CISO verse

# Application Security in the Age of AI

Curated from the inaugural CISO roundtable

## Partners & Supporters

BSIDES GOA

AHMEDABAD BSIDES

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 senior security leaders to tackle the toughest challenges in cybersecurity. It’s a peer-to-peer forum where CISOs exchange insights, stress-test new ideas, and shape the future of Application Security in the AI era.

The urgency is clear: 84% of cyberattacks now target applications, and early studies show the risks are multiplying with AI. A 2025 Veracode report found that 45% of AI-generated code failed security tests, with critical flaws like Cross-Site Scripting and languages like Java showing a 72% failure rate. At the same time, organizations adopting ASPM have seen a 40% faster mean-time-to-remediate, proving that unification and orchestration are key to managing this new reality.

Each CISOverse session produces a CISO Playbook, capturing practical insights and action items that leaders can take back to their enterprises.

## Executive Summary

CISOverse, organized by Boman.ai, brought together CISOs and cybersecurity leaders for an in-depth discussion on application security in the era of AI. As AI accelerates software development 10x, it also amplifies risk at the same pace. Traditional approaches to application security cannot keep up with this velocity. The solution isn't simply adding more tools, it lies in orchestration, visibility, and trust, enabled by Application Security Posture Management (ASPM). Through three dedicated tracks: Technology, Business, and Compliance, CISOs from diverse industries examined the most pressing AppSec challenges. This playbook captures their insights, experiences, and practical guidance to help organizations modernize application security for an AI-driven software lifecycle.

## CISOverse- Top Highlights

- *AI accelerates development, but risk multiplies*
  AI-assisted coding speeds up software delivery but expands attack surface and creates new classes of vulnerabilities, requiring stronger security oversight.

- *Security tools must evolve, not disappear*
  SAST and DAST remain essential but must integrate AI-driven intelligence for faster triage, noise reduction, and prioritization of exploitable risks.

- *Trust and transparency define the AI-era AppSec*
  Governance and explainability frameworks are critical to ensure AI-powered tools make secure and reliable decisions.

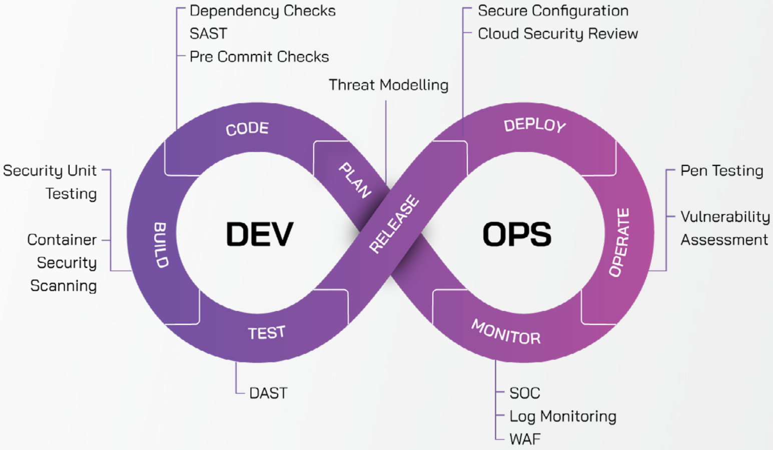
- *Developers are the frontline defenders*
  Security Champion Programs can integrate AI-focused training to enable, educate, and empower developers, and AI should provide context and guidance to them, not just flag vulnerabilities.

- *Demonstrating business value is essential*
  AI-powered AppSec must demonstrate tangible ROI- faster remediation, reduced regulatory exposure, improved brand protection, and accelerated go-to-market timelines.

AI accelerates development, but it also multiplies risk. To keep pace, organizations need more than point solutions; they need **ASPM as the orchestration layer.** ASPM unifies fragmented tools, reduces noise, and translates AppSec into a language that **board regulators and developers** can understand. It's not just another tool; it's the missing link between speed, security, and business value.

## Contents

## ASPM encompasses everything



## Diving Deep: AI in Application Security

The inaugural chapter of CISOverse, August 2025, welcomed **15 senior security leaders and CISOs from enterprises across India**. They are industry frontrunners driving large-scale security transformations, shaping AppSec strategies, and championing cybersecurity innovation within their organizations. Many of them are active voices in the cybersecurity community, contributing to thought leadership, policy influence, and knowledge-sharing across the ecosystem. The discussion revolved around three pivotal tracks on AI in Application Security:

***Technology:*** How should AppSec evolve in an AI-driven world- balancing speed with security, redefining the role of SAST/DAST, defending against emerging AI-driven threats, and establishing a maturity model for the future?

***Business:*** How can CISOs identify real value in AI-driven AppSec amid vendor hype, justify investments despite budget constraints, and demonstrate measurable business impact to the CEO and Board?

***Compliance:*** How can enterprises balance rapid AI-driven innovation with evolving AppSec risks, regulatory compliance, and third-party AI-related dependencies?

In the following chapters, you will get the insights of the attendees on these topics and more.

# Chapter 1: Technology

How should AppSec evolve in an AI-driven world- balancing speed with security, redefining the role of SAST/DAST, defending against emerging AI-driven threats, and establishing a maturity model for the future?

*"If we had to design an AI-integrated AppSec maturity model, I think its top three pillars would be:*
*1. Trust*
*2. Visibility*
*3. Business context awareness"*

*Divyendu Bhatt,*
CISO- Tech Startup

"The real problems AI should solve in AppSec are: false positives, reachability (are vulnerabilities exploitable?), developer enablement, and prioritization with consolidation. These are burning issues, and AI must address them to deliver real value."

*Shashank Dixit*
Co-creator Boman.ai

"AI writes code faster than humans... but with speed comes risk. AppSec must be fortified and enhanced with extra checks."

*Prashant Kandloor,*
Head of Research Group, Cybersecurity & Trust- Siemens Technology India

| *Insights* | *Recommendations* |
|---|---|
| AI accelerates development but expands the attack surface. | Treat AI-generated code as untrusted by default. Sandbox, review, and enforce policy-driven approvals before production. |
| Traditional SAST/DAST are foundational but insufficient | Evolve them into AI-augmented, intelligence-driven platforms that deduplicate findings, reduce noise, and prioritize based on exploitability. |
| AI introduces new attack vectors (prompt injection, model poisoning, malicious APIs) | Extend AppSec to cover AI-specific threat modeling and deploy real-time anomaly detection. |
| Without explainability, AI becomes just another black box, unacceptable for compliance. | Implement AI-explainability frameworks and maintain transparent logs of model decisions, data lineage, and remediation actions. |
| Developers are now frontline defenders | Launch AI-focused Security Champion Programs and embed just-in-time contextual training into developer workflows. |
| AppSec is shifting from detection-heavy to value-driven defense | Prioritize vulnerabilities based on business risk and runtime exploitability, not just counts. |

AI-driven Appsec should act as a business enabler and not an overhead. AppSec must prove ROI, business resilience, faster releases, and reduce downtime.

## Chapter 2: Business

How can CISOs pilot AI-driven AppSec tools before scaling to move beyond hype and demonstrate measurable business impact to the CEO and Board?

"Third-party risk is often the weakest link for any organization. Tools like OneTrust help with assessments, but many vendors treat compliance as a checkbox. When integrated into the enterprise, their weaknesses can expose vulnerabilities. That's a big risk area that needs attention with AI tools."

*Sheetal Suvarna*

Architecture Engineering, and Emerging Technologies Leader
Ernst & Young Global Consulting Services

"Don't present AI or AppSec as just another tool, show the business problem it solves. To win board support, speak their language; show how AI-driven AppSec drives revenue, manages risk, and avoids costly breaches."

*Shivakanth*

vCISO I Cybersecurity Advisor

"Many vendors confuse us by branding simple features as AI. Often, what they call AI is just content generation through LLMs. In demos, they highlight AI-powered features that aren't really AI. We should be clear on what counts as AI in security tools, and not get carried away by vendor marketing. That's an important distinction."

*Hilal Ahmad Lone*

CISO & VP- Liminal Custody

AI-driven AppSec isn't about finding more bugs- it's about protecting millions in breach costs, accelerating innovation, and giving the business the regulatory confidence to move faster.

*Dr. Chidhanandham Arunachalam*

Chief Program Officer, Sumeru

| *Insights* | *Recommendations* |
|---|---|
| Position AI-driven AppSec as a business enabler | Frame security as a driver of innovation, resilience, and revenue protection rather than a cost center. |
| Translate technical metrics into business outcomes | Replace vulnerability counts with business-aligned KPIs like breach-cost avoidance, downtime prevented, compliance penalties averted, and accelerated release cycles. |
| Speak the board's language | Communicate in terms of ROI, risk reduction, and competitive advantage, showing both the cost of inaction and the value delivered. Boards don't want to know how many vulnerabilities you've found; what matters is how much risk you've reduced, and how quickly you've reduced it. |
| Cut through AI-vendor hype | Demand proof-of-concept pilots and validate claims with measurable outcomes like improved remediation times, reduced false positives, and enhanced developer productivity. |
| Consolidate tools for cost and clarity | Use ASPM platforms to unify fragmented tools, simplify reporting, and deliver a centralized view of risk. |
| Assess third-party AI-risks proactively | Establish a vendor risk framework that evaluates model provenance, data handling, ethics, and compliance readiness. Vendor AI-failures will expose you to reputational and compliance damage. |
| Make security a growth accelerator | Collaborate with product and engineering teams to embed security into product roadmaps, enabling safe innovation at AI speed. |

**Future with AI in AppSec:** The focus must shift from counting vulnerabilities to demonstrating measurable business impact - risk avoided, downtime prevented, regulatory penalties averted, faster time to market, and protected customer trust and reputation.

## Chapter 3: Compliance

How can enterprises balance rapid AI-driven innovation with evolving AppSec risks, regulatory compliance, and third-party AI-related dependencies?

"Data is a goldmine, and without proper regulations and guardrails, managing privacy in the AI era will be extremely challenging. It's not just personal data, it's business data too."

*Sailaja Vadlamudi*

Vice President Security & Data Privacy Supply Chain Management- SAP Labs India

"In an AI-driven world, compliance can't be a checkbox- it demands continuous metrics, strong governance, and constant monitoring to balance speed with security."

*Amit Subhanje,*

Cybersecuirty Leader- RTX

"Another concern is malware in third-party dependencies. For example, there was a recent NPM vulnerability where contributors went rogue and injected malicious code. These supply chain attacks are very worrying, and AI must help detect and stop them."

*Saran Govindarajan*

CISO, Security Architect, Cumulocity IoT- Cumulocity

| *Insights* | *Recommendations* |
|---|---|
| Continuous assurance is the new standard | Embed continuous compliance controls into CI/CD pipelines with real-time risk scoring, evidence collection, and audit readiness. |
| AI introduces new compliance risks | Implement AI-explainability frameworks to track model provenance, decision logic, and third-party dependencies. |
| Compliance must move at AI-speed | Create compliance-by-design frameworks to ensure new features, AI-integrations, and releases meet regulatory requirements; automating checks against regulations like DPDP (India), EU AI Act (Europe), and SEC rules (US). AppSec must unify readiness and regulatory compliance across borders. |
| Third-party AI-risk is a compliance liability | Strengthen vendor risk assessments by evaluating AI-ethics, data usage, and compliance readiness during procurement. |

**Compliance in the AI era:** Organizations must unify readiness and regulatory compliance across borders.

### *Technology*

Goal: Secure AI-driven development, modernize AppSec, and reduce exploitability.

1. Treat AI-generated code as untrusted
2. Upgrade AppSec tooling
3. Expand AI-specific threat modeling
4. Implement AI-explainability frameworks
5. Launch Security Champion Program
6. Prioritize vulnerabilities by business risk

### *Business*

Goal: Align AppSec investments with business value and competitive advantage.

1. Position security as an enabler
2. Use business-aligned KPIs
3. Communicate in board language
4. Validate AI-vendor claims
5. Consolidate security tooling
6. Assess third-party AI-risks proactively
7. Embed security into product roadmaps

### *Compliance*

Goal: Automate, accelerate, and future-proof compliance for AI-driven environments.

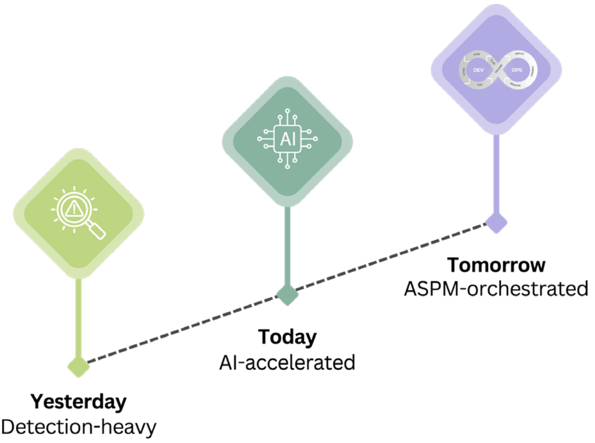
1. Implement continuous compliance
2. Track AI-specific compliance risks
3. Adopt compliance-by-design
4. Automate compliance checks
5. Strengthen vendor AI-risk assessments

## The Collective Verdict

The first edition of CISOverse reached a clear consensus: AI is accelerating development while multiplying risk, expanding the attack surface, and introducing a flood of new tools and methods of analysis. Fragmented solutions and siloed security approaches are no longer sustainable.

The path forward is orchestration: consolidating and unifying Application Security into a framework that speaks the language of developers, board regulators. ASPM is emerging as that orchestration layer: enabling trust, governance, and continuous validation while aligning security with business outcomes and regulatory priorities.

The verdict is clear: Application Security is shifting from yesterday's detection-heavy approach to today's AI-accelerated reality and toward tomorrow's ASPM-orchestrated future.



# List of Attendees

Amit Subhanje
Cybersecuirty Leader- RTX

Divyendu Bhatt
CISO- Tech Startup

Dr. Devam R Shah
CISO & DPO- Locus

Hilal Ahmad Lone
CISO & VP- Liminal Custody

Manikant R Singh
Senior Vice President & CISO- DMI Finance Private Limited

Prashant Kadloor
Head of Research Group, Cybersecurity & Trust- Siemens Technology India

Sailaja Vadlamudi
Vice President Security & Data Privacy Supply Chain Management- SAP Labs India

Saran Govindarajan
CISO & VP- Liminal Custody

Satish Kumar Dwibhashi
CISO- Fintech/NBFC

Sheetal Suvarna
Architecture Engineering, and Emerging Technologies Leader- Ernst & Young Global Consulting Services

Shivakanth
vCISO I Cybersecurity Adviso

Vasanth Kumar V
CISO & VP- Liminal Custody

Anand M R
Program Director- CySeck

Dr. Chidhanandham Arunachalam
Chief Program Officer, Sumeru

Shashank Dixit
Co-creator Boman.ai

## 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 ASPM tool powered by AI/ML for effortless, secure software development and to make DevSecOps easy to adopt. It offers security automation in a plug-and-play manner to find, prioritize, and provide guidance powered by AI/ML to remediate vulnerabilities early in the development lifecycle.

To know more, visit **www.sumerusecurity.com & www.boman.ai**

## CISOverse- Next Chapters

- CISOverse is evolving into a roundtable series where each session explores the latest challenges in AI-driven security.

- **Upcoming Theme:** *"ASPM in Action: Turning Application Security into Business Decisions."*

- With every session, the Playbook will grow, creating a dynamic, living repository of insights by *CISOs, for CISOs*.

CISOverse's first edition thrived because of the insights, experiences, and collective wisdom shared by our incredible community. And this is just the beginning. Stay connected with **CISOverse** and join us in building a stronger, smarter, and more secure AppSec ecosystem.

*If you'd like to be part of the **second edition** of CISOverse, reach out to us at **support@boman.ai** - let's shape the future of AppSec together.*

Partners & Supporters

Hosted by