CISOverse

ASPM in Action:

Turning Application Security into Business Decisions

Built from real-world insights shared by CISOs

Bangalore, Edition 2- December 12, 2025

Partners & Supporters

BSides Goa · BSides Bengaluru · 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 to have 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: **CISO Playbook and CISO Speaks Series.** These practitioner-first artifact captures shared insights, points of agreement, areas of friction, and actionable guidance that leaders can take back to their organizations. And 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, and this marks the second edition of the series.

Executive Summary

This edition of CISOverse highlighted a critical inflection point for application security, with ASPM emerging as the bridge that enables CISOs to translate technical security posture into clear, board-level insight and action.

As organizations adopt AI-assisted development and scale software delivery at unprecedented speed, CISOs face a familiar but intensified challenge. Visibility is fragmented across tools, developers are overwhelmed by noise, and boards increasingly demand clarity on risk, ROI, and business impact.

This CISOverse discussion explored how **Application Security Posture Management (ASPM)** is acting as the connective layer that transforms application security into business-aligned decisions. Rather than adding additional tools, participants emphasized orchestration, context, and prioritization, ensuring that security signals translate into actions that protect revenue, enable velocity, and support compliance.

Across the three tracks: **Visibility, Velocity, and Value,** the conversation moved from identifying problems to clarifying decisions. CISOs recognized that the core challenge is not the lack of security data, but the inability to consistently convert that data into prioritized action, developer-aligned workflows, and board-level confidence. The discussions reinforced that when exploitability, reachability, compliance impact, and business criticality are evaluated together and delivered through workflows teams already use, application security shifts from reactive reporting to intentional, outcome-driven decision-making.

Who Should Use This Playbook

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

CISOverse- Top Highlights

- *Prioritization is the real blind spot*
  Organizations are not lacking vulnerability data; they are struggling to determine which risks actually matter to the business.

- *Developer trust determines AppSec success*
  Security controls must live inside developer workflows and speak their language, or they will be ignored or bypassed.

- *ASPM is about orchestration and enabling business decisions*
  The value of ASPM lies in unifying existing tools (SAST, DAST, SCA, etc.), reducing noise, triaging vulnerabilities, preserving business context, and guiding remediations to enable business decisions.

- *Boards care about risk, not vulnerability counts*
  Application security must be communicated in terms of revenue impact, downtime prevented, and regulatory exposure avoided.

- *Human judgment remains essential*
  AI can automate scale and speed, but decision-making, risk acceptance, and ethical oversight must remain human-led.

- *CISO consensus on secure AI adoption for developers*
  CISOs broadly agreed that AI tools for developers are a net positive when they accelerate delivery without weakening security, are adopted at the organizational level, and operate within clearly defined guardrails.

- *Enabling AI support through guardrails code access*
  CISOs agreed that code can be shared in controlled environments with defined guardrails, allowing AI to assist in security requirement analysis and threat modeling without compromising data protection or control.

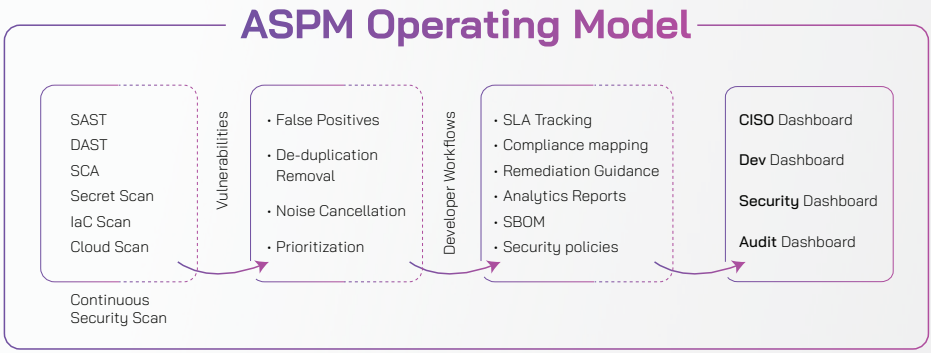
Developers are not opposed to security; they are willing partners when security is contextual, actionable, and embedded within their workflows. The challenge in modern application security is no longer about identifying vulnerabilities, but the ability to make consistent, informed business decisions. ASPM platforms address this gap by building confidence across developers, security leaders, and the board, through prioritized, context-rich insights that drive outcomes, not dashboards.

Contents

CISO verse Moments

Diving Deep: ASPM in Action

The December CISOverse session brought together CISOs and senior security leaders from enterprises across Bangalore to explore how ASPM works in practice. 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.



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. And 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.

The conversation was structured across three core tracks:

Chapter 1- Visibility: How can CISOs gain a single, trustworthy view of application risk that preserves business context, prioritizes what truly matters, and provides audit-ready proof in an AI-accelerated development environment?

Chapter 2- Velocity: How can organizations embed security guardrails into AI-assisted development workflows in a way developers accept, delivering only relevant, actionable findings while balancing AI automation with human oversight?

Chapter 3- Value: How can we quantify and communicate AppSec ROI in terms of measurable risk reduction and business impact, so that security posture can be answered confidently with a clear metric, influence board-level decisions, and be understood by leadership as a business enabler rather than a cost centre?

The following chapters capture the collective insights from these discussions.

Chapter 1: Visibility

Visibility gaps create uncertainty, not just technical risk. CISOs highlighted that the biggest challenge is not discovering vulnerabilities, but understanding which ones truly matter.

"Visibility gaps don't just create risk, they create uncertainty in business decisions. False positives waste developer time, slow releases, and weaken trust. We have plenty of findings, but prioritizing the right ones is where things break."

Dr. Chidhanandham Arunachalam
Chief Program Officer, Sumeru & Co-creator Boman.ai

"Context which is added to the different applications, prod, non-prod, internet-facing, business criticality, data sensitivity, compliance-heavy, all of this adds a lot of value and really helps to prioritize."

Shashank Dixit
Co-creator Boman.ai

"It actually comes down to how good your application security engineer is. It's never about the tools alone. Without ownership, it's just a fancy dashboard and the numbers will only keep growing."

Anvesh Yah
CISO- Exotel

Insights	*Recommendations*
Prioritization consistently emerged as the weakest link. High volumes of findings across SAST, DAST, SCA, IaC, and cloud tools delay remediation when teams cannot determine exploitability and business impact.	Rank vulnerabilities by business impact and exploitability, not just technical severity.
CVSS scores do not represent actual business risk. Severity ratings lack operational context and often overstate exposure when vulnerabilities are not exploitable or reachable at runtime.	Correlate signals across tools into a single, asset-centric risk view that preserves context.
Prioritization is a critical blind spot. An overwhelming volume of vulnerabilities reduces both developer focus and security team efficiency, delaying action on what truly matters.	Application risk must be tied to business context. Factors such as environment (prod vs non-prod), internet exposure, data sensitivity, compliance impact, and business criticality are essential for accurate prioritization.
Traditional, audit-driven compliance cannot keep pace with AI-accelerated development. Compliance becomes effective only when security findings are continuously mapped to real applications, data flows, and regulatory controls.	Automate compliance by embedding regulatory mapping directly into application security workflows and generating audit-ready reports.

AppSec's challenge is no longer finding vulnerabilities; it's deciding which ones matter.
Without a business context, severity-based prioritization creates noise and slows remediation. ASPM enables asset-centric, context-aware decisions that reduce real risk and position AppSec as a business enabler.

Chapter 2: Velocity

Developers are not opposed to security; they are opposed to friction. When security lives outside IDEs, PRs, and CI/CD pipelines, it is ignored.

"Security gates have to be where developers write code. IDE plugins and pipeline workflows are critical; that's where security has to live."

Anvesh Yah
CISO- Exotel

"When there's a flood of AI tools, it becomes an organizational responsibility, for the CISO, CTO, and security leaders, to decide which tools are allowed and how guardrails are applied."

Lalit Rawat
CISO- Kanerika

"No process can stop engineers from bypassing controls. The only way is to make PRs unmergeable and keep everything inside the ecosystem they already use."

Snehanshu Bhusan
CISO- Multiplier

"Getting security inside developer tools like Jira, Slack, and GitHub changes the whole game. Developers don't want to log into another platform."

Shashank Dixit
Co-creator Boman.ai

"In the AI era, speed is a business advantage only when security keeps pace. The real challenge isn't how fast we ship, it's how safely we can sustain that speed."

Dr. Chidhanandham Arunachalam
Chief Program Officer, Sumeru & Co-creator Boman.ai

Insights	*Recommendations*
Dashboards do not change behavior. Actionable guidance inside familiar tools such as GitHub, Jira, Slack, and IDEs was repeatedly emphasized as critical.	Embed AppSec controls directly into developer workflows by integrating security into IDEs, pull requests, and CI/CD pipelines, and automatically creating Jira tickets with clear ownership, remediation guidance, and SLAs supported by Slack or PR-based notifications instead of standalone dashboards.
Noise erodes trust. Duplicate findings, false positives, and unclear ownership reduce developer confidence in AppSec outputs.	Filter and enrich findings before they reach developers, focusing only on relevant, exploitable risks.
Security gates must be unavoidable but reasonable. Controls such as unmergeable PRs work when paired with clear remediation guidance and minimal disruption.	Provide clear ownership, remediation steps, and context with every issue.
AI should automate scale, not replace judgment. Participants agreed that AI excels at detection, deduplication, and prioritization, while humans remain essential for complex risk decisions.	Use AI to accelerate triage and guidance, while keeping risk acceptance and exceptions human-led.

AppSec succeeds only when it aligns with developer workflows.
Dashboards don't drive remediation; clear, contextual actions do. ASPM embeds precise, low-noise security guidance into IDEs, PRs, and CI/CD pipelines, using AI to accelerate triage while keeping risk decisions human-led.

Chapter 3: Value

Boards do not want vulnerability counts. They want clarity on **risk reduction, financial exposure, and business resilience.** To get the budget, we need to show business value.

"Boards speak the language of revenue and EBITDA. The moment you say this is a three million dollar risk and the tool costs five hundred thousand, the ROI becomes clear."

Abhishek Suresh
Associate Director & CISO- Alfahive Inc.

"For startups especially, justifying ROI is hard until an incident happens. Showing future risk prevention is always a challenge."

Snehanshu Bhusan
CISO- Multiplier

"External validation makes a difference. Independent penetration testing helps confirm that we've done our part and validates the issues we've identified internally."

Prathap R
Director Security Engineering- Circles

"If AppSec can't influence revenue, risk, or release decisions, it's just an expense!"

Dr. Chidhanandham Arunachalam
Chief Program Officer, Sumeru & Co-creator Boman.ai

Insights	*Recommendations*
ROI is best demonstrated through avoided costs: fewer breaches, reduced downtime, faster remediation, and earlier issue detection.	Translate AppSec metrics into business-aligned KPIs such as MTTR improvement, risk reduction, and compliance readiness. (Some key metrics are listed at the end of this chapter.)
Application security maturity increasingly affects M&A readiness and valuation. Buyers scrutinize AppSec posture as part of due diligence.	Establish a structured and mature application security program that provides measurable assurance to stakeholders. A well-governed AppSec practice builds confidence during due diligence, and supports higher valuation outcomes.
ASPM is often misunderstood as another security expense. The perception shifts only when outcomes are visible and measurable.	Frame ASPM as an enabler of safe innovation and delivery speed, not as a control layer.
Leadership alignment remains challenging. Buy-in gaps between CISO, CTO, and CIO can stall adoption even when security value is clear.	Engage leadership with outcomes, not tooling discussions. Use consolidated visibility to demonstrate how security investments protect revenue and customer trust.
Application security ROI is best demonstrated through measurable business outcomes- reduced risk, faster remediation, and avoided downtime; rather than vulnerability counts or dashboards. When security improvements translate into operational efficiency and resilience, their value becomes clear to leadership.	Communicate AppSec ROI using business-aligned metrics such as risk reduction, MTTR improvement, and downtime prevented. Focus on outcomes that protect revenue, ensure uptime, and enable faster, safer releases, positioning application security as a business enabler rather than a cost. (Some key metrics are listed at the end of this chapter.)

Key Metrics for Business-Aligned AppSec Decisions

AppSec ROI is realized when security outcomes drive business outcomes.
Value is measured by avoided breaches, reduced downtime, faster remediation, and assured compliance, not scan and tool coverage. By making risk measurable and defensible, ASPM elevates AppSec from a cost center to a strategic enabler of growth, valuation, and executive confidence.

Metric	What it measures?	Why it matters?
MTTR (Mean Time to Remediate)	Average time taken to fix vulnerabilities.	Shows remediation efficiency and security maturity.
Vulnerabilities vs Owners	Number of vulnerabilities mapped to teams/owners.	Drives accountability and clear ownership of risk.
Vulnerabilities vs Overall Risk	Vulnerabilities weighted by business criticality, data sensitivity, compliance risk.	Focuses effort on issues that matter most to the business.
Risk Introduced vs Risk Remediated	New risk added vs risk reduced per sprint/release.	Indicates whether security debt is increasing or decreasing.
False Positive Ratio	Percentage of reported findings that are false positives.	Reflects tool accuracy and developer trust.
Production Risk Exposure	High/critical vulnerabilities in production environments.	Highlights immediate, real-world business risk.

Non-negotiables for Modern AppSec

Visibility

Prioritize vulnerabilities based on exploitability and business context

Correlate multi-tool signals into a unified risk view

Treat AI models and third-party components as governed assets

Velocity

Embed security into IDEs, PRs, and CI/CD pipelines

Reduce noise through deduplication and reachability analysis

Use AI for scale, with humans retaining decision authority

Value

Communicate AppSec outcomes in board-level language

Track ROI through risk avoided and downtime prevented

Align AppSec strategy with business and M&A priorities

CISO Speaks

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

Anvesh Yah - Offers a succinct, one-line CISO perspective on ASPM and its role in modern application security programs, and explores how posture management tools connect the sources of vulnerabilities and help to prioritize them.

Abhishek Suresh - Shares his perspective on measuring AppSec maturity through meaningful metrics that align with business priorities like speed and revenue, and offers a crisp, CISO-level view on what ASPM truly represents.

Dr. Sashank Dara - Discusses how ASPM is evolving to enable executive-level visibility and decision-making, and explores strategies for securing AI-generated code while balancing innovation, speed, and acceptable risk.

Snehansu Bhusan - Shares his concise definition of ASPM from a CISO's lens and explains how security leaders can maintain strong AppSec standards as AI accelerates software delivery and expands the attack surface.

The Collective Verdict

The December edition of CISOverse, "ASPM in Action: Turning Application Security into Business Decisions", made one thing unmistakably clear: the AppSec problem is no longer about finding vulnerabilities; it's about what we prioritize, decide, and defend at a business level.

Participants agreed that most organizations already have enough scanners, dashboards, and reports. What they lack is the ability to confidently answer simple but critical questions: Which applications matter most to the business? Which risks actually need action now? And how do we explain those decisions to leadership without drowning in technical detail?

Across Visibility, Velocity, and Value, CISOs consistently pointed to the same gap. Application security breaks down when context is lost, when vulnerabilities are disconnected from business units, revenue impact, compliance obligations, and developer workflows. In that vacuum, prioritization fails, trust erodes, and security is seen as friction rather than enablement.

The collective view was that ASPM's real promise is not aggregation, but alignment; aligning security signals with how developers build, how leaders decide, and how businesses measure risk. When AppSec can show why something matters, who should act, and what happens if it is ignored, it stops being a reporting function and starts influencing outcomes.

The verdict from December edition of CISOverse was pragmatic and grounded: organizations that succeed will not be the ones that find the most issues, but the ones that connect application risk to business decisions and act on it consistently.

List of Attendees

Abhishek Suresh
Associate Director & CISO- Alfahive Inc.
Cybersecurity / Software (with AI services)

Anvesh Yah
CISO- Exotel
Cloud Communication / Telecom Tech

Dr. Sashank Dara
CTO, CISO & Co-founder- Seconize
Cybersecurity / Risk & Compliance Software

Lalit Rawat
CISO- Kanerika
IT Services & Consulting

Prathap R
Director Security Engineering- Circles
Telecommunications Technology

Snehansu Bhusan
CISO- Multiplier
Global Workforce Platform

Shivaling Salakki
Program Manager- CySeck
Cybersecurity / Government-Led Research & Skill Development

Aswin GM
Lead Engineer, Boman.ai
Cybersecurity

Neha Nanda
Program Coordinator, CISOverse

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 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**

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,** 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**

Current edition 2 took place on **12th December,** centered on **"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 editions are thriving because of the insights, experiences, and collective wisdom shared by our incredible community. And this is just the beginning.

Stay connected as we gear up for the next edition of **CISOverse** and join us in building a stronger, smarter, and more secure AppSec ecosystem.

If you'd like to be part of the **third edition** of CISOverse, reach out to us at **neha.n@sumerusolutions.com** - let's shape the future of AppSec together.

Partners & Supporters

Hosted by