threatsys LMS360 ai

ADVANCED CYBERSECURITY TRAINING FOR ORGANISATIONS

Threatsys LMS 360

Awareness · Compliance · Simulation · Proof

Role-based cybersecurity training that improves security awareness, supports regulatory compliance and protects organisational digital assets - delivered through one scalable platform.

- ROLE-BASED · EVIDENCE FOR EVERY AUDIT

+91 9668200222 support@threatsys.co.in www.threatsys.co.in

THREATSYS ONE AI

Your all-in-one cybersecurity suite, extraordinarily unified

SOC, GRC, CRM, AppSec, DPDP and LMS - unified under a single roof. One platform, one login, one intelligence layer powering every layer of your security posture.

threatsys soc360 ai

AI-Native Security Operations Console

AI SIEM, SOAR, FIM and XDR fused into one AI-driven response system with threat hunting and an agentic SOC assistant.

threatsys grc360 ai

Every risk. One record. All-in-one control.

Risk, policy and audit converged into one self-updating compliance cycle - audit automation, scoping and evidence.

threatsys DPDP360 ai

AI-Mastered DPDP Suite

Consent, rights, grievance SLAs, notices, DPIAs, vendor risk and evidence for the DPDP Act, 2023.

threatsys CRM360 ai

Effortless AI-powered delivery management

Every signal and interaction turned into one relationship - clients, engagements and delivery unified in one place.

threatsys appsec360 ai

Automated Application Security Testing

SAST, DAST, API testing and PTaaS with validated, evidence-backed findings across code and cloud.

threatsys LMS360 ai

THIS DECK

Building a cyber-ready workforce

Role-based cybersecurity training, compliance awareness and practical skilling delivered at organisational scale.

FOCUS · 1 OF 6

Your people are the control that fails first

Modern organisations run on digital systems, cloud platforms and connected work. That makes employees a critical part of the defence. LMS 360 delivers structured, role-based learning that strengthens security posture while reducing operational and reputational risk.

Awareness

Fewer human-error incidents

Everyday secure practice for every employee.

- Phishing and social engineering
- Password and device hygiene
- Incident reporting duties

Compliance

Audit questions answered

Training aligned to the standards you are audited against.

- PCI DSS and ISO expectations
- Privacy and DPDP handling
- Evidence for auditors

Capability

Stronger technical defence

Technical depth for the teams who run security.

- Secure configuration
- Access control practice
- Threat recognition drills

Proof

Evidence on demand

Completion, scores and certificates on record.

- Per-user completion status
- Assessment results
- Certificates and expiry

WHY ORGANISATIONS NEED TRAINING

Every other control assumes the user does the right thing

The exposure 01

Employees handle sensitive data across cloud platforms, email and connected devices every day.

- Phishing remains the first step in most breaches
- Sensitive data leaves through everyday tools
- Remote and hybrid work widens the surface

Human risk is the residual risk

What structured learning changes 02

A programme, not a poster: assigned, tracked, assessed and refreshed.

- Teams recognise emerging threats
- Secure practice becomes routine
- Compliance expectations are understood

Posture strengthened, risk reduced

THE COST OF DOING NOTHING

Six risks that grow when the workforce is untrained

Six exposures that grow every month the workforce is untrained.

01 Data breach exposure

Untrained employees mishandle sensitive information or fall for phishing.

- Unauthorised access to systems
- Serious data compromise incidents

02 Regulatory penalties

Weak awareness undermines compliance readiness.

- Audit findings and failures
- Penalties under PCI DSS and privacy law

03 Privacy violations

Improper handling of personal information triggers investigations.

- Regulatory scrutiny
- Customer complaints

04 Operational disruption

Incidents caused by human error interrupt business services.

- Delayed operations
- Reduced productivity

05 Financial fraud

Staff unaware of fraud tactics enable scams.

- Phishing and invoice manipulation
- Credential misuse

06 Reputation damage

Security incidents reduce stakeholder confidence.

- Weaker customer trust
- Strained relationships

TRAINING PROGRAMMES

Six role-based programmes, One platform

Employee awareness

Common threats, secure working practice and reporting duties.

- Password responsibilities
- Phishing recognition
- Incident reporting

Everyday secure behaviour

Executive risk

Cyber risk exposure, governance duties and decision support.

- Board-level risk framing
- Oversight responsibilities

Informed leadership

IT security

Secure configuration, access control and operational security.

- Hardening practice
- Privilege management

Stronger infrastructure

Compliance readiness

Awareness aligned to PCI DSS, ISO and privacy expectations.

- Control-linked learning
- Evidence for audits

Audit-ready workforce

Data privacy

Responsible handling of personal and customer information.

- Data minimisation in practice
- Sharing and retention rules

Privacy by habit

Industry focused

Sector-aligned learning for banking, healthcare, manufacturing and services.

- Sector threat scenarios
- Regulator expectations

Relevant to your business

THE OPERATING MODEL

Assess · Assign · Train · Prove

threatsys | Your 360° Cyber Security Partner

01

Assess

Establish the baseline: who needs what, and where the human risk sits.

- Role and department mapping
- Baseline phishing simulation
- Regulatory obligations identified

Starting point on record

02

Assign

Courses assigned by role, with deadlines and automatic reminders.

- Role-based curricula
- Due dates per cohort
- Escalation to managers

Everyone knows their path

03

Train

Modules, scenarios and simulations delivered at the learner's pace.

- Practical, scenario-led content
- Assessments after each module
- Refreshers as threats change

Behaviour actually changes

04

Prove

Completion, scores and certificates exported as audit evidence.

- Per-user completion records
- Certificates with validity
- Auditor-ready reports

Evidence without scrambling

THE LEARNING PLATFORM

Built to Train a Whole Organisation Without Disruption

Scalable delivery
No operational disruption

Train employees across locations, departments and business units.

- Cohorts by team or entity
- Multi-location rollout

Quick deployment
Value in days, not months

Fast onboarding without complex setup.

- Bulk user import
- Pre-built curricula

Continuous modules
Never out of date

Content refreshed as threats and regulations change.

- Regular content updates
- New scenarios added

Reporting
Visibility for leadership

Completion, scores and gaps by team and role.

- Manager dashboards
- Exportable evidence

REAL THREAT SIMULATIONS

Practice On Safe Attacks, Not Real Ones

Phishing simulation 01

Realistic campaigns sent to cohorts on a schedule.

- Templates by sophistication
- Click and report tracking
- Just-in-time coaching on failure

Measured susceptibility

Scenario exercises 02

Situations employees actually meet, worked through in the platform.

- Vendor payment fraud
- Data request from a stranger
- Lost device response

Judgement, not memorisation

Response drills 03

Reporting and escalation practised until it is automatic.

- Who to tell, how fast
- What evidence to preserve

Faster real-world reporting

CERTIFICATION PATHWAYS

From awareness to industry certification

For technical teams and career-track learners, structured paths lead to recognised industry certifications alongside corporate awareness training.

Offensive security

01

Practical attack skills for defenders and testers.

- CEH
- eJPT
- CRTP
- LPT

Test like an attacker

Network & systems

02

Foundations that underpin every other control.

- CNSP
- Secure configuration
- Network defence

Solid technical base

Cloud

03

Cloud fundamentals for teams moving workloads.

- AWS Academy Cloud Foundations
- Shared responsibility model

Cloud-ready teams

Governance

04

Assurance and control skills for GRC roles.

- CAP
- FCA
- Audit readiness practice

Assurance capability

TRAINING ACROSS INDUSTRIES

Sector-aligned learning where the risk actually sits

01	**Banking & finance**	Protect transactions and strengthen employee awareness. Fraud prevention practice · PCI DSS compliance support	**Safer financial services**
02	**Fintech**	Secure digital payment platforms and customer data. Threats targeting fintech · Secure product practice	**Trust in the platform**
03	**Insurance**	Safeguard policyholder information and prevent fraud. Sensitive data handling · Fraud risk awareness	**Policyholder confidence**
04	**Payment service providers**	Secure processing and cardholder data protection. Cardholder data handling · PCI DSS awareness	**Compliance sustained**

WHY ORGANISATIONS TRUST US

Practical training that changes behaviour, not just completion rates

Business focused learning

Programmes built around real business risk, applied in daily workflows.

- Operational relevance
- Role-specific scenarios

Learning that sticks

Improved accountability

Employees understand their part in protecting systems and information.

- Clear responsibilities
- Manager visibility

Ownership, not blame

Enhanced risk visibility

Training insight reveals human-related vulnerabilities.

- Weak cohorts identified
- Repeat-failure tracking

Target the real gaps

Regulatory driven

Aligned with PCI DSS, ISO and data protection requirements.

- Evidence for auditors
- Control-linked modules

Confident audits

Scalable & quick

Deploy across the organisation without a long project.

- Fast onboarding
- Multi-site delivery

Immediate value

Trusted platform

Structured, professional training used by organisations across sectors.

- Consistent experience
- Reliable delivery

A programme, not a one-off

TRACK RECORD

A training partner with an audit practice behind it

10+

Years of industry experience

Cybersecurity assessment and advisory delivered across regulated sectors.

1,000+

Organisations served

From banks and fintechs to healthcare, manufacturing and services.

3,000+

Custom projects delivered

Audits, testing and compliance programmes completed end to end.

500+

Legacy processes transformed

Manual compliance and training processes moved onto structured platforms.

50+

Awards and certifications

Recognition and credentials held across the consulting team.

4.7

Rating on Clutch

Independent client feedback on delivery and outcomes.

AUTOMATION, AI & INTEGRATIONS

The administration handled for you

01 Assignment automation

New joiners and role changes trigger the right curriculum.

- Rules by role and department
- Automatic due dates

No manual chasing

02 AI learning assistant

Answers policy questions and recommends the next module.

- Plain-language answers
- Personalised next steps

Support at the moment of need

03 Reminders & escalation

Staged nudges to learners, then to their manager.

- Email and in-app alerts
- Escalation on overdue

Completion rates rise

04 Integrations

HR systems, single sign-on and the Threatsys suite.

- SSO and directory sync
- GRC 360 and DPDP 360 evidence

One record across products

DASHBOARDS & REPORTING

Human risk, finally measurable

Completion, performance, simulations and hotspots - one reporting layer.

01 Completion

Who has finished, who is overdue, by team and role.

- Progress against deadline
- Manager-level rollup

02 Assessment performance

Scores by module and topic, with weak areas surfaced.

- Topic-level breakdown
- Repeat attempts tracked

03 Simulation results

Click, report and repeat-failure rates over time.

- Susceptibility trend
- Cohort comparison

04 Risk hotspots

Departments and roles carrying the most human risk.

- Ranked by exposure
- Linked to remediation training

05 Compliance evidence

Records and certificates packaged for auditors.

- Exportable per standard
- Validity and expiry tracked

06 Trend over time

Awareness maturity measured quarter on quarter.

- Baseline versus current
- Board-ready summary

RECOMMENDED DEMO FLOW

How to walk a client through LMS 360

threatsys | Your 360° Cyber Security Partner

Demo storyline

1 · Show the baseline: departments, roles and current awareness gaps.

2 · Assign a role-based curriculum to a cohort with due dates.

3 · Take a module as a learner, including the assessment.

4 · Launch a phishing simulation and show the coaching on failure.

5 · Open the dashboard: completion, scores and risk hotspots.

6 · Export the compliance evidence pack and a certificate.

Tip **Run the phishing simulation live – seeing a click turn into a coaching moment sells the platform faster than any feature list.**

ROLLOUT & VALUE

Rollout phases and client value

A practical path from first baseline to a continuous, measurable awareness programme.

Phase 1 · Weeks 1-2

Baseline

Users imported, roles mapped, baseline simulation run and curricula agreed.

Phase 2 · Weeks 3-8

Train

Role-based programmes assigned, assessments completed, managers reporting on progress.

Phase 3 · Quarter 2

Sustain

Refresher cycles, ongoing simulations, certification paths and audit evidence on tap.

Client value

Lower human risk
Fewer clicks, faster reports

Compliance ready
Evidence for every audit

Whole workforce
Every site, every role

Measurable
Baseline to board report

threatsys | Your 360° Cyber Security Partner

threatsys LMS360 ai

Thank you

Let us build your awareness programme with your own roles and regulators - baseline, train, simulate and prove.

- **ROLE-BASED · EVIDENCE FOR EVERY AUDIT**

CALL
+91 9668200222

EMAIL
support@threatsys.co.in

WEB
www.threatsys.co.in