AI-NATIVE SECURITY OPERATIONS CONSOLE

Threatsys AI SOC 360

Detect · Investigate · Respond · Prove

AI SIEM, SOAR, XDR and file integrity monitoring fused into one AI-driven response system - with continuous threat hunting and an agentic SOC assistant that carries the routine investigation work.

- 24×7 MONITORING · CERT-IN EMPANELLED

+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.

THIS DECK

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

Building a cyber-ready workforce

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

FOCUS · 1 OF 6

One console for the whole detection and response cycle

Telemetry from endpoints, network, cloud and identity lands in one place, is correlated once, and drives one investigation and one response - not four tools and four tickets.

Detect
Signal, not noise

Correlated detections across endpoint, network, cloud and identity telemetry.

- AI SIEM correlation
- MITRE-mapped detections
- Behavioural baselining

Investigate
Context assembled for you

The full incident story - assets, users, timeline and blast radius - built automatically.

- Automated enrichment
- Asset and user context
- Timeline reconstruction

Respond
Contained in minutes

Playbook-driven containment with approval gates on destructive actions.

- Isolate, block, disable
- Approval-gated actions
- Case managed to closure

Prove
Evidence for auditors

Every alert, action and decision retained as a defensible record.

- Immutable action log
- SLA and MTTR reporting
- Feeds GRC 360 evidence

threatsys | Your 360° Cyber Security Partner

The problem was never the data. It was the triage.

LEGACY SIEM AND POINT TOOLS

Alert fatigue

Thousands of low-context alerts, and no way to tell which one matters.

- Analysts triage manually
- Real intrusions missed in the noise

Tool sprawl

Endpoint, network, cloud and identity each in their own console.

- Context switching per alert
- Correlation done in an analyst's head

Slow, uneven response

Containment depends on who is on shift and how tired they are.

- No consistent playbook
- MTTR measured in hours or days

The breach is found by someone else

WITH THREATSYS AI SOC 360

AI triage first

Alerts are correlated, enriched and scored before a human sees them.

- False positives suppressed
- Analysts see cases, not alerts

One correlated surface

Endpoint, network, cloud and identity telemetry on one timeline.

- XDR coverage in one console
- Blast radius visible immediately

Automated containment

Playbooks act in seconds, with approval gates where it matters.

- Consistent every shift
- MTTR measured in minutes

You find it first, and you can prove it

THE OPERATING MODEL

Collect · Correlate · Investigate · Respond · Report

One pipeline from raw telemetry to a closed case with evidence attached.

01

Collect

Logs, endpoint, network, cloud and identity telemetry normalised on ingest.

- Agent and agentless sources
- Parsers for common stacks
- Retention set by policy

One data model

02

Correlate

Detections built on behaviour and threat intelligence, not single log lines.

- MITRE ATT&CK mapping
- Behavioural baselining
- Intel-matched indicators

Signal separated from noise

03

Investigate

Cases arrive with context already assembled by the SOC assistant.

- Asset, user and process tree
- Related alerts grouped
- Recommended next step

Minutes, not hours

04

Respond

Playbooks isolate hosts, block indicators and disable accounts.

- Approval gates on destructive actions
- Rollback recorded
- Ticket raised automatically

Consistent containment

05

Report

SLA, MTTR and incident evidence packaged for management and auditors.

- Executive summaries
- Regulator-ready incident record
- Evidence into GRC 360

Defensible every time

MODULE LANDSCAPE

One console, six engines

AI SIEM, SOAR, XDR, FIM, threat intelligence and hunting on a single correlated data model.

01 AI SIEM

Log ingestion, normalisation and behavioural correlation at scale.

- Detection engineering
- Long-term retention

02 SOAR

Orchestrated playbooks that act across your existing tooling.

- Automated containment
- Approval workflows

03 XDR

Endpoint, network, cloud and identity detection on one timeline.

- Cross-layer correlation
- Blast radius mapping

04 FIM

File integrity monitoring on critical systems and configurations.

- Change detection
- Baseline drift alerts

05 Threat intelligence

Indicator feeds matched continuously against your telemetry.

- IOC and TTP matching
- Sector-relevant intel

06 Threat hunting

Analyst-led hypothesis hunts across historical data.

- Hunt library
- Findings become detections

threatsys | Your 360° Cyber Security Partner

Detection built on behaviour, not keyword rules

Every source normalised into one schema so a detection written once applies everywhere it should.

01 Ingest anything

Agent and agentless collection from infrastructure, applications and cloud.

- Syslog, API and agent sources
- Cloud audit trails
- Normalised on arrival

One schema, many sources

02 Behavioural detection

Baselines per user, host and service so deviation is what triggers.

- Impossible-travel and privilege abuse
- Rare-process execution
- Volume and timing anomalies

Catches the unknown

03 Detection engineering

A managed rule set mapped to MITRE ATT&CK and tuned to your estate.

- Coverage gaps identified
- False positives tuned out
- New TTPs added continuously

Coverage you can audit

04 Retention & search

Searchable history for hunting, forensics and regulatory obligations.

- Policy-driven retention
- Fast historical search
- Export for investigations

Evidence still there later

threatsys | Your 360° Cyber Security Partner

SOAR & AUTOMATED RESPONSE

The first ten minutes, handled automatically

The actions an analyst would take on a confirmed detection, executed in seconds and recorded in full.

Playbook library

Prebuilt responses for phishing, malware, credential abuse and lateral movement.

- Per-detection playbooks
- Customised to your tooling

Consistent every time

Containment actions

Isolate a host, block an indicator, kill a process, disable an account.

- Endpoint and firewall actions
- Identity provider integration

Spread stopped early

Approval gates

Destructive actions pause for a named approver where policy requires.

- Segregation of duties
- Full reason recorded

Automation you can trust

Case management

Every incident tracked from detection to closure with a full timeline.

- Owner and SLA clock
- Analyst notes retained

Nothing quietly dropped

Enrichment

Reputation, intel and asset context attached before triage begins.

- Threat intel lookups
- Asset criticality applied

Faster, better decisions

Integrations

Actions executed through the tools you already run.

- EDR, firewall, IdP, ITSM
- API-first connectors

No forklift replacement

threatsys | Your 360° Cyber Security Partner

Every layer an attacker touches, on one timeline

Cross-layer correlation is what turns four unremarkable alerts into one obvious intrusion.

01	**Endpoint**	Process, file and memory activity with response actions built in. EDR telemetry · Process trees · Host isolation	**Where the attack lands**
02	**Network**	Flow, DNS and perimeter telemetry for lateral movement and exfiltration. Flow and DNS logs · Firewall and proxy events	**Where it spreads**
03	**Cloud**	Control-plane and workload activity across your cloud accounts. Audit trails · Misconfiguration signals	**Where it scales**
04	**Identity**	Authentication, privilege and session activity across directories and SSO. MFA and privilege events · Session anomalies	**Where it escalates**
05	**Email & SaaS**	Phishing, mailbox rule abuse and SaaS data movement. Mail security events · SaaS audit logs	**Where it usually starts**

threatsys | Your 360° Cyber Security Partner

FILE INTEGRITY MONITORING

The quiet change nobody noticed

Attackers and misconfiguration both show up as unexpected change on systems that should be stable.

01 Baselines

Known-good state captured for critical files, binaries and configurations.

- Per-system baselines
- Approved change windows

A reference to compare against

02 Change detection

Additions, edits, permission changes and deletions detected as they happen.

- Who, what and when
- Hash-level comparison

Tampering visible

03 Drift alerts

Unapproved configuration drift raised as a case, not a report nobody reads.

- Routed to the system owner
- Linked to change tickets

Estate stays as designed

04 Compliance evidence

Integrity monitoring records that satisfy PCI DSS and ISO expectations.

- Audit-ready logs
- Retention by policy

One control, two jobs

threatsys | Your 360° Cyber Security Partner

INTELLIGENCE & HUNTING

Looking for what the rules have not learned yet

Detections cover what is known. Hunting is how the unknown gets found and turned into a detection.

Intel matching

Indicator and TTP feeds matched continuously against live and historical telemetry.

- IOC sweeps across history
- Sector-relevant intel

Known-bad found fast

Hypothesis hunts

Analyst-led hunts against a specific attacker behaviour.

- Hunt library maintained
- Findings documented

Blind spots surfaced

Purple-team validation

Detections tested against real attacker technique, not assumed to work.

- ATT&CK coverage tested
- Gaps fed to engineering

Coverage that is proven

Detection improvement

Every hunt and incident feeds back into the rule set.

- New rules from real cases
- Tuning to cut noise

The SOC gets smarter

Compromise assessment

Point-in-time hunt for existing footholds before monitoring begins.

- Baseline the estate
- Findings triaged with you

Start from a clean read

Advisories

Sector-specific alerts when a campaign is relevant to you.

- Actionable guidance
- Mapped to your coverage

Forewarned, not surprised

threatsys | Your 360° Cyber Security Partner

An analyst's first hour, in a few seconds

The assistant does the assembling and drafting; the analyst decides. Nothing acts on your estate unreviewed.

01 Automated triage

Alerts grouped, scored and de-duplicated into a single case.

- Related alerts merged
- Severity justified in plain words

Queue cut dramatically

02 Investigation summary

A written account of what happened, on which assets, in what order.

- Timeline and blast radius
- Evidence cited per claim

Handover without re-reading

03 Recommended actions

The containment and remediation steps for this case, ready to approve.

- Playbook proposed
- Impact stated before execution

Decisions made faster

04 Ask the SOC

Natural-language questions across your telemetry and case history.

- "Has this IP been seen before?"
- No query language needed

Junior analysts perform senior

MANAGED SERVICE MODEL

Platform, or platform with our analysts on it

Run AI SOC 360 yourself, or have CERT-In empanelled analysts run it with you around the clock.

01	**Onboarding**	Sources connected, baselines established and playbooks agreed before go-live. Source inventory · Runbook workshop	**Live in weeks**
02	**24×7 monitoring**	Continuous triage with defined response times by severity. Follow-the-sun coverage · Severity-based SLAs	**Nights and weekends covered**
03	**Escalation**	A defined path from analyst to your named contact and back. Agreed contact tree · Out-of-hours protocol	**No ambiguity at 3am**
04	**Incident response**	Senior responders engaged on confirmed compromise, with forensics. Containment and eradication · Root-cause report	**Help when it is real**
05	**Reporting cadence**	Weekly operational review and a monthly management report. MTTD and MTTR trend · Coverage and tuning changes	**Progress you can show**

DASHBOARDS & REPORTING

The SOC, readable by everyone who needs it

One record read three ways - the analyst queue, the security posture, and the board summary.

SOC operations

Live queue, case ageing and analyst workload.

- Open cases by severity
- Ageing and ownership

Nothing sits unworked

Executive view

Posture, incident volume and risk concentration for leadership.

- Month-on-month trend
- Top risks named

Board-ready in one screen

Detection coverage

ATT&CK coverage and telemetry gaps made explicit.

- Techniques covered
- Sources missing

Know what you cannot see

SLA performance

MTTD and MTTR measured against the agreed targets.

- Per-severity performance
- Breaches explained

Service held to account

Compliance evidence

Monitoring and incident records auditors ask for.

- Retention proof
- Incident register

Audit questions answered

Threat landscape

What was actually seen against your estate this period.

- Campaigns observed
- Actions taken

Context for investment

INTEGRATIONS

Built onto the stack you already run

Telemetry in, response actions out - through the tools already deployed in your environment.

01	**Endpoint & EDR**	Detection telemetry in, isolation and process kill out. EDR and antivirus · MDM posture	**Response at the host**
02	**Network & perimeter**	Flow and DNS telemetry in, indicator blocking out. Firewalls and proxies · DNS and VPN logs	**Response at the edge**
03	**Cloud platforms**	Control-plane and workload telemetry from your cloud accounts. AWS · Azure · Google Cloud	**Cloud in the same timeline**
04	**Identity & SSO**	Authentication events in, account disable and session revoke out. Entra, Okta, Workspace · Directory and privilege events	**Response at the identity**
05	**ITSM & suite**	Cases raised where your teams work, evidence pushed to compliance. Jira and ServiceNow · GRC 360 and DPDP 360	**One record end to end**

TRACK RECORD

A SOC platform with a testing practice behind it

24×7

Monitoring coverage

Continuous triage with severity-based response times, including nights and weekends.

6

Engines in one console

AI SIEM, SOAR, XDR, FIM, threat intelligence and analyst-led hunting on one data model.

1,000+

Organisations served

Across BFSI, fintech, government, healthcare, media and manufacturing.

CERT-In

Empanelled testing

The same practice that performs VAPT and regulatory audits runs the SOC.

PCI QSA

Authorised consultants

Monitoring and integrity controls designed to satisfy assessors, not just alert.

One

Suite, one record

Incidents, evidence and compliance obligations connected across Threatsys One AI.

RECOMMENDED DEMO FLOW

How to walk a client through AI SOC 360

Demo storyline

1 · Open the live queue and show raw alert volume.
Then show how many cases that actually became after correlation.

2 · Open one case: timeline, assets, users, blast radius.
Point out that nobody assembled this by hand.

3 · Read the assistant's investigation summary aloud.
Every claim in it links back to the evidence behind it.

4 · Approve a containment playbook and watch it execute.
Show the approval gate and the recorded action log.

5 · Run a threat hunt across historical telemetry.
Turn the finding into a new detection in front of them.

6 · Finish on the executive dashboard and MTTR trend.
Close on the number their board will ask about.

Tip **Lead with the alert-to-case reduction. Every prospect already knows what alert fatigue costs them - show that number falling before you show a single feature.**

ROLLOUT & VALUE

Rollout phases and client value

A practical path from first log source to a tuned SOC with hunting and reporting in rhythm.

Phase 1 · Weeks 1-3

Onboard

Critical sources connected, baselines captured and severity definitions agreed.

- Source and asset inventory
- Compromise assessment run

Phase 2 · Weeks 4-8

Operate

Detections tuned, playbooks live and 24×7 triage running to SLA.

- False positives driven down
- Escalation path exercised

Phase 3 · Quarter 2

Mature

Hunting cadence, coverage testing and reporting embedded with leadership.

- ATT&CK coverage reviewed
- MTTD and MTTR trending down

Client value

Fewer, better alerts
Analysts work cases, not noise

Minutes to contain
Automation acts on hour one

One console
Endpoint to cloud on one timeline

Audit-ready
Incident evidence retained

threatsys | Your 360° Cyber Security Partner

threatsys soc360 ai

Thank you

Let us connect a few of your real sources and show you the queue, the case and the containment on your own telemetry.

- **24×7 MONITORING · CERT-IN EMPANELLED**

CALL
+91 9668200222

EMAIL
support@threatsys.co.in

WEB
www.threatsys.co.in