys VISION builds not just better security, but a permanent institutional advantage: an intelligence asset that grows stronger with every case, every alert, and every incident resolved.

VISION by Trinetra Cyber Defense

See Everything. Miss Nothing. Respond in Seconds.

India's most capable, affordable, and sovereign SIEM platform — purpose-built for every Indian organisation across every sector and size.

To schedule a live demonstration or receive a customised proposal, please contact Trinetra Cyber Defense:

trinetracyberdefense.com
contact@trinetracyberdefense.com