ASPM in Action:

Application Security in the Age of AI

Built from real-world insights shared by CISOs

Chennai, Edition 3- April 10, 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.

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

Executive Summary

This edition of CISOverse reflects a pivotal shift in application security, as AI reshapes how software is built, tested, and deployed. With ASPM in action, CISOs are moving beyond fragmented security approaches toward a more unified, context-driven model that enables clearer decisions and stronger control in increasingly dynamic environments.

AI-driven development introduces new layers of complexity, unpredictability, and risk. CISOs are now navigating challenges that go beyond visibility, ranging from managing AI-generated code and autonomous workflows to dealing with rapidly evolving vulnerabilities and increasing signal noise. At the same time, business leaders continue to demand clarity on risk, measurable outcomes, and alignment with compliance and operational resilience.

Software is now being written, modified, and deployed at machine speed, often with limited human oversight. As development becomes increasingly autonomous, traditional AppSec approaches built around periodic testing, siloed tooling, and vulnerability counting struggle to keep pace with continuously evolving risk. In this environment, ASPM is emerging as the operational layer for modern application security.

This CISOverse discussion explored how Application Security Posture Management (ASPM) is becoming a practical approach to address these challenges. Rather than adding more tools, the focus has shifted toward unifying security signals, enabling contextual prioritization, and embedding decision-making into development workflows.

Across the three chapters: AI-driven AppSec, From AppSec Noise to Business Value, and Secure Development at AI Speed, the conversation evolved from understanding the impact of AI on application security to redefining how security is executed and measured. CISOs emphasized that the real challenge is not just identifying risks, but governing them in continuously changing environments, translating them into business-relevant outcomes, and operationalizing security without slowing innovation.

The discussions reinforced that when context, speed, and decision-making are aligned, application security transforms from a reactive function into a continuous, adaptive capability, one that enables organizations to innovate with confidence in the age of AI.

Who Should Use This Playbook

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

CISOverse- Top Highlights

- *AI Expands Risk Faster Than Security Can Keep Up*
  AI is enabling even non-developers to write and deploy code. However, it introduces unmanaged risks, including insecure code and unknown dependencies, which require secure development practices.

- *Noise Is the New AppSec Problem*
  AI-generated code is increasing vulnerability volumes rather than reducing them. Organizations are overwhelmed with findings, making it harder to identify what truly matters.

- *AppSec Must Speak the Business Language*
  Boards are not interested in vulnerability counts. CISOs must communicate in terms of financial risk, compliance exposure, revenue impact, and quantification. Storytelling is becoming core to AppSec leadership.

- *AI-Driven AppSec Still Lacks Trust*
  Trust in AI-generated systems at enterprise scale is still evolving. CISOs recognize the potential but remain cautious about reliability, control, and long-term sustainability.

- *Human Roles Are Moving Up the Value Chain*
  With AI handling L1 and L2 tasks, the role of humans is evolving toward L3-level expertise, focusing on risk acceptance, strategic decisions, and oversight. In short, the "human-in-the-loop" remains critical.

- *Traditional AppSec Is Breaking in the Age of AI*
  AI is transforming the entire software lifecycle, including writing, testing, reviewing, and even attempting remediation. In this multi-agent, continuously evolving environment, periodic assessments like VAPT are no longer sufficient.

AI is not just accelerating development; it is amplifying complexity, noise, and uncertainty across the application security landscape. The challenge is no longer about finding issues, but about making high-confidence decisions on what truly matters.

To address this, modern ASPM unifies fragmented signals and enables risk-based prioritization. It helps organizations move toward AI-aware, decision-driven application security aligned with business outcomes.

Contents

Diving Deep: ASPM in Action 1

ASPM Operational Model 3

Chapter: 1 AI-driven AppSec 4

Chapter: 2 From AppSec Noise to Business Value 6

Chapter: 3 Secure Development at AI Speed 8

Non-Negotiable for Modern AppSec 10

CISO Speaks 11

The Collective Verdict 13

List of Attendees 14

Glossary 15

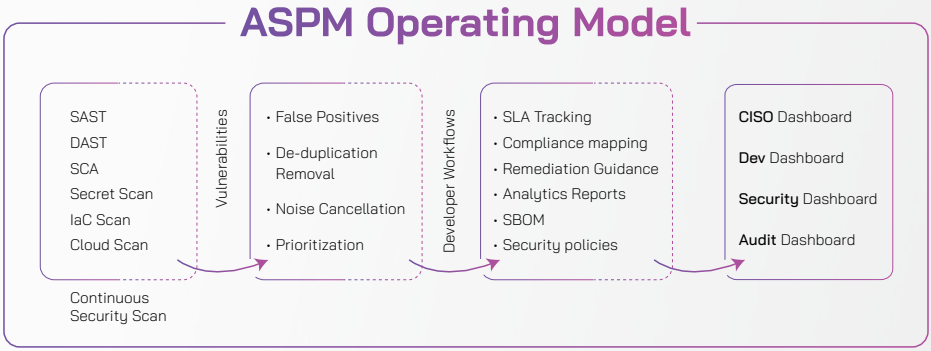
About Us 16

CISOverse - Next Edition 16

CISOverse Moments

Diving Deep: ASPM in Action

The April CISOverse session brought together CISOs and senior security leaders from enterprises across Chennai to explore how ASPM works in practice. These leaders are industry frontrunners driving large-scale security transformations, shaping AppSec strategies, and championing cybersecurity innovation within their organizations. Many of them are also active voices in the cybersecurity community, contributing to thought leadership, policy influence, and knowledge sharing across the ecosystem.



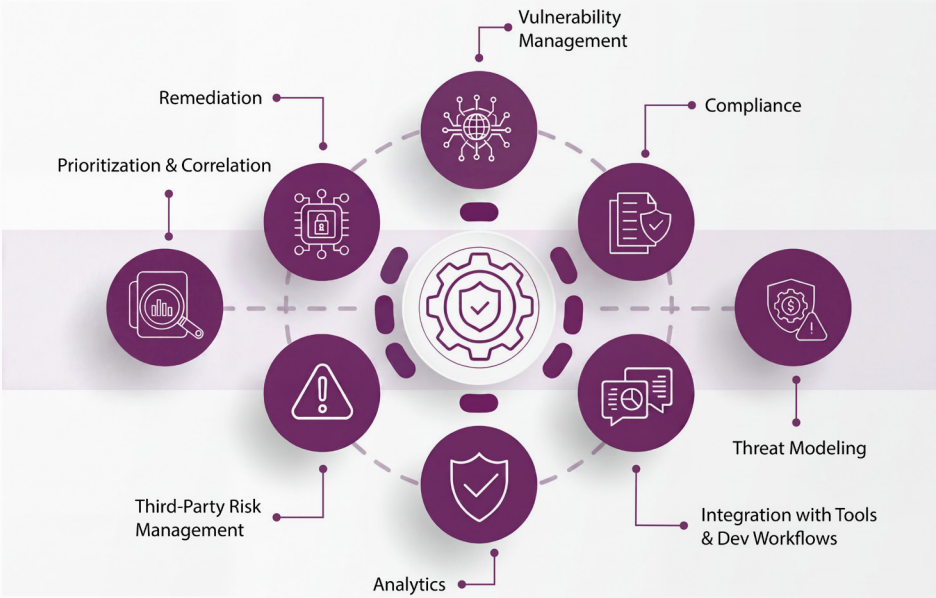
What is ASPM?

Application Security Posture Management (ASPM) tools are transforming application security by making it simpler, more accessible, and more effective. They unify scanning, vulnerability management, and remediation guidance into a single platform, replacing fragmented and complex workflows with a streamlined approach that enables teams of all sizes to adopt strong security practices.

When integrated into CI/CD pipelines, ASPM tools enable real-time vulnerability detection and mitigation support without slowing development. They deliver clear, actionable, and prioritized insights, allowing teams to quickly understand risks and remediate issues with confidence.

Core Components of ASPM Platforms

ASPM platforms go beyond traditional vulnerability scanning. They function as a central intelligence layer that aggregates, correlates, and prioritizes security signals across the entire SDLC.



The conversation was structured across three core tracks:

Chapter 1- AI-Driven AppSec: As AI is redefining both code creation and risk, organizations must achieve continuous, real-time visibility across complex application environments. This requires consolidating siloed tools into a unified view and focusing on the most critical risks at scale. AI-driven AppSec is also enabling intelligent remediation and continuous risk reduction.

Chapter 2- From AppSec Noise to Business Value: Amid thousands of findings, organizations must distill security data into a clear, business-relevant risk narrative. This requires contextual, measurable reporting, continuous compliance mapping, and the ability to quantify risk reduction, enabling CISOs to demonstrate ROI and align AppSec outcomes with business priorities.

Chapter 3- Secure Development at AI Speed: As AI accelerates development, security must be embedded seamlessly without slowing teams down. This requires unified workflows across Dev, Security, and Ops, along with automated generation of security requirements and continuously evolving threat models aligned with real-time code context.

The following chapters capture the collective insights from these discussions.

Chapter 1: AI-Driven AppSec

In the modern era, where application development is highly dependent on artificial intelligence, CISOs emphasize the key role AI will play in ensuring application security. They also highlight one of the most controversial points: AI still struggles to identify real risk and remediate what truly matters.

"While AI capabilities are now embedded across most tools, their fragmented implementation and inconsistent user competency often create more complexity than clarity, especially in multi-tool SaaS environments."

Dr. Kannan Srinivasan

Cybersecurity Business Unit Head, Happiest Minds Technologies

"The real concern with AI agents is governance: who controls them, what permissions they have, and how those are managed, because if a privileged system is compromised, the impact can be catastrophic at scale."

Santhosh Srinivasan

Vice President - Information Security, IT Infrastructure & Site IT, Celestica

"We leveraged Python and AI to consolidate vulnerabilities across multiple tools into a single unified dashboard, giving us a more streamlined and comprehensive view of risk."

Saravanakumar Krishnamurthy

CISO, Vivriti Capital

"The concern with AI is not just the access it has, but its ability to manipulate and expand that access, often beyond what we fully understand. That makes it a highly powerful and potentially risky capability."

Chidha

CISO & CPO, Sumeru Technology Solutions

Insights	*Recommendations*
AI does not inherently understand business logic, access boundaries, or misuse scenarios, leading to vulnerabilities that are technically valid but contextually risky.	AI agents operating with elevated access, unclear boundaries, and autonomous execution create new attack vectors that are not addressed by conventional vulnerability management approaches.
Individual tools perform as expected, but the lack of correlation across SAST, DAST, and runtime signals prevents teams from identifying compounded risks across the application lifecycle.	Adopt ASPM and implement unified correlation across SAST, DAST, SCA, and runtime data to uncover interconnected risks and eliminate fragmented visibility.
Frequent code changes and AI-generated modifications shift vulnerability locations and patterns, making it difficult to track recurrence, validate fixes, and maintain reliable security baselines.	Replace one-time assessments with continuous security validation that adapts to frequent code changes and evolving application behavior.
Traditional scanning and threat modeling struggle to keep pace with continuously evolving AI-driven application environments.	Continuously update threat models based on live code, behavior, and evolving attack surfaces.

AI-driven AppSec is moving beyond the traditional concept of securing code. In fact, it is more about governing autonomous systems that write, test, and modify applications in real time. As AI agents interact across the development lifecycle, the primary focus for CISOs and enterprises should not be limited to securing code, but to ensuring that systems operate within safe and intended boundaries. AI has also amplified the AppSec problems by increasing complexity and continuously evolving risks. In this environment, ASPM operationalizes the response through continuous visibility, contextual prioritization, and adaptive risk management.

Chapter 2: From AppSec Noise to Business Value

Today, application security is exposed to increasing noise, making it difficult to identify what actually impacts business outcomes. Therefore, CISOs must connect technical signals to real risk by shifting from vulnerability management to measurable, contextual decision-making aligned with business ROI.

"In India, the CISO role remains less clearly defined than in the Western world, often spanning strategic, tactical, and operational responsibilities, making the shift from operations to strategy a significant challenge."

Diptesh Saha
CISO & Practice Head, SNS India Pvt. Ltd.

"Organizations may be able to absorb compliance fines, but they cannot ignore the impact on share prices and investor confidence, which is what ultimately drives real accountability."

Dhanasekaran Madaswamy
Cybersecurity Leader, L&T Technology Services

"AI today makes it easy to quickly build and showcase products, but earning enterprise trust and achieving large-scale adoption will take time."

Shashank Pramod Dixit
Co-Founder, Boman.ai

"Organizations across the board are actively exploring how to leverage AI, whether in small use cases or larger initiatives, as it becomes a priority across all levels of business."

Gokulavan Jayaraman
Infosec Leader, Mahindra Group

Insights	*Recommendations*
While security tools generate extensive data, there is no standardized way to convert technical findings into business-relevant narratives.	Define a consistent model to translate technical findings into business risk.
The same security posture is interpreted differently by CISOs, developers, and business leaders. This misalignment creates gaps in decision-making.	Tailor communication for different audiences: developers, CISOs, and boards.
Even after remediation efforts, new vulnerabilities continue to emerge due to continuous scanning and code changes	Track how remediation impacts actual risk exposure over time rather than focusing solely on vulnerability closure metrics.
Organizations still rely on periodic, manual compliance activities that do not reflect real-time application risk. This results in audit-driven security rather than risk-driven security.	Continuously map application risk to compliance frameworks, ensuring alignment with actual system behavior.
Security findings are distributed across Dev, DevOps, and Security teams, often through ticketing systems. While this creates visibility, it also leads to diffused ownership and inconsistent remediation outcomes.	Define clear ownership across Dev, DevOps, and Security teams through structured workflows and measurable outcomes.

AppSec creates value only when risk is understood in business terms.
Raw findings alone are not enough to ensure application security and scalability. Business-relevant risk, continuous compliance, and contextual visibility enable leaders to move beyond noise, act with clarity, and justify investments to boards and key business stakeholders with confidence. This shift marks the evolution of modern AppSec from visibility to decision intelligence.

Chapter 3: Secure Development at AI Speed

The ever-evolving AI-based development process must embed security seamlessly without affecting developers' productivity and bring Dev, Security, and Ops into a shared workflow on a single platform. This shift is driving security from periodic validation to continuous governance across the development lifecycle.

"As AI makes development more accessible, more people are building applications without fully understanding the SDLC or Agile practices, creating a growing risk for organizations."

Gaurav Singh
CISO, Synergy Marine Group

"The real challenge with AI-developed solutions is ensuring control after deployment, as systems built and deployed by AI must be governed carefully to prevent them from acting beyond their intended purpose in production environments."

Maharajan Suriyanarayanan
VP - IT Infrastructure & CISO, Navitas Life Sciences

AI cannot yet be fully trusted with production data, and while it may be suitable for experimentation in controlled environments, organizations, especially in sensitive sectors like pharmaceuticals and life sciences, must be cautious about exposing critical data to it.

Vinod Senthil
Founder and Managing Director, digiALERT

"We are actively using AI in development and testing, but its application in cybersecurity is still evolving for us, which is why engaging with industry experts remains essential to better understand its role and potential."

Satish Kannan Marimuthu
CISO Associate Director, Sensiple

Insights	*Recommendations*
Security still sits outside developer workflows, creating friction in high-speed environments.	Embed security directly into developer tools (IDEs, PRs, CI/CD) to eliminate workflow friction.
AI-generated code lacks embedded security intent at the point of creation.	Integrate security requirements alongside functional requirements at the code generation stage.
Dev, Security, and Ops workflows remain disconnected, limiting end-to-end control.	Utilize unified platforms like ASPM to align Dev, Security, and Ops workflows end-to-end.
Continuous code changes outpace existing security validation mechanisms.	Implement automated validation to keep pace with rapid code changes.
Threat modeling is not aligned with rapidly evolving development cycles.	Adopt real-time, AI-assisted threat modeling integrated into the development lifecycle for proactive mitigation as applications evolve

Secure development at AI speed requires security to be built into the system, not applied as a checkpoint. As applications evolve rapidly, security must operate as an adaptive process that keeps pace with development and should not be treated as a bottleneck or afterthought.

Non-negotiables for Modern AppSec

AI-driven AppSec

Treat AI-generated code and decisions as untrusted by default, requiring continuous validation.

Consolidate fragmented tools into a unified, correlated risk view.

Establish feedback loops where human decisions continuously train and refine AI-driven security outcomes.

From AppSec Noise to Business Value

Focus on exploitable and high-impact risks over total vulnerability counts.

Continuously align application risk with compliance and audit requirements.

Present security outcomes as meaningful business risk insights.

Secure Development at AI Speed

Break silos by driving shared ownership across Dev, Security, and Ops.

Embed security directly into developer workflows without disrupting velocity.

Minimize developer decision fatigue by delivering only high-confidence, relevant actions.

CISO Speaks

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

Vinod Senthil - Shares his perspective on ASPM as an evolution of traditional application security, strengthening secure development and code protection. He highlights platforms like CISOverse for practical security insights and knowledge sharing.

Dhanasekaran Madaswamy - Explores the dual impact of AI on application security - AI for AppSec and AppSec for AI - highlighting how AI enhances visibility, identifies security gaps, and brings business context into risk management across applications. truly represents.

Dr. Kannan Srinivasan - Describes ASPM as a critical enabler for gaining a comprehensive view across application layers, APIs, and vulnerabilities, helping organizations accelerate secure development while maintaining complete visibility and control.

CISO Speaks

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

Gaurav Singh - Highlights how ASPM is evolving into a centralized decision-making layer, providing unified visibility across security tools and enabling CISOs, CTOs, and boards to prioritize risks and drive informed, executive-level decisions.

Diptesh Saha - Advises security leaders to focus on securing AI systems themselves, emphasizing the need for continuous risk quantification, board-level alignment, and embedding privacy-by-design principles when integrating AI into development.

The Collective Verdict

The Chennai edition of CISOverse highlighted a defining reality for modern application security: AI is accelerating software creation faster than traditional security models can adapt. Applications are now being developed, modified, and deployed in continuously evolving environments, introducing greater complexity, expanding attack surfaces, and increasing uncertainty across the software lifecycle. In many ways, AI has amplified the AppSec problem, not only by increasing the volume of risk, but by making security decisions significantly harder at scale.

Across discussions, CISOs agreed that security is shifting from periodic validation to continuous governance. Static assessments, isolated tooling, and vulnerability-centric approaches are no longer sufficient in environments where applications, dependencies, and AI-generated behaviors change constantly. The challenge is no longer limited to identifying findings, but to continuously governing risk in dynamic, AI-driven ecosystems without disrupting innovation.

This shift was reflected across all three conversations. In AI-driven AppSec, the focus has moved toward governing intelligent systems rather than simply securing code. In From AppSec Noise to Business Value, the emphasis shifted from visibility to decision intelligence, enabling organizations to prioritize risks in a business-relevant context. And in Secure Development at AI Speed, CISOs explored how security must evolve into a continuously adaptive function embedded directly into development workflows.

The discussions also reinforced a critical principle: while AI can accelerate detection, remediation, and operational efficiency, high-impact security decisions must remain human-led. Human judgment, contextual understanding, and governance remain essential in environments increasingly driven by autonomous systems.

The collective direction was clear: The future of AppSec will not be defined by who finds the most vulnerabilities. It will be defined by who can continuously govern risk across AI-generated, rapidly changing software ecosystems without slowing innovation.

ASPM is emerging as the operational response to this shift, bringing together visibility, context, prioritization, and governance into a continuous decision-making layer for modern application security.

And that is the future CISOs are now preparing for, and the conversation CISOverse is helping shape.

List of Attendees

Vinod Senthil
Founder and Managing Director, digiALERT

Dhanasekaran Madaswamy
Cybersecurity Leader, L&T Technology Services

Diptesh Saha
CISO & Practice Head, SNS India Pvt. Ltd.

Dr. Kannan Srinivasan
Cybersecurity Business Unit Head, Happiest Minds Technologies

Gaurav Singh
CISO, Synergy Marine Group

Gokulavan Jayaraman
Infosec Leader, Mahindra Group

Maharajan Suriyanarayanan
VP - IT Infrastructure & CISO, Navitas Life Sciences

Santhosh Srinivasan
Vice President - Information Security, IT Infrastructure & Site IT, Celestica

Saravanakumar Krishnamurthy
CISO, Vivriti Capital

Satish Kannan Marimuthu
CISO Associate Director, Sensiple

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 ASPM tool built with CISOs' inputs for the community at large. Powered by AI/ML for effortless, secure software development, it makes DevSecOps easy to adopt. It offers plug-and-play security automation to find, prioritize, and AI/ML-powered guidance to remediate vulnerabilities early in the development lifecycle.

To know more, visit **www.sumerusecurity.com and 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**

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 fourth edition of CISOverse, reach out to us at **tushar.gupta@sumerusolutions.com.** Let's shape the future of AppSec together.

In association with

CySeck
K-Tech Cell for Cyber Security

Hosted by

boman.ai SUMERU