threatsys | Your 360° Cyber Security Partner

threatsys appsec360 ai

DEVSECOPS-READY APPLICATION SECURITY

Threatsys AppSec 360

SAST · DAST · API · PTaaS platform

Automatically find and validate vulnerabilities across your code, applications, APIs and cloud infrastructure - with verified, audit-ready evidence.

- Validated Findings
- No False Positives

+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 India's DPDP Act, 2023.

threatsys CRM360 ai

Effortless AI-powered delivery management

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

THIS DECK

threatsys appsec360 ai

Automated Application Security Testing

SAST, DAST, API testing and PTaaS with validated, evidence-backed findings and no false positives across code and cloud.

threatsys LMS360 ai

Building India's cyber-ready workforce

Enterprise cybersecurity training, compliance awareness and placement-linked skilling through practical learning.

CONTINUOUS SECURITY · STRONGER APPLICATIONS

Automate security testing, end to end

4-in-1 application security. Automated SAST and DAST paired with CERT-In empanelled senior manual VAPT - catch the obvious fast and the dangerous too, with evidence that stands up in an audit.

SAST | DAST | API security testing | PTaaS

WHAT WE TEST

- **Source code & repositories**
  SAST across languages, binaries and open-source dependencies.
- **Web & mobile applications**
  DAST against the running app, plus authenticated business-logic testing.
- **APIs & microservices**
  Auth, access control, injection and data-exposure testing on every endpoint.
- **Cloud & infrastructure**
  Configuration, exposure and hardening review of the hosting estate.

PLATFORM OVERVIEW

One platform for complete application security

SAST, DAST, API testing and PTaaS unified to discover, validate and remediate vulnerabilities across your whole portfolio.

01
Discover
SAST + DAST scans

02
Validate
Proof-of-exploit

03
Remediate
Guided + retest

04
Prove
Audit reports

Shift-left
Security inside the CI/CD pipeline and SDLC.

Audit-ready
Verified findings and evidence, full traceability.

4-in-1
SAST·DAST·API·PTaaS

8
STEPS

24x7
VISIBILITY

Mapped to the frameworks that matter: OWASP Top 10 · PCI DSS · ISO 27001 · SOC 2

WHY AUTOMATED SECURITY TESTING

Continuous testing, not periodic surprises

Manual assessments alone leave applications exposed - periodic, time-consuming and often too late to act on.

01

Continuous protection

Find and fix vulnerabilities early across your SDLC.

Shift-left | Early detection

02

Save time & resources

Eliminate manual effort and speed testing with automation.

10x faster | Automated

03

Reduce risk

Catch more issues, prioritise better, cut security debt.

Prioritised | Less debt

04

Audit-ready evidence

Verified findings and compliance-ready reports with traceability.

Verified | Traceable

By the numbers

10x

Faster issue detection

95%+

Accuracy, fewer false positives

100%

Coverage across apps & APIs

Secure. Compliant. Confident.

threatsys | Your 360° Cyber Security Partner

ONE PLATFORM, EVERY TEAM

Built for engineering, security and assurance

Developers, AppSec, DevOps, GRC and leadership - each sees the findings, evidence and workflows that matter to them.

DE Developers

Findings in the pipeline with fix guidance and reproduction steps.

CI/CD | Fix steps

AS AppSec team

Validated findings, severity scoring and false-positive elimination.

Validation | Triage

DO DevOps

Shift-left scans wired into GitHub, GitLab and Jenkins.

Pipelines | Gates

GR GRC & Compliance

Findings mapped to OWASP, PCI DSS and ISO 27001 for audits.

Frameworks | Evidence

PE Pentest / PTaaS

Expert-led manual testing with on-demand retesting.

Manual VAPT | Retest

LA Leadership / Auditor

Security posture dashboards, coverage and audit-ready reports.

Posture | Reports

THE OPERATING MODEL

Discover · Validate · Remediate · Prove

The application-security loop, closed on one platform.

01 Discover	02 Validate	03 Remediate	04 Prove
SAST, DAST and API scans across the attack surface	Expert verification and proof-of-exploit	Guided fixes, ownership and retesting	Audit-ready reports and evidence exports
Source code scan	Manual verification	Remediation guidance	Framework mapping
Running-app scan	Proof-of-exploit	Owner assignment	Evidence package
API endpoint scan	Severity scoring	On-demand retest	Compliance report
Cloud & repos	False-positive filter	Fix verification	Feeds GRC platform

Shift-left, prove-right. **Automation finds fast; senior auditors confirm what actually gets you breached.**

THE APPSEC 360 WORKFLOW

Eight steps, one security pipeline

01
SAST scanning
Analyse code, binaries and dependencies before deployment.

Output · prioritised code defects

02
DAST
Test running apps in real time to find runtime flaws.

Output · exploitable runtime issues

03
API security
Test endpoints for auth, access and injection risks.

Output · API risk register

04
Validated findings
Proof-of-exploit, repro steps and severity prioritisation.

Output · zero false positives

05
PTaaS
Expert-led pentesting with on-demand retesting.

Output · signed pentest report

06
Multi-asset coverage
Repos, web, mobile, APIs and cloud from one platform.

Output · single asset inventory

07
DevSecOps integration
GitHub, GitLab, Jenkins and CI/CD for shift-left testing.

Output · security gate in the pipeline

08
Compliance reporting
Audit-ready reports for PCI DSS, ISO 27001, OWASP, SOC 2.

Output · evidence pack for auditors

STATIC ANALYSIS · SAST

Comprehensive SAST scanning

Analyse source code, binaries and dependencies for security flaws to detect vulnerabilities before deployment.

01
Connect
Repo / build

02
Scan
Code & deps

03
Detect
Insecure patterns

04
Prioritise
By severity

05
Fix early
Pre-deploy

What it analyses

Source code

Binaries

Open-source dependencies

Config & secrets

Outputs

Prioritised findings

Remediation guidance

SDLC-stage detection

WHAT SAST CATCHES

- **Injection & unsafe input handling**
  SQL, command and template injection paths traced from source to sink.
- **Hard-coded secrets & keys**
  Credentials, tokens and keys committed into the repository.
- **Weak crypto & auth logic**
  Deprecated algorithms, weak session handling and broken access checks.
- **Vulnerable dependencies**
  Known-CVE open-source components and outdated libraries.

threatsys | Your 360° Cyber Security Partner

DYNAMIC ANALYSIS · DAST

Real-world attack simulation

Test running applications in real time with automated scans that simulate attacks to uncover runtime flaws, misconfigurations and injection issues.

RT Runtime testing

Exercise the live application the way an attacker would.

Live app | Real conditions

AT Attack simulation

Injection, broken auth and misconfiguration probes.

Injection | Auth flows

MV Multi-vector

Web, API, mobile and cloud environments in scope.

Web | Mobile | Cloud

MC Misconfig checks

Surface insecure settings before attackers exploit them.

Headers | TLS

CO Continuous scans

Automated, scheduled runs for ongoing visibility.

Scheduled | 24x7

Outputs

Runtime vulnerability list

Reproduction steps

Severity scoring

threatsys | Your 360° Cyber Security Partner

API SECURITY TESTING

Find the risks hiding in your APIs

Discover and test API endpoints for authentication weaknesses, broken access controls, injection attacks and data-exposure risks.

01 **Discover** Endpoints

02 **Auth** Weakness

03 **Access** Controls

04 **Injection** Attacks

05 **Exposure** Data leaks

06 **Report** Evidence

What we test for

- Broken authentication
- Broken object / function-level authorization
- Injection and mass assignment
- Excessive data exposure
- Rate limiting & abuse

Coverage

- REST & GraphQL endpoints
- Authenticated & unauthenticated
- Internal & public APIs
- Automated endpoint discovery
- Continuous re-scanning

Outputs

- **Endpoint inventory**
- **Validated API findings**
- **Proof-of-exploit**
- **OWASP API mapping**

VALIDATED FINDINGS · PTAAS

Real threats, not a wall of false positives

Every finding is validated by an expert - proof-of-exploit evidence, reproduction steps and severity-based prioritisation.

01	02	03	04	05
Detect	**Verify**	**Prove**	**Fix**	**Retest**
Automated	Expert	Exploit evidence	Guided	On demand

Validated findings

- Proof-of-exploit evidence
- Reproduction steps
- Severity scoring
- Remediation guidance
- Zero false-positive noise

PTaaS model

- Automated scanning + expert testing
- Senior manual VAPT
- Business-logic & chained exploits
- On-demand retesting
- Continuous validation

Why it wins

- **Focus on real threats**
- **Prioritise fixes accurately**
- **No wasted effort**
- **Fixes proven to hold**

MULTI-ASSET COVERAGE

Your whole attack surface, one platform

Connect and scan every asset from a single console for complete attack-surface visibility.

RE

Code repos

GitHub, GitLab and other source repositories.

WE

Web apps

Public and internal web applications.

MO

Mobile apps

iOS and Android application testing.

AP

APIs

REST and GraphQL endpoint testing.

CL

Cloud infra

Cloud configuration and infrastructure.

100% coverage. One console across apps, APIs and cloud - no blind spots, no tool sprawl.

DEVSECOPS INTEGRATION

Shift security left into the pipeline

Seamless connectivity to your development tools runs automated scans as part of every build.

CI CI/CD integration

Scans triggered on commit, merge and build across your pipeline.

GitHub · GitLab · Jenkins

SL Shift-left testing

Catch issues at code time, when they are cheapest to fix.

Early detection · Lower cost

GA Build gates

Break the build on critical findings before release.

Policy gates · Thresholds

FE Feeds your GRC

Evidence flows into SigmaTrust so AppSec is part of continuous compliance.

Continuous compliance · No silos

threatsys | Your 360° Cyber Security Partner

COMPLIANCE-READY REPORTING

Reports your regulator will accept

Audit-ready reports and exportable evidence packages, aligned to the frameworks that matter - not raw scanner output.

OWASP	PCI DSS	ISO 27001	SOC 2
Top 10 mapping	Testing evidence	Control support	Audit alignment

In every report

- Verified findings, not noise
- Proof-of-exploit & repro steps
- Severity & prioritisation
- Remediation status & retest
- Full traceability

Delivered as

- Real-time dashboards
- Exportable evidence packages
- Executive posture summary
- QSA / enterprise-ready format
- Feeds SigmaTrust GRC

Accepted by

- **Regulators**
- **PCI QSAs**
- **Enterprise customers**
- **Internal audit & boards**

threatsys | Your 360° Cyber Security Partner

AUTOMATED SPEED · AUDITOR DEPTH

A scanner shows the obvious. An auditor finds what breaches you.

Automated SAST & DAST

Static analysis of source code early in the SDLC

Dynamic scanning of the running application

Fast, continuous, wide coverage

Runs on every build and pull request

Dependency and open-source component checks

Findings deduplicated and severity-scored

Speed and coverage, on every release

Senior manual VAPT

CERT-In empanelled senior auditors

Business-logic flaws scanners miss

Chained exploits and abuse cases

Every finding expert-verified

Threat modelling for critical user journeys

Free retest after remediation

Depth and proof, before the attacker finds it

✓ Manual verification

✓ Remediation tracking & retest

✓ Framework mapping

✓ Audit-ready reports

Feeds SigmaTrust GRC

threatsys | Your 360° Cyber Security Partner

AUTOMATED + MANUAL

APPSEC 360 IN ACTION

Four surfaces your teams work in every day

01

Security dashboard

Posture, coverage and open findings at a glance, by application and by team.

Filter by application, business unit or release train, and see whether risk is trending down week on week.

Risk by severity | Scan coverage | SLA ageing

02

Findings & triage

Validated, severity-scored findings with an owner, a due date and a fix path.

Duplicates are merged across SAST, DAST and manual testing so a team fixes each issue once, not three times.

Deduplicated | Owner assigned | Retest queue

03

Finding detail

Proof-of-exploit, reproduction steps and developer-ready remediation guidance.

Developers get the exact request, payload and code location, plus the secure pattern to replace it with.

Evidence attached | Repro steps | Fix guidance

04

Report & export

Audit-ready packs mapped to the frameworks your auditors and clients ask for.

Board summary, technical annexure and remediation status in one pack, reissued after every retest.

PCI DSS | ISO 27001 | OWASP · SOC 2

RECOMMENDED DEMO FLOW

Recommended client presentation flow

Use this sequence to show AppSec 360 as a working application-security platform.

01	02	03	04	05
Connect	**Scan**	**Validate**	**Remediate**	**Report**
Repo / app	SAST + DAST	Findings	Fix + retest	Evidence

Demo storyline

1 · Connect a repository or application in the live AppSec 360 console.

2 · Run combined SAST and DAST scans across the attack surface.

3 · Show validated findings with proof-of-exploit and severity scoring.

4 · Assign an owner, apply remediation guidance and trigger a retest.

5 · Show the API and multi-asset coverage in one console.

6 · Export an audit-ready, framework-mapped report as evidence.

Tip **Run a live scan in the console - a real finding with proof-of-exploit lands better than slides.**

threatsys | Your 360° Cyber Security Partner

ROLLOUT & VALUE

Rollout phases and client value

A practical path from onboarding to continuous application-security assurance.

Phase 1 · Weeks 1-2

Onboard

- Connect repos and apps
- Baseline SAST & DAST scans
- User roles and access
- Asset inventory

Phase 2 · Weeks 3-6

Operate

- CI/CD integration & gates
- API and multi-asset coverage
- Validation & PTaaS retests
- Remediation tracking

Phase 3 · Weeks 7+

Assure

- Audit-ready reporting
- Framework mapping & exports
- Feeds SigmaTrust GRC
- Continuous compliance

Client value

Faster detection	Fewer false positives	Secure releases	Audit-ready proof
10x earlier	95%+ accuracy	Shift-left	Framework-mapped

threatsys

Your 360° Cyber Security Partner

threatsys appsec360 ai

Thank you

- Validated Findings
- No False Positives

CALL
+91 9668200222

EMAIL
support@threatsys.co.in

WEB
www.threatsys.co.in