CISO verse

Building Trust in Applications with AI and SBOM

Mumbai, Edition 4 | 31st July, 2026

In Association with

CySecK Cyber Security Karnataka
K-Tech CoE for Cyber Security

Hosted by

boman.ai

SUMERU

> **“CISOverse is about shaping how we, as security leaders secure innovation in the AI era.”**

About CISOverse

CISOverse is an invite-only roundtable series that brings together CISOs and senior security leaders for honest, peer-driven conversations on the most pressing challenges in application security. Unlike traditional conferences or slide-heavy webinars, CISOverse is built for dialogue. It’s an inclusive, trusted community where 15-20 CISOs come together to share real-world experiences, challenge assumptions, and collaboratively explore how application security must evolve in modern, AI-driven software environments.

Each CISOverse edition culminates in two key outcomes: the CISO Playbook and the CISO Speaks Series. These practitioner-first artifacts capture shared insights, points of agreement, areas of friction, and actionable guidance that leaders can take back to their organizations. The playbook captures what CISOs agreed on, what they challenged, and what to do next.

For every edition, a topic is defined in advance. Three to four focused tracks are then identified, each supported by curated questions. These questions are shared with participating leaders ahead of time, enabling thoughtful reflection and more meaningful discussions during the session.

The first edition of CISOverse, **“Application Security in the Age of AI Era”**, was held on 29th August 2025 in Bangalore.

The second edition of CISOverse, **“ASPM In Action: Turning Application into Business Decisions”**, was held on 12th December 2025 in Bangalore. This marks the third edition of the series.

The third edition of CISOverse, **“ASPM in Action: Application Security in the Age of AI”**, was held on 10th April 2026 in Chennai. This marks the fourth edition of the series.

The details can be found at cisoverse.org

Executive Summary

This edition of CISOverse explores a critical shift in application security: as AI accelerates software development and software supply chains become increasingly complex, how can organizations build and maintain trust in their applications?

AI is changing how applications are written, tested, deployed, and secured, while expanding reliance on third-party components, open-source dependencies, and AI-generated code. At the same time, CISOs face growing expectations to demonstrate that risks are understood and security decisions are supported by meaningful evidence.

The CISOverse discussion explored how SBOM and AI are shaping the next phase of application security, moving the conversation beyond compliance and vulnerability visibility toward stronger governance, continuous assurance, and business confidence.

Across the three pillars—Trusted Software Supply Chain, AI, Trust & Governance, and Measuring Trust & Business Confidence—the discussions examined how organizations can understand the foundations of their software, establish responsible practices around AI, and communicate security exposure in terms the business can act upon.

This is where Application Security Posture Management (ASPM) becomes increasingly relevant. By connecting security signals, application context, risk prioritization, software supply-chain information, and governance, ASPM can help turn fragmented security data into a more connected view of application risk.

What emerges from these conversations is that confidence cannot come from any single security control or point-in-time assessment. It must be built through consistent assurance, clear accountability, and meaningful evidence that security decisions are producing outcomes as the application environment evolves.

Who Should Use This Playbook

- CISOs
- Engineering leaders (CTO/CIO/Tech Lead, etc.)
- Heads of AppSec
- GRC and audit leaders

CISOverse - Top Highlights

SBOMs Provide Visibility, Not Complete Supply-Chain Assurance

An SBOM shows software components, but third-party and transitive dependencies can remain unclear, leaving organizations exposed beyond their immediate vendor relationships and creating gaps in risk visibility.

Supply-Chain Trust Requires Provenance and Accountability

Knowing where software comes from is only the starting point; organizations also need evidence of integrity, clear ownership, and accountability throughout the development and delivery processes.

AI Adoption Is Outpacing Governance

As AI becomes embedded in development and security, unclear ownership, employee usage, and data handling can introduce risks faster than governance practices evolve across the organization.

AI Should Augment Security, Not Replace Judgment

AI can accelerate detection, testing, and remediation, but organizations still need human oversight, defined guardrails, and accountable decision-making for security-critical outcomes and high-impact decisions across the organization.

Security Confidence Depends on Continuous Evaluation and Evidence

Trust is stronger when security, privacy, and compliance are supported by consistent evidence and independent validation that can withstand leadership and audit scrutiny over time.

Business Risk Matters More Than Technical Severity Alone

Effective security reporting connects vulnerabilities to business exposure, operational impact, and accepted risk, giving leadership a clearer basis for prioritization, investment, and resilience across critical areas.

The collective inference of the above is clear: Building trust in applications is becoming a continuous discipline rather than a one-time security exercise. As software supply chains expand and AI reshapes development, organizations need to understand what they are using, govern how it is used, and validate the decisions made around it.

Ultimately, confidence comes from connecting technical security with clear accountability, reliable evidence, and the business impact of risk.

Contents

CISOverse Moments

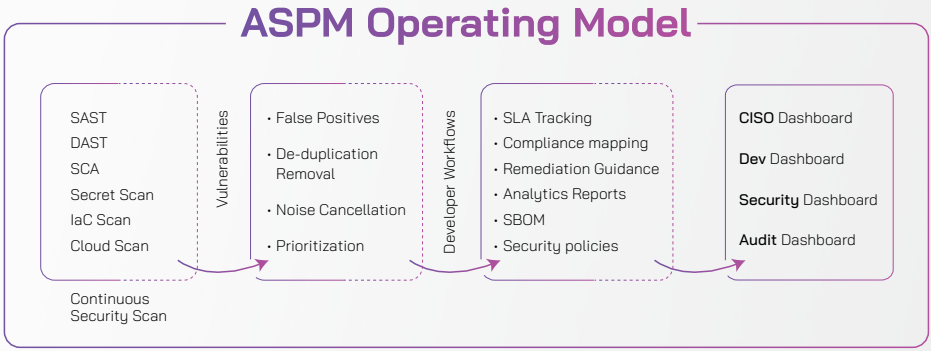
What is ASPM?

Application Security Posture Management (ASPM) tools are transforming application security by making it simpler, more accessible, and more effective. They bring together scanning, vulnerability management, remediation guidance, SBOM management, compliance, and software transparency in one platform, reducing fragmented workflows and making strong security practices easier to adopt.

When integrated into CI/CD pipelines, ASPM tools enable real-time vulnerability detection and mitigation without slowing development. They provide prioritized, actionable insights that help teams understand risk, maintain compliance, improve supply-chain visibility, and remediate issues with confidence.

How ASPM Connects SBOM, Secure Development & AI

The Mumbai CISOverse session brought together CISOs and senior security leaders from across Mumbai to examine how application security is evolving as AI accelerates software development and expands software supply-chain complexity. The discussions explored how ASPM can act as a connecting layer between SBOM intelligence, secure development practices, and broader application security, helping teams bring fragmented signals into context and make more informed risk decisions.



The conversation was structured across three core tracks:

Chapter 1- Trusted Software Supply Chain: As software ecosystems expand, SBOMs must move beyond static inventories toward continuous visibility across dependencies, artifacts, and deployments. Trust increasingly depends on understanding component risk, validating provenance and integrity, and strengthening security across development, build, and runtime environments.

Chapter 2- AI, Trust & Governance: As AI becomes embedded across development and application security, organizations must balance speed with governance, accountability, and human judgment. Establishing trust in AI-generated software requires clear ownership, security standards, and controls that ensure AI augments, not replaces, critical security decisions.

Chapter 3- Measuring Trust & Business Confidence: As security moves beyond vulnerability counts, organizations need meaningful evidence of risk reduction, resilience, and business impact. This requires metrics that connect application security to business outcomes, while using AI and ASPM to strengthen prioritization, demonstrate assurance, and build confidence with leadership.

Chapter 1: Trusted Software Supply Chain

Modern applications are no longer built in isolation. Their reliability increasingly depends on a wider ecosystem of code, components, vendors, and software artifacts that organizations may not directly control. This makes software supply-chain trust an essential part of application security, not simply a technical consideration, but a foundation for confidence in what an organization builds and delivers.

"An SBOM should be more than a compliance requirement or a list of software components. It gives organizations visibility into what is in their software, helps identify critical risks, and enables faster remediation. When used effectively, an SBOM becomes a practical capability for managing software supply-chain risk and making security easier for developers to act on."

Ninad Chavan
Cyber Security Consultant

"An SBOM provides visibility, but visibility alone cannot prevent a supply-chain attack. If an open-source maintainer account is compromised, organizations can unknowingly pull a malicious package into their environment. Software supply-chain security requires not only knowing what components you use, but also continuously monitoring and implementing proactive controls across the supply chain."

Shashank Dixit
Co-creator Boman.ai

"Applications are continuously evolving, so an SBOM cannot be a one-time compliance exercise. If an application goes through multiple deployments, its SBOM must evolve with it to provide an accurate view of the software supply chain and its risks. This is why SBOM is moving from a regulatory mandate and compliance checkbox to a strategic security necessity."

Chidha
CISO & CPO, Sumeru Technology Solutions

Insights	Recommendations
Supply-chain risk varies across applications. A vulnerable component does not create equal exposure; risk depends on where it is used, how it connects, and whether it reaches production.	Prioritize component risk using application context, linking dependencies to affected applications, environments, and exposure.
An SBOM provides component visibility, but not necessarily ownership or actionability. Vendors may rely on third-party and open-source dependencies they cannot fully account for, leaving organizations exposed to risks deeper in the software chain.	Extend SBOM visibility beyond direct dependencies by mapping transitive components and vendor dependencies, continuously correlating them with vulnerabilities, and establishing clear ownership for remediation. Require vendors to provide SBOMs for the software they supply.
Modern supply chain attacks increasingly target developers, build systems, package registries, and CI/CD pipelines rather than production environments directly.	Extend security controls to the development ecosystem. Secure repositories, build pipelines, developer workstations, package sources, and automation workflows.
Artifact trust depends on provenance and integrity. Knowing where software came from does not confirm it remained intact throughout the build and delivery process.	Strengthen artifact assurance with provenance and integrity checks across the build and release process.

Software supply-chain trust requires more than knowing which components an application contains. It depends on understanding how those components are connected, where risk can enter, and whether software remains trustworthy throughout its journey to production.

A resilient approach therefore combines continuous dependency visibility, secured development infrastructure, and verified artifact provenance to build confidence across the entire software supply chain.

Chapter 2: AI, Trust & Governance

AI is changing the nature of software decisions, extending its influence from how code is created to how security risks are assessed and addressed. This raises a broader question for CISOs: as AI becomes part of the application lifecycle, what does responsible trust look like when decisions are increasingly influenced by systems that organizations did not traditionally govern?

"AI adoption can create a significant compliance blind spot when organizations do not know where their data is processed or stored. As AI becomes embedded across business operations, understanding data location and ensuring it meets applicable regulatory requirements must become part of AI governance."

Anuj Jha
CISO, Epimoney Pvt. Ltd.

"A key challenge is the gap in how boards approach cybersecurity. Security teams are expected to provide assurance while facing limits on resources and investment. Cybersecurity must be treated as a business responsibility, with leadership understanding the risks and acting before a breach forces the issue."

Dr. Gopal Ji Gupta
CISO, Guardify Tech Pvt. Ltd.

"As organizations integrate AI and LLMs into existing environments, protecting data confidentiality becomes critical. AI adoption must be supported by clear safeguards to prevent data leakage while enabling organizations to realize the value of these technologies."

Vinay Bhide
Chief Business Officer- Cyber Security, Pentagon System & Services Pvt. Ltd.

Insights	Recommendations
AI adoption is moving faster than organizational ownership. As AI writes code and influences security decisions, unclear accountability can create gaps when things go wrong.	Define AI risk ownership early. Clearly assign responsibility across security, technology, governance, and business teams for AI decisions and outcomes.
AI risk is also an employee behavior problem. As employees increasingly use AI for everyday work, uninformed usage can expose sensitive information or bypass intended controls.	Build AI awareness into organizational security practices, with practical training on approved AI use, data handling, and common risks alongside existing security awareness programs.
Trust in AI starts with knowing where data goes. Public AI tools can create uncertainty around data processing, residency, retention, and reuse.	Make data handling a prerequisite for AI approval. Verify where data is processed, how it is controlled, and whether it can be retained or reused.
AI-generated assurance cannot validate itself. Relying on AI to generate and validate its own recommendations can create a false sense of confidence.	AI can accelerate detection, testing, and response; fully autonomous security remains a distant goal, making human oversight and decision-making a critical part of the security process.

AI adoption is moving faster than traditional governance structures can adapt, making ownership and accountability central to building trust. As AI influences code, data, and security decisions, organizations need clear boundaries around its use and stronger awareness of associated risks. Human oversight remains essential to validate AI-driven outcomes and maintain confidence in security decisions.

Chapter 3: Measuring Trust & Business Confidence

Security confidence is becoming harder to establish as applications, technologies, and business dependencies continue to evolve. For CISOs, the question is no longer simply whether security controls exist, but whether the organization can demonstrate that its software remains dependable, resilient, and worthy of business trust.

"One of the biggest challenges is the lack of visibility into third-party dependencies within vendor products. A product may appear complete, but it can still rely on external components with their own security risks. Organizations need visibility into these dependencies to understand and manage the risks they inherit."

Melwyn Rebeiro
CISO, Julius Baer

"The question is no longer whether organizations should adopt AI, but how they adopt it responsibly. As businesses accelerate AI adoption, clear controls and guardrails are essential to ensure these technologies are used safely, effectively, and with the right level of oversight."

Yogesh Rajawat
CISO and Head IT, Axium Global

"Organizations need to test their security readiness, not simply assume it. Strengthening Red Team activities and conducting regular incident response drills can reveal gaps in defenses and show how effectively teams would respond to real-world threats such as ransomware."

Shailendra Kumar Srivastava
CISO

Insights	Recommendations
Security confidence weakens when the same team builds and validates a control.	Use independent validation for critical controls and assurance claims, supported by evidence that can withstand leadership and audit scrutiny.
Trust depends on the intersection of security, privacy, and compliance. Treating them separately can leave gaps in overall assurance.	Bring security, privacy, and compliance evidence into a common assurance view for a more complete assessment of application trust.
Some security risk will remain even after controls are applied; confidence depends on knowing which risks are accepted and why.	Document accepted risks with defined owners, acceptance criteria, and review dates. Prioritize remediation based on business criticality, exploitability, and operational impact, not technical severity alone.
Security reporting often measures activity, but the Board needs to understand risk movement, business exposure, and resilience.	Shift from technical security metrics to business risk metrics, show what changed, where exposure is increasing or decreasing, and what decision or investment is required.

Building business confidence requires more than proving that security controls exist. It requires connecting assurance across security, privacy, and compliance while making remaining risk visible and understandable to decision-makers.

As application environments change, organizations must continuously reassess exposure, validate what has been achieved, and connect security performance to the decisions and investments that matter most to the business.

Non-negotiables for Modern AppSec

Trusted Software Supply Chain

Validate third-party components, dependencies, and SBOM accuracy before accepting them into your environment.

Increase SBOM coverage to transitive and vendor components, track vulnerabilities continuously, and mandate vendor SBOMs with clear remediation ownership.

Secure the development ecosystem across repositories, pipelines, workstations, packages, and automation.

AI, Trust & Governance

Establish clear AI risk ownership early, assigning accountability across security, technology, governance, and business teams.

Define required data validation before approving AI use, including data sensitivity, processing location, access controls, retention, and reuse.

Treat AI-generated recommendations as inputs that need validation, context, and supporting evidence.

Measuring Trust & Business Confidence

Independently validate critical controls with audit-ready evidence that withstands leadership scrutiny

Unify security, privacy, and compliance evidence to deliver a complete view of application trust.

Align security priorities and investments to business risk and outcomes.

CISO Speaks

After the event, we asked CISOs a few questions - here's what they had to say.

Ninad Chavan - Shares his perspective on SBOM as a strategic asset rather than a compliance checkbox, highlighting its role in understanding application components, identifying vulnerabilities early, and strengthening software supply-chain security.

Anuj Jha - Emphasizes the importance of a maker-checker approach to governance, where security practices are not only executed but independently validated, with clear accountability for the decisions and objectives behind them.

Shailendra Kumar Srivastava - Emphasizes that board-level trust must be backed by evidence, highlighting security-by-design, vulnerability management, and measurable SLAs such as mean time to detect and respond rather than simply reporting vulnerability counts.

Melwyn Rebeiro - Explains SBOM as a fundamental inventory of an application's building blocks and runtime components, highlighting its importance for identifying vulnerable components and versions before they can become attack vectors.

The Collective Verdict

The Mumbai edition of CISOverse highlighted a fundamental shift in application security: confidence in software is becoming a broader organizational concern as applications grow more interconnected and AI becomes embedded across the lifecycle. Applications are increasingly shaped by third-party components, open-source dependencies, software artifacts, and AI-driven development, making assurance harder to establish through isolated controls.

The discussions suggest that trust is no longer something organizations can establish at a single point in the application lifecycle. It has to be built into how software is sourced, developed, changed, governed, and ultimately evaluated for business impact.

This changes the role of AppSec from identifying individual weaknesses to establishing confidence in the decisions made around them. That means knowing which risks require action, understanding which risks can be accepted, ensuring AI-driven activity remains accountable, and having sufficient evidence to support those decisions.

For CISOs, the challenge is therefore not simply to increase security coverage, but to create a posture where risk can be understood in context and acted upon with confidence. This requires security, development, technology, governance, and business stakeholders to operate from a shared understanding of what matters and why.

ASPM can help enable this shift by connecting the signals, context, and workflows required to turn application security into a more continuous and decision-oriented practice.

Ultimately, trusted applications are not defined by the absence of risk, but by an organization's ability to understand that risk, govern it responsibly, and make informed decisions about it.

List of Attendees

Ninad Chavan
Cyber Security Consultant

Anuj Jha
CISO, Epimoney Pvt. Ltd.

Dr. Gopal Ji Gupta
CISO, Guardify Tech Pvt. Ltd.

Vinay Bhide
Chief Business Officer- Cyber Security, Pentagon System & Services Pvt. Ltd.

Melwyn Rebeiro
CISO, Julius Baer

Yogesh Rajawat
CISO and Head IT, Axium Global

Shailendra Kumar Srivastava
CISO

Shashank Dixit
Co-founder Boman.ai
Cybersecurity

Dr. Chidhanandham Arunachalam
Chief Program Officer- Sumeru & Co-founder- Boman.ai
Cybersecurity

Glossary

ASPM (Application Security Posture Management)
A centralized approach to aggregating, correlating, and prioritizing application security findings across tools (SAST, DAST, SCA, IaC, cloud, etc.) to enable business-aligned risk decisions, not just vulnerability reporting.

Audit-Ready Evidence
Continuously updated, verifiable proof that security controls are implemented and operating effectively. This includes mappings between vulnerabilities, applications, remediation actions, and compliance controls.

Business Criticality
The importance of an application or service to core business operations, revenue, customer trust, or regulatory obligations. Vulnerabilities in high-criticality applications carry greater business risk.

Compliance Mapping
The process of linking security findings and controls to regulatory frameworks (e.g., ISO, SOC 2, PCI-DSS) to demonstrate adherence without manual, point-in-time audits.

CVSS (Common Vulnerability Scoring System)
A standardized severity score for vulnerabilities based on technical factors. While useful, CVSS alone does not reflect real business risk without additional context such as exploitability, reachability, and asset criticality.

Developer Workflows
The tools and environments developers use daily, such as IDEs, pull requests, CI/CD pipelines, Jira, Slack, and GitHub, where security controls must be embedded to drive action.

Exploitability
The likelihood that a vulnerability can realistically be exploited by an attacker. This considers factors such as the availability of public exploits, attacker effort required, and environmental exposure.

False Positives
Reported security findings that are not real vulnerabilities or are not exploitable in practice. High false-positive rates erode developer trust and slow remediation efforts.

MTTR (Mean Time to Remediate)
The average time taken to fix identified vulnerabilities. Lower MTTR indicates higher security maturity, better developer alignment, and reduced exposure to risk.

Prioritization
The process of ranking vulnerabilities based on business impact, exploitability, reachability, and compliance risk, rather than technical severity alone, to determine what must be fixed first.

Production Risk Exposure
The presence of high or critical vulnerabilities in live, customer-facing (production) environments, where exploitation can result in immediate financial, operational, or reputational impact.

Reachability
Whether vulnerable code paths are actually accessible during runtime. Vulnerabilities in unreachable or unused code often pose little to no real-world risk despite high severity scores.

Risk Acceptance
A formal, documented decision by leadership to accept a known security risk when remediation is not feasible or justified, based on business context and impact.

Security Noise
Excessive, duplicate, or low-value security findings that overwhelm teams and distract from addressing real, exploitable risks.

About Us

Sumeru Information Security is a trusted cybersecurity partner for enterprises and startups alike, helping organizations secure their digital assets, manage risks, and build resilience in an AI-driven world. Backed by innovative products like Boman.ai, it's an AI-powered Application Security Posture Management (ASPM) platform, SOC 2 Type II certified, designed to make secure software development and DevSecOps easier to adopt.

It seamlessly integrates with developer workflows automating security across the development lifecycle to identify, prioritize, and provide AI-powered remediation guidance for vulnerabilities early, without disrupting developer productivity.

To learn more, visit **www.boman.ai**

The CISOverse Journey

CISOverse is a community-driven, vendor-agnostic initiative built by CISOs, focused on what CISOs truly need and believe in, not what vendors market or sell. It's evolving into a curated roundtable series, with each edition diving deep into the most pressing challenges in AI-driven security.

Edition 1 was held on 29th August 2025, focused on "Application Security in the AI Era." Key insights from this session were captured in the form of the CISO Speaks Series and a Playbook. More about it here: **https://cisoverse.org/August-2025.html**

Edition 2 took place on 12th December 2025, centered on "ASPM in Action: Turning Application Security into Business Decisions." Key insights from this session were captured in the form of the CISO Speaks Series and a Playbook. More about it here:
https://cisoverse.org/December-2025.html

Edition 2 took place on 10th April 2026, centered on "ASPM in Action: Application Security in the Age of AI." Key insights from this session were captured in the form of the CISO Speaks Series and a Playbook. More about it here: **https://cisoverse.org/April-2026.html**

With every session, the Playbook will grow, creating a dynamic, living repository of insights by CISOs, for CISOs. CISOverse's editions are thriving because of the insights, experiences, and collective wisdom shared by our incredible community. This is just the beginning. Stay connected as we gear up for the next edition of CISOverse to build a stronger, smarter, and more secure AppSec ecosystem.

If you'd like to be part of the 5th edition of CISOverse, reach out to us at tushar.gupta@ sumerusolutions.com. Let's shape the future of AppSec together.

In Association with

CySeck
Cyber Security Karnataka
K-Tech CoE for Cyber Security

Hosted by

boman.ai

SUMERU