

# iSMIG *Studio*

at Nullcon 2025



# Foreward from the Nullcon Founder



As we mark the 15th edition of Nullcon, I am filled with a sense of pride. What began in 2010 as a modest gathering of security researchers, hackers and enthusiasts has now grown into one of Asia's most influential platforms for hacking, learning, and collaborative cyber defense. Over the past 14 years, Nullcon has evolved into a confluence of hackers, researchers, policymakers, engineers, students, and C-suite professionals from India and global enterprises - all driven by one mission: building a more secure and resilient digital world.

An idea born out of the vibrant Null community — India's largest open security community and now having active international chapters — Nullcon continues to carry forward the values of openness, skill-building, and knowledge-sharing that defined its roots.

Nullcon Goa 2025 was more than just a milestone. With its hallmark features like the intense CTF battles, the groundbreaking Live Bug Bounty programs, and a spectrum of deep-dive trainings on reverse engineering, web application Security, IoT security, cloud and AI threats, we reinforced our commitment to hands-on learning and real-world impact.

This year, our collaboration with ISMG brought an added dimension of strategic dialogue and media depth. The in-depth interviews conducted at the ISMG Studio and curated discussions, the essence of Nullcon – disruptive ideas, technical excellence, and human connections – have been documented and amplified for a global audience.

This compendium not only captures the energy and purpose of Nullcon 2025 but also will help amplify the message to the global community. Thank you for being part of this journey. The next chapter begins now, and as always, Nullcon will remain a place “where hackers meet.”

## **Antriksh Shah**

*Founder,  
Nullcon*

---

Visit us online for more ISMG at Nullcon 2025 coverage:

[ismg.studio](https://ismg.studio)



# Nullcon Security Conference 2025: Asia's Largest Hacking Event for Shaping the Cybersecurity Industry



The 15th edition of the Nullcon Security Conference, hosted at the BITS Goa campus, convened a vibrant community of cybersecurity professionals, including policymakers, tech innovators, hackers, developers, students, partners and bug bounty programmers. The event fostered immersive learning, innovation and collaboration, all aimed at building a more secure digital world.

As the world faces unique cybersecurity challenges, there is a critical need for a strategic plan to secure the overall ecosystem. As strategic partners, ISMG - a global media organization focused on cybersecurity, IT, OT and artificial intelligence - partnered with Nullcon to engage deeply with the community and drive conversations that foster resilience across the cybersecurity ecosystem.

Over the past decade, Nullcon has evolved into a hub for cybersecurity advancement, skills developments and community engagement. The 15th edition of the event continued this legacy, with ISMG's editorial team facilitating insightful discussions and interviews with cybersecurity thought leaders, aimed at redefining leadership and securing the digital world.

As part of this strategic partnership, the ISMG.Studio division captured insights from distinguished speakers, including CEOs, CISOs, policymakers, government leaders, researchers, innovators, hackers, investigators and legal experts, through distinct, in-depth interviews. These conversations explored innovative approaches, collaborative thinking, skills development, talent acquisition and industry vision for embracing emerging technologies and disruptive tools.

Key topics discussed included iOS security, third-party SaaS, cyber defense, AI in cybersecurity, bridging silos through cyber fusion centers, rethinking security in a hyper-connected world, AI in SecOps, zero trust, API security, secure by design and cloud-first strategies.

Comprehensive coverage of Nullcon Goa 2025 is featured across ISMG's Asia media network, including [inforisktoday.asia](https://inforisktoday.asia), [bankinfosecurity.asia](https://bankinfosecurity.asia) and [databreachtoday.asia](https://databreachtoday.asia). You will also find engaging panel discussions and Profiles in Leadership interviews featuring members of our CyberEdBoard community.

Within these pages, you'll discover exclusive interviews and key takeaways from the leaders and practitioners shaping the future of cybersecurity. Nullcon Goa 2025 was not just an event, it was a movement to build a stronger, smarter and more secure digital world.

## **Geetha Nandikotkur**

*Vice President - Conferences, Asia, Middle East and Africa,  
Information Security Media Group*

Visit us online for more ISMG at Nullcon 2025 coverage:

[ismg.studio](https://ismg.studio)



# Video Interviews

Matthias Frielingsdorf, <i>iVerify</i> .....6	Ashish Shrivastava, <i>Honeywell Int.</i> ..... 16
Shubham Mittal, <i>RedHunt Labs</i> .....6	Vikas Goyal, <i>FIS Global</i> ..... 17
Arindam Roy, <i>SANS Institute</i> .....6	Hilal Lone, <i>Razorpay</i> ..... 17
Rishi Rajpal, <i>Concentrix</i> .....6	Saikat Datta, <i>DeepStrat</i> ..... 17
Chandrashekhara Basavanna, <i>SecPod Tech</i> .8	Satyavathi Divadari, <i>Freshworks</i> ..... 17
Cassie Crossley, <i>Schneider Electric</i> .....9	Asuka Nakajima, <i>Elastic</i> ..... 18
Mathan Babu Kasilingam, <i>Vi</i> .....10	Parag Deodhar, <i>Accenture</i> ..... 19
Varun Singla, <i>Bharti Airtel</i> ..... 11	Prateek Singh, <i>Eaton</i> ..... 20
Daniel Cuthbert, <i>Black Hat Review Board</i> .11	Komal Vora, <i>Equifax Credit Information</i> ..... 21
Pavan Mohan, <i>ServiceNow &amp; Pankaj Mouriya, Kong</i> ..... 11	Dennis Giese, <i>Amazon</i> ..... 22
Pablo Endres, <i>SevenShift</i> ..... 11	Krishna Pandey, <i>Xerox Cybersecurity</i> ..... 22
Yogi Kapur, <i>Salesforce</i> ..... 13	





“We've historically followed a build-deploy-fix cycle, but that's no longer sustainable. With AI agentic models gaining traction, we need security embedded at the foundational level.”

**Daniel Cuthbert**

Security Researcher, Black Hat Review Board

## iOS Security Survives EU's App Store Shakeup

iVerify's **Matthias Frielingsdorf** on Using Forensic Data Against Zero-Click Threats



Apple's walled garden faces new openings as EU regulations mandate third-party app store access. But iOS's fundamental security architecture stands firm against potential threats, said Matthias Frielingsdorf, co-founder and vice president research at iVerify.

[WATCH ONLINE](#)

## Security Blind Spots: The Hidden Risk of Third-Party SaaS

RedHunt Labs CEO **Shubham Mittal** on Overlooked Attack Surface Risks



Security teams monitor their digital assets, but third-party SaaS tools such as GitHub, Docker and Postman remain blind spots. RedHunt Labs CEO Shubham Mittal explains why enterprises must enhance their attack surface management and how RedHunt Labs' research is uncovering widespread security gaps.

[WATCH ONLINE](#)

## Bridging South Asia's Skill Gap With AI-Focused Training

SANS Institute's **Arindam Roy** on Hands-On Learning for Real-World Security Threats



South Asia faces a critical cybersecurity skills gap. This shortage extends across private enterprises and government sectors, exacerbated by insufficient quality certification bodies and training institutes in the region, said Arindam Roy, country director for South Asia at SANS Institute.

[WATCH ONLINE](#)

## Beyond the Black Box: Building Trust in AI Cybersecurity

Concentrix's **Rishi Rajpal** on AI Defense Strategies and Data Protection Compliance



AI is reshaping cybersecurity operations, both as an attack tool and as a defense mechanism, said Rishi Rajpal, global vice president of global security at Concentrix. He discusses the importance of explainable AI, building trust in automation and aligning AI governance with regulatory frameworks.

[WATCH ONLINE](#)



“Maybe a sophisticated attacker can trick a user into installing their application and use additional exploits, and maybe there is a little bit more lack in remediation afterwards.”

**Matthias Frielingsdorf**

Co-Founder, iVerify

A portrait of Chandrashekhara Basavanna, CEO of SecPod Technologies. He is a man with dark hair, wearing a light blue blazer over a white collared shirt. He is looking directly at the camera with a neutral expression. The background is dark and out of focus.

**Chandrashekhara Basavanna**

CEO, SecPod Technologies

## Prevention-First Security: A Game-Changer in Cyber Defense

SecPod CEO **Basavanna** on the Shift From Detection to Proactive Risk Mitigation

The cybersecurity landscape is undergoing a significant shift as organizations move from a reactive detection-and-response model to a prevention-first approach. This transformation focuses on identifying and mitigating vulnerabilities before attackers can exploit them.

---

“Relying solely on detection and response is like playing a losing game.”

-*Chandrashekhara Basavanna*

---

WATCH ONLINE



**Cassie Crossley**

Vice President, Supply Chain Security,  
Cybersecurity & Product Security Office, Schneider Electric

## Secure by Design Must Lead Software Development

**Crossley** of Schneider Electric Urges Supplier Scrutiny and Continuous Risk Review

To strengthen defenses, organizations must adopt secure-by-design practices, select mature open-source components and embed risk awareness throughout development, according to Cassie Crossley, vice president, supply chain security, cybersecurity and product security office, Schneider Electric.


WATCH ONLINE

---

“As software developers, we're not necessarily trained on cybersecurity and that part of the process, which is the secure by design.”

-Cassie Crossley

---

A portrait of Mathan Babu Kasilingam, a middle-aged man with short, graying hair, wearing a light-colored button-down shirt. He is looking directly at the camera with a neutral expression. The background is dark and out of focus.

**Mathan Babu Kasilingam**

CISO, Vi

## DPDP Act: Compliance and Data Protection Challenges

**Kasilingam** of Vi on Breach Notification and Managing Data Privacy at Scale in India

India's DPDP Act mandates significant changes for enterprises handling consumer data. Ensuring informed consent across a diverse population presents significant hurdles. With a population of 1.4 billion, ensuring informed consent is complex, said Mathan Babu Kasilingam, CISO, Vi.

[WATCH ONLINE](#)

---

“Take your time to investigate the breach, but in a time-defined manner. Close that and report back is the expectation. So it is an easily acquirable and doable path.”

*-Mathan Babu Kasilingam*

---

## AI, Zero Trust and the Next Cybersecurity Frontier

AI and Zero Trust Are Reshaping Cybersecurity and Risk Management



Artificial intelligence in cybersecurity is evolving from anomaly detection to predictive capabilities, and organizations are embracing AI-driven threat detection and zero trust architectures over traditional security measures, said Varun Singla, senior vice president and CISO at Bharti Airtel.

WATCH ONLINE

## Rethinking Security in a Hyperconnected Digital World

Security Researcher **Daniel Cuthbert** on Why a Security-First Approach Is Essential



A senior security researcher Daniel Cuthbert emphasizes the need for a proactive security mindset, urging developers to integrate robust threat modeling and secure software architecture from the ground up rather than relying on reactive fixes.

WATCH ONLINE

## Bridging Cybersecurity's Skill Gap Through Open Communities

ServiceNow's **Mohan** and Kong's **Mouriya** Discuss Mentorship in Security Training



The cybersecurity industry faces a critical skills gap, with companies struggling to find skilled professionals with not only qualifications but also real-world expertise. The Null Community is tackling this challenge by fostering mentorship, networking, and hands-on learning.

WATCH ONLINE


## IoT Security: A Business Imperative

SevenShift's **Pablo Endres** on Shadow IoT, Compliance Pressures and Risk Mitigation



IoT security remains a critical challenge as organizations integrate more connected devices into their environments. A strong security program requires "asset visibility, secure protocols and network segmentation," said Pablo Endres, managing director and security consultant at SevenShift.

WATCH ONLINE

A close-up portrait of a man with long, dark brown hair and a full, dark beard. He is looking directly at the camera with a neutral expression. The background is dark and out of focus. The lighting is soft, highlighting his facial features. In the bottom right corner, there is a small, stylized graphic of a blue and white pattern, possibly representing a circuit or data flow.

“Teaching reverse engineering techniques to security engineers or to developers helps you to understand what your threat actually is, and it enables you to design threat models, way more efficiently, because most of the time, security engineers don't have an idea what exactly is possible.”

**Dennis Giese**

Senior Researcher, Amazon



## Yogi Kapur

Sr. Director, Security Operations, Salesforce

# Human Intelligence vs. AI Threats - the Fusion Advantage

Salesforce's **Kapur** on Creating Cohesive Security Units Across Global Operations

Cyber fusion is transforming traditional security operation centers into proactive defense mechanisms, said Yogi Kapur, senior director of security operations at Salesforce. Despite AI advancements benefiting defenders, "threat actors are always slightly ahead" in exploiting emerging technologies.

---

"The most precious resource, even in this AI world, is human time."

-Yogi Kapur

---

WATCH ONLINE



“That [robust API security design and architecture] includes not only the runtime on which it's going to run, it's also the infrastructure that's going to interact with the dependencies and the permissions that it has - basically, identity and access management - how we authenticate and authorize any requests that come for the APIs.”

**Hilal Lone**

CISO, Razorpay



“Since the Cyber Resilience Act also has fines like GDPR, that's going to make a big impact, because the moment that C-level feels, 'if we make a mistake here, this will cost us 5% of our global income,' that is something that they bring it to their table.”

**Pablo Endres**

MD & Security Consultant, SevenShift

A portrait of Ashish Shrivastava, a man with dark hair and glasses, wearing a blue suit jacket over a light blue and white striped shirt. He is looking directly at the camera with a slight smile.

## Ashish Shrivastava

Director - Cyber Security, Honeywell International

# Industrial Security Crises Demand Design-Phase Interventions

Honeywell's **Ashish Shrivastava** on Security by Design for OT Environments

Industrial control systems face security crises as legacy systems - designed without security safeguards - connect to modern cloud infrastructures, leading to critical vulnerabilities across operational environments, said Ashish Shrivastava, director of cybersecurity at Honeywell International.

WATCH ONLINE

---

“Wherever we use security by design, the purpose is to integrate security in the very initial stage in the product life cycle, and it has to be maintained throughout from starting until the product is going in the market.”

-Ashish Shrivastava

---

## Cyber Fusion Centers Shift Security From Silos to Synergy

FIS Global's **Vikas Goyal** on Unifying Tools and Teams to Improve Threat Detection



Cyber fusion centers represent a shift from siloed security operations to unified, real-time threat response. By integrating teams and tools, organizations can streamline incident handling, reduce false positives, and respond to zero-day threats more effectively, said FIS Global's Vikas Goyal.

[WATCH ONLINE](#)

## Backbone to Battleground: Safeguarding APIs in FinTech

Razorpay CISO **Hilal Lone** on API Security, Architecture and Proactive Defense



API security is essential for fintech platforms to prevent threats such as credential stuffing and API scraping. A strong architecture, authentication and proactive defense will shape the future of API security, according to Hilal Lone, CISO at Razorpay.

[WATCH ONLINE](#)

## Security by Design, Not an Afterthought

DeepStrat CEO **Saikat Datta** on Embedding Cybersecurity in Business Priorities



The relationship between government regulations and enterprise security practices remains fraught with challenges - both at the human level and on the technological front, said Saikat Datta, founder and CEO, DeepStrat, who makes the case for better collaboration between enterprises and government.

[WATCH ONLINE](#)

## Security as an Enabler in Cloud-First Environments

Freshworks' **Satyavathi Divadari** on Transforming Security From Gatekeeper to Enabler



Modern SaaS companies must embed security from the beginning rather than as an afterthought, said Satyavathi Divadari, deputy CISO at Freshworks. She shares insights on shifting security left, creating a security-focused culture and preparing for evolving threats in cloud-native environments.

[WATCH ONLINE](#)



## Asuka Nakajima

Senior Security Research Engineer, Elastic

# How Threat Actors Weaponize Keylogging With Malware Bundles

Elastic's **Asuka Nakajima** Discusses Detection Methods for API-Based Keyloggers

Today's sophisticated malware incorporates key logging features along with other information-stealing techniques to capture sensitive data, including financial information that traditional credential-dumping methods might miss, said Asuka Nakajima, senior security research engineer at Elastic.

WATCH ONLINE

---

“When a hotkey-based keylogger captures a user's keystroke, it emulates the user input, just to make that key input appear as standard to the computer normally, and that circumvents detection.”

-Asuka Nakajima

---

A portrait of Parag Deodhar, a middle-aged man with dark hair, wearing a dark suit jacket over a light blue checkered shirt. He is looking directly at the camera with a slight smile.

## Parag Deodhar

Managing Director – Internal Audit, Global IT Audit Lead, Accenture

# AI's Role in SecOps: Speed, Efficiency and Data Challenges

**Parag Deodhar** of Accenture Says AI Accuracy Hinges on Clean, Unbiased Data

AI is transforming SecOps by automating threat detection, triaging alerts and accelerating incident response. But its effectiveness depends on model and data accuracy to avoid false positives, said Parag Deodhar, managing director, internal audit, and global IT audit lead at Accenture.

---

“Analysts have to go through manually checking each alert and checking whether it's a false positive or whether it needs to be investigated.”

*-Parag Deodhar*

---

WATCH ONLINE



## Prateek Singh

Lead, OT Cybersecurity Services, APAC, Eaton

# OT Security Requires Skills Beyond IT

**Prateek Singh** of Eaton on Bridging the OT Security Gap in Industry 4.0

As industrial systems connect to cloud networks and remote users, they become more vulnerable to cyberthreats. Ensuring security across these environments means adopting stronger governance and training professionals who understand both domains, according to Prateek Singh of Eaton.

[WATCH ONLINE](#)

---

“Cybersecurity has been always inclined toward IT. We do not have people who have knowledge about how industrial domains work, how systems or machines work on the shop floor.”

*-Prateek Singh*

---



## Komal Vora

CISO, Equifax Credit Information

# Why AI and Encryption Are Essential for Finance

Equifax Credit's **Komal Vora** on AI, Data Security and Rapid Incident Response

AI-driven technologies have transformed incident response, replacing manual threat detection with automation. Komal Vora, CISO at Equifax Credit Information, shares insights on rapid threat mitigation, the critical role of encryption and vendor risk management amid rising cyberthreats.

---

“I have worked in the financial sector, so data is most critical for us - at rest, as well as in transit.”

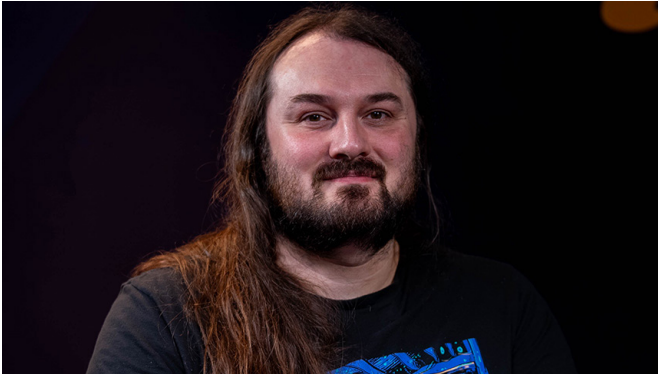
-Komal Vora

---

[WATCH ONLINE](#)

## IoT Security Gaps Put Enterprises at Risk

**Dennis Giese** on Reverse Engineering, Flawed Authentication, Poor Threat Modeling



IoT security flaws expose users and businesses to serious risks. Weak authentication methods allow attackers to manipulate devices, leading to data breaches and privacy violations. Reverse engineering highlights these weaknesses, said Dennis Giese, IoT security and privacy researcher.

[WATCH ONLINE](#)

## Why Responsible AI Is No Longer Optional for Enterprises

Xerox Cybersecurity's **Krishna Pandey** on AI Hallucinations, Governance and Shadow AI



With regulatory demands and public trust at stake, Krishna Pandey of Xerox Cybersecurity underscores the urgency of human oversight, ethical governance and risk-aware AI adoption. "We have seen hallucinations where you can't trust the AI, so there has to be a human in the loop," he said.

[WATCH ONLINE](#)

# iSMG Studio

## About ISMG

ISMG is the world's largest media organization devoted solely to cybersecurity and risk management. Each of its 38 media properties provides education, research, and news that is specifically tailored to key vertical sectors including banking, healthcare, and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, AI, OT, and fraud. Its annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

## Contact

(800) 944-0401  
info@ismg.io

## Sales & Marketing

**North America:** +1-609-356-1499  
**APAC:** +91-22-7101 1500  
**EMEA:** + 44 (0) 203 769 5562 x 216

BANK  INFO SECURITY® CAREERS  INFO SECURITY® C  INFO SECURITY® Just for Credit Unions

Data Breach  
Prevention, Response, Notification. TODAY

 HEALTHCARE  INFO SECURITY

 GOV  INFO SECURITY®

infoRisk  
TODAY

CyberEd.io FraudToday.io PaymentSecurity.io DeviceSecurity.io CyberEdBoard

OT.today

AIToday.io

CIO.inc

ATHENA

CYBER  
THEORY

Xtra mile  
LIFECYCLE MARKETING

OC MEDIA

SUMMIT

custom  
events

roundtables

NULLCON

hardwear.io  
Hardware Security Conference and Training

iSMG  
Studio

# iSMG

902 Carnegie Center • Princeton, NJ • 08540 • ismg.studio