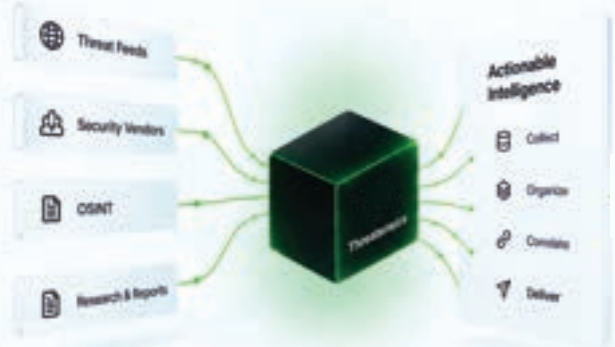
Threatensics™

Turn Threat Intelligence Into Action

Threat intelligence now comes from more sources than security teams can practically manage. Threatensics™ automatically collects, organizes, correlates, and delivers threat intelligence so teams can focus on what matters.



Know what is happening.
Know what belongs to you. Act sooner.

You Could Be Part of the Attack Chain Without Knowing It.

Attackers reuse infrastructure, capabilities, and attack patterns across multiple victims. Each organization may see only its own piece of the campaign. Traditional security operations often require analysts to manually correlate external threat data with internal assets, manage feeds, tune data, and maintain integrations.

Most platforms can tell you whether an indicator is malicious. Threatensics™ helps determine whether that indicator is relevant to your environment—including whether one of your assets may be involved.

Threat Intelligence at Scale

70+
Pre-integrated threat intelligence sources

44%
SANS[1] reports that lack of time is a top barrier to effective cyber threat intelligence implementation.

84%
IBM X-Force® [2] observed an 84% increase in emails delivering infostealers in 2024 compared with the previous year.

48%
Check Point Research[3] reports a 48% year-over-year increase in extorted ransomware victims.

What Changes with Threatensics™

ASSET-CORRELATED
Intelligence
Automatically connect external threat data to your internal assets instead of manually matching indicators to your environment.

BIDIRECTIONAL
Visibility
Look beyond incoming threats. Surface potential outbound abuse involving your own assets.

OPERATIONAL
Automation
Reduce the manual work involved in feed management, correlation, enrichment, and delivery.

CALL US
+91 9871 944 633

VISIT US
www.threatensics.com

EMAIL US
support@threatensics.com

Threatensics™

From Threat Data to Actionable Intelligence

Collect
Bring intelligence in from any source.

- OSINT feeds
- Commercial feeds
- Private feeds
- Custom feeds
- Webhooks

01

Organize
Turn fragmented data into usable intelligence.

- Ingest
- Parse
- Validate
- Map
- Deduplicate
- Enrich
- Label
- Annotate
- Store

02

Deliver
Get intelligence where your team needs it.

- Email
- REST APIs
- STIX/TAXII

03

Why Threatensics™

End-to-End Automation
Automate collection, normalization, enrichment, and delivery.

Governed Sharing
Control what intelligence is shared, with whom, and how.

Deploy in Hours
Move from installation and configuration to useful intelligence quickly.

Capabilities at a Glance

70+
Pre-integrated sources

STIX / TAXII
Standards-based sharing

REST APIs
Connect to your tools

Live Dashboards
Charts, maps, tables, filters

Make Threat Intelligence Work at Scale.
Threatensics™ automates the journey from threat data to actionable intelligence.

References:

1. SANS Institute, 2026 SANS Cyber Threat Intelligence (CTI) Survey Insights, 15 May 2026.
2. IBM, 2025 X-Force® Threat Intelligence Index, 17 April 2025.
3. Check Point Research, Cyber Security Report 2026, 28 January 2026.

CALL US
+91 9871 944 633

VISIT US
www.threatensics.com

EMAIL US
support@threatensics.com

FLOM™
Visibility. Control. Intelligence.

Threatensics™

Multi-BOM Software

Composition Analysis Platform

Identify software, AI, and cryptographic risks from a single scan.

One Scan. Complete Visibility.

Flexible Input Sources

- Upload Files
- Source Code Repositories
- Container Registries
- CLI

→ FLOM™ Visibility. Control. Intelligence. →

Reports

- SBOM
- AIBOM
- CBOM

GitHub • GitLab • Docker Hub • Nexus Repository • JFrog Artifactory • APKs • CLI • Source Code (ZIP)

Why FLOM™?

FLOM™ provides a single source of truth for your software supply chain.

Modern applications can comprise hundreds—or even thousands—of software components, AI technologies, and cryptographic implementations. Without complete visibility, organizations struggle to identify vulnerable components, understand dependency risks, and respond quickly to threats.

End-to-End Visibility

Discover

Scan version control systems, containers, binaries, CI/CD pipelines, CLI, and source code archives from a single platform.

Analyze

Leverage a centralized intelligence engine with 400,000+ vulnerability records, 2,000+ license identifiers, and support for 10+ programming languages and ecosystems to surface real-world risks.

Remediate

Prioritize issues with guided remediation, shift security left, and understand the blast radius of vulnerable components.

Govern

Apply security and licensing policies, detect compliance drift, and enforce governance before release.

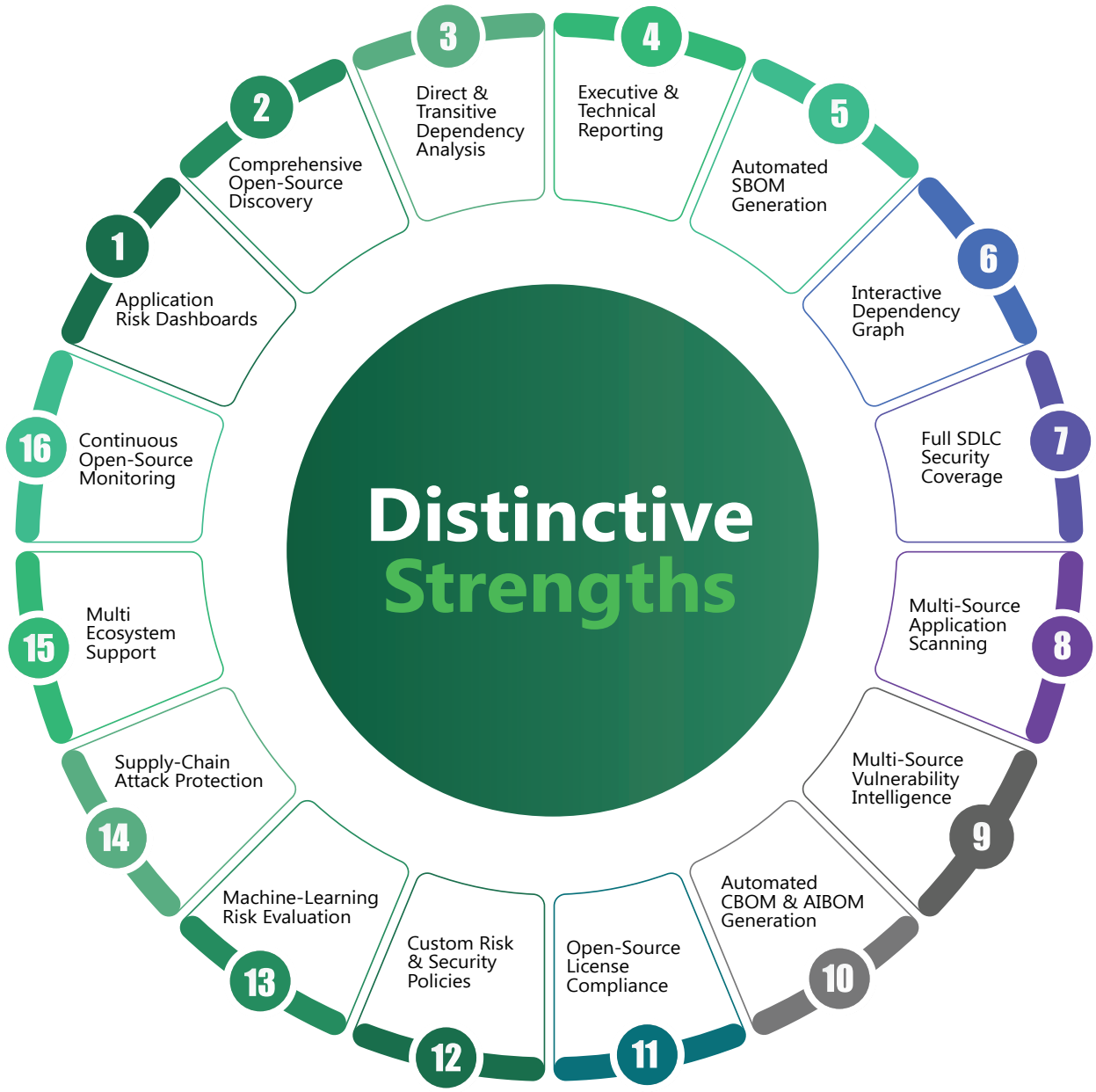
CALL US
+91 9871 944 633

VISIT US
www.threatensics.com

EMAIL US
support@threatensics.com

FLOM™
Visibility. Control. Intelligence.

Threatensics™



Composition Intelligence

SOFTWARE COMPOSITION (**SBOM**)

SBOM generation based on CycloneDX specifications that inventory open-source and third-party components, including direct, transitive, and hidden dependencies.

CRYPTOGRAPHIC COMPOSITION (**CBOM**)

Discover cryptographic primitives, keys, and certificates extracted from source code while identifying algorithms that require post-quantum migration.

AI COMPOSITION (**AIBOM**)

Inventory AI models, training data lineage, and AI-specific dependencies to improve transparency and support emerging regulatory requirements.

CALL US
+91 9871 944 633

VISIT US
www.threatensics.com

EMAIL US
support@threatensics.com