DSCI
PROMOTING DATA PROTECTION

FINSEC CONCLAVE 2024

EVENT REPORT

INNOVATION-CENTRIC REGULATIONS
ESG ADOPTION
FINANCIAL DIGITAL INFRASTRUCTURE
NEXT GEN TECH
DATA CENTRALITY
FRAUD CONSCIOUSNESS
OPEN BANKING & FINANCE
CYBER RESILIENCE
DATA SECURITY COUNCIL OF INDIA
FINANCIAL SECURITY CONCLAVE 2024

04-05
JUNE'24

THE WESTIN
POWAI LAKE, MUMBAI

FINSEC2024
# DSCI

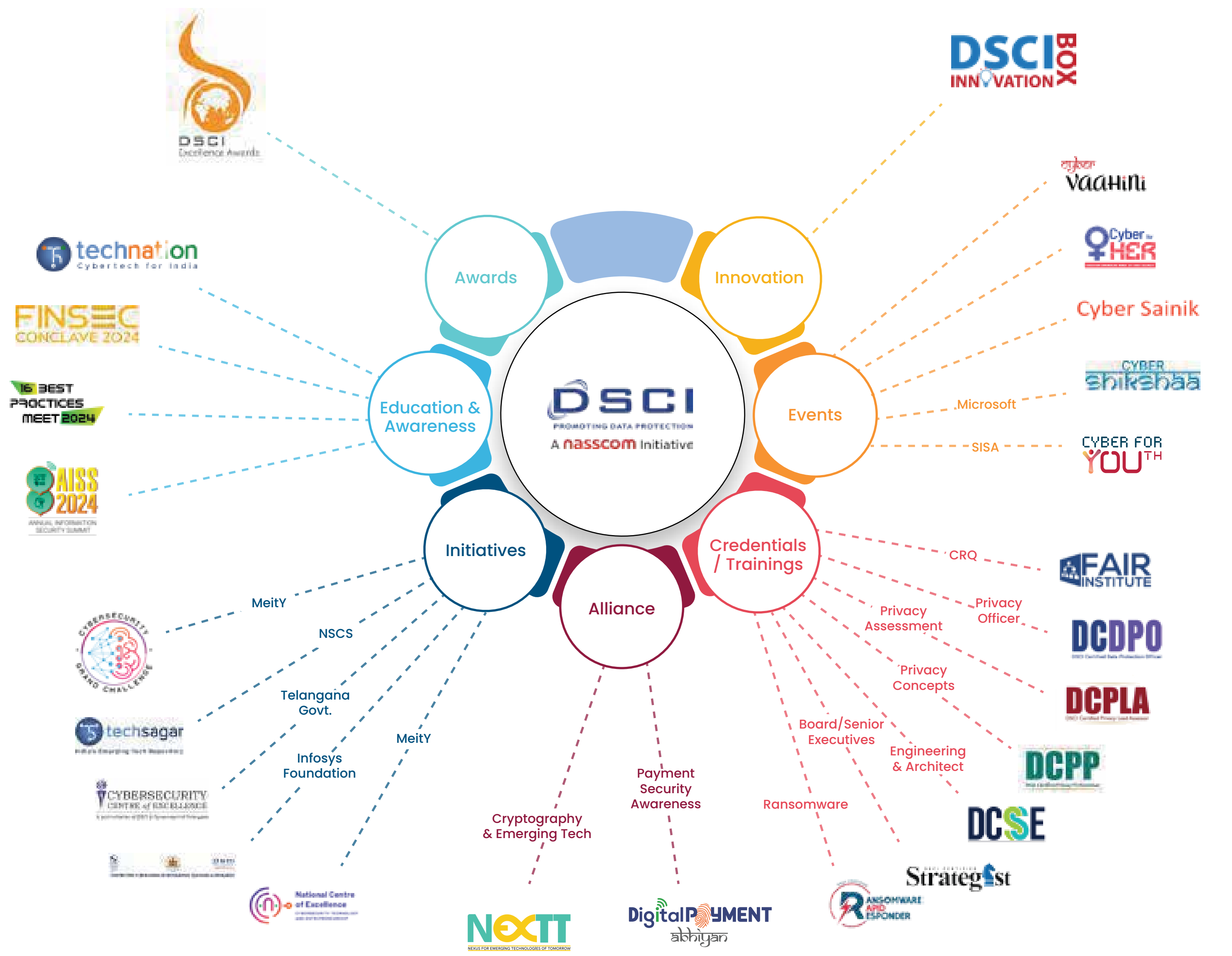
CONTENT

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by Nasscom®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy.

DSCI works together with the government and their agencies, Law Enforcement Agencies (LEA), industry sectors including IT-BPM, BFSI, CII, telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: www.dsci.in



About FINSEC 2024

The sixth edition of the DSCI FINSEC Conclave examined key developments and trends that transpired over the past year, especially those that had the potential to significantly impact the future Security & Privacy roadmaps of the BFSI sector. It endeavored to accomplish this by drawing upon the expertise, experience, and foresight of leaders, practitioners, policymakers, researchers, developers, and innovators. While nefarious elements continued to upgrade their arsenals to infiltrate organizational networks, organizations also sought to equip themselves with state-of-the-art security measures.

Some of the pressing themes that were part of this year's agenda included Ransomware Resilience, Modernization of Security Operations, Innovation-centric Regulations, ESG Adoption and Sustainable Finance, the AI-fueled Financial Services Landscape, the Future of Authentication and Authorization, and Expectations and Obligations at the Board Level, among others. The conclave also brought together banks, neo-banks, insurers, securities firms, banking financial entities, cooperatives, and fintech companies to network and engage in immersive dialogues, knowledge-sharing sessions, and deliberations.

As the country made substantive progress toward comprehensive Data Privacy legislation, the emphasis was on preparedness and the implementation aspects of Privacy, which was one of the core focus areas for financial services organizations that year. FINSEC 2024 placed keen focus on the implementation challenges that organizations grappled with in the realms of data governance, data protection, and data management.

In essence, the Summit provided insights into the Cybersecurity landscape of the country's BFSI sector by highlighting the technological flux that fueled digitization while also generating Security & Privacy concerns and opportunities.

Bird’s Eye View

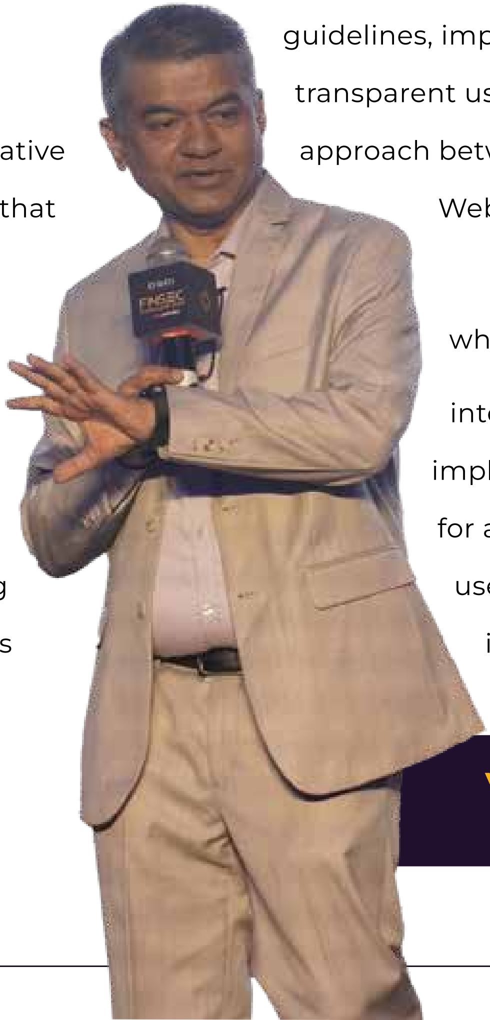
80+	Global Leaders / Industry Experts
400+	Companies Participated
05	Workshops
26	Total Sessions
05	Startups competing at DSCI Innovation Box – FINSEC
11	Industry Keynotes
03	Reports/ Whitepapers Launched
900+	Delegates
50+	Partners & Exhibitors from BFSI
20	Exhibition Booths
02	Networking Dinners
17	Start-ups Showcased at NCoE Innovation Arcade
👩	Women in Security Program Launch – Cyber Vahini

Inaugural Session

The inaugural session was led by **Mr. Vinayak Godse, CEO, Data Security Council of India (DSCI)**, who helped everyone explored the transformative potential of Web 5.0 and its implications for the future of connectivity and interaction. He explained how Web 5.0 aimed to create a more emotionally intelligent and intuitive internet, moving beyond the static nature of Web 1.0, the user-driven content of Web 2.0, the semantic capabilities of Web 3.0, and the automation of Web 4.0. Mr. Godse further emphasized that Web 5.0 sought to integrate artificial intelligence (AI) and brain-computer interfaces (BCIs) to enable digital systems to understand and respond to human emotions in real time. He discussed how such advancements could revolutionize industries like education, where learning platforms could adapt dynamically to students' emotional states, and healthcare, where AI-driven systems could offer immediate mental health support based on emotional analysis.

However, he also acknowledged the significant ethical and privacy challenges associated with this evolution. He even pointed out that the collection and processing of emotional and cognitive data raised concerns about security, consent, and potential misuse. He warned that if corporations or governments gained unrestricted access to users' emotional insights, it could lead to exploitation, manipulation, or discrimination. Additionally, he noted that biases in AI models could result in misinterpretations, reinforcing stereotypes or excluding certain groups from fair digital experiences establishing clear ethical guidelines, implementing robust data protection measures, and ensuring transparent user consent frameworks. He concluded by calling for a collaborative approach between technologists, policymakers, and ethicists to ensure that Web 5.0 remains ethical, inclusive, and beneficial for all.

In conclusion, he emphasized that while Web 5.0 had the potential to revolutionize digital interactions, its success would depend on responsible implementation and ethical safeguards. He reiterated the need for a balanced approach that harnesses innovation while protecting user rights, ensuring that the next phase of the internet remains inclusive, secure, and beneficial for society.



Vinayak Godse
CEO, DSCI

Workshops

Workshop by SISA

Protecting Digital Payments from AI-powered adversaries ...
A workshop on MXDR

Workshop by paloalto NETWORKS

Revolutionising Secure Access for Dynamic Workforce -
SASE with Precision AI

Workshop by KPMG

Building robust and innovative Cyber and Tech Risk capability in the context of evolving regulatory landscape

Workshop by SentinelOne

Secure the Future: Become the Next Cybersecurity Champion with SentinelOne's Autonomous Platform

Workshop by CHECK POINT

Stop Phishers in Their Tracks: Become Zero Trust &
Qishing Defense SuperHero

01 Workshop by SISA

Forensics-driven Cybersecurity

Transforming Security Operations with AI

Presented by:

1. Dharshan Shanthamurthy, Founder & CEO, SISA
2. Mahendran Chandramohan, VP-Managed Extended Detection & Response (MXDR), SISA
3. Pravin Kumar, Chief Market Information Security Officer and Data Protection Officer - NPCI

The session, led by SISA's CEO, Dharshan Shanthamurthy, focused on the evolving landscape of payment security and compliance, with a strong emphasis on Managed Extended Detection and Response (MXDR) and other allied security solutions. Mr. Shanthamurthy opened the discussion by highlighting the increasing sophistication of cyber threats targeting payment systems and the urgent need for organizations to adopt proactive security strategies. He stressed that traditional security measures were no longer sufficient and that businesses must shift towards real-time threat detection and response mechanisms. He introduced SISA's MXDR solution, explaining how it integrates AI-driven analytics, threat intelligence, and automated incident response to provide organizations with comprehensive protection against cyber threats.

Mahendra Chandramohan, Head of Product Management at SISA, delved deeper into the technical capabilities of MXDR and its allied security solutions, explaining how they empower organizations to detect, respond to, and mitigate threats in real-time. He showcased how MXDR leverages AI, machine learning, and behavioural analytics to provide continuous threat monitoring and automated risk mitigation. He also stressed that compliance and security must go hand in hand, ensuring that organizations not only detect cyber threats but also stay aligned with regulatory frameworks. Pravin Kumar, Chief Market Information Security Officer and Data Protection Officer at NPCI, added valuable insights from a regulatory and risk management perspective. He emphasized that collaboration between industry leaders, solution providers, and regulatory bodies was essential to building a robust and adaptive security framework that could withstand the rapidly evolving threat landscape.

In conclusion, the session reinforced that as cyber threats continue to grow in complexity, organizations must adopt advanced security solutions like MXDR while fostering a culture of continuous security awareness and regulatory alignment. By integrating AI-driven security intelligence, real-time monitoring, and proactive risk mitigation strategies, businesses can build a future-ready, resilient payment security infrastructure.

DSCI
FINSEC CONCLAVE 2024
JOIN US FOR THE MXDR WORKSHOP
PROTECTING DIGITAL PAYMENTS FRO
AI-POWERED ADVERSARIES
4th JUNE 2024
GBR 1
FOLLOWED BY AN INVIGORATING PANEL DISCUSSION WITH OUR EXPERTS
VINAYAK GODSE

02

Workshop by paloalto NETWORKS

Revolutionising Secure Access for Dynamic Workforce - SASE with Precision AI.

Presented by:

- Tarique Ansari, Senior Manager - Systems Engineering, Palo Alto Networks
- Ashish Chalke, SASE Solution Architect, Palo Alto Networks
- Saikumar M, SASE - Sales Specialist, Palo Alto Networks

The session was led by Tarique Ansari, Senior Manager - Systems Engineering, Palo Alto Networks, along with Ashish Chalke, SASE Solution Architect, and Saikumar M, SASE - Sales Specialist. The discussion focused on revolutionizing secure access for a dynamic workforce and addressed the increasing security challenges organizations face due to remote work, hybrid environments, and the rise of unmanaged devices. Ansari opened the session by highlighting how traditional security architectures struggle to keep up with evolving threats, emphasizing the need for a Zero Trust approach that ensures secure access across all users, devices, and locations. He introduced Palo Alto Networks' Prisma SASE (Secure Access Service Edge) as a comprehensive security solution, integrating AI-driven security, Zero Trust principles, and high-performance application access to safeguard modern workforces.

Ashish Chalke provided deeper technical insights into Prisma SASE's advanced capabilities, explaining how AI-powered data security and automated threat detection help organizations mitigate risks in real time. He emphasized that secure access isn't just about protection but also about optimizing user experience, introducing features like AI-driven application acceleration, seamless integration with cloud services, and enterprise-grade security for both managed and unmanaged devices. Saikumar M further elaborated on real-world use cases, demonstrating how organizations can simplify network security, improve visibility, and enhance compliance while ensuring employees have fast and secure access to applications. He stressed that businesses must adopt a proactive security approach to stay ahead of sophisticated cyber threats, making Prisma SASE a crucial component in modern enterprise security strategies.

In conclusion, the session reinforced the critical role of Prisma SASE in enabling secure and high-performance access for today's dynamic workforce. By leveraging AI-powered security intelligence, Zero Trust enforcement, and optimized cloud connectivity, organizations can build a future-ready security framework that ensures both protection and productivity in an evolving digital landscape.

03

Workshop by KPMG

Building robust and innovative Cyber and Tech Risk capability in the context of evolving regulatory landscape

Presented by: ·
Chandra Prakash, Partner and Co-Head Cyber Defense and Incident Response, KPMG in India
Mr. Kunal Pande, National Co-Head for Digital Risk and Cyber National leader for Digital Trust financial services sector, KPMG in India

The session was led by Chandra Prakash, Partner and Co-Head of Cyber Defense and Incident Response, KPMG in India, along with Kunal Pande, National Co-Head for Digital Risk and Cyber & National Leader for Digital Trust in the Financial Services Sector, KPMG in India. The discussion focused on building innovative and resilient cyber and technology risk capabilities to address the ever-evolving cyber threat landscape. Chandra Prakash opened the session by highlighting the growing sophistication of cyber threats and the limitations of traditional risk management approaches. He emphasized that organizations must shift from reactive security models to proactive, intelligence-driven strategies that enable early threat detection and swift response.

Kunal Pande expanded on the integration of advanced technologies such as artificial intelligence and machine learning in risk management frameworks. He explained how these technologies enhance real-time threat detection, predictive analytics, and automated incident response, reducing the impact of cyberattacks. The speakers also stressed the importance of cybersecurity governance, highlighting the role of leadership in fostering a strong security culture. They underscored the need for comprehensive security policies, regular audits, and continuous employee training programs to strengthen organizational resilience. The session also touched upon regulatory compliance and digital trust, particularly within the financial services sector, where security breaches can have severe consequences.

In conclusion, the session reinforced that organizations must embrace proactive, technology-driven risk management strategies to stay ahead of cyber threats. By integrating advanced security frameworks, fostering a culture of cyber awareness, and strengthening regulatory compliance, businesses can build a future-ready cybersecurity infrastructure capable of withstanding modern cyber challenges.

04

Workshop by SentinelOne

Secure the Future: Become the Next Cybersecurity Champion with SentinelOne's Autonomous Platform

Presented by:
Prateek Bhajanka, APJ Field CISO, SentinelOne
Shanker Sareen, Director-Marketing, SentinelOne

The session, led by Prateek Bhajanka, APJ Field CISO, SentinelOne, and Shanker Sareen, Director-Marketing, SentinelOne, focused on how AI-driven security solutions are essential in combating modern cyber threats. Bhajanka opened the discussion by highlighting the evolving sophistication of cyberattacks, where traditional security models fail to keep pace with adversaries leveraging automation and AI. He introduced SentinelOne’s Singularity XDR (Extended Detection and Response) platform, which provides real-time, autonomous threat detection and response across endpoints, cloud environments, and identity infrastructures. He emphasized that behavioral AI and machine learning-driven analytics form the core of SentinelOne’s technology, enabling organizations to proactively detect, analyze, and neutralize even the most advanced threats, such as fileless malware, ransomware, and zero-day vulnerabilities.

Shanker Sareen expanded on the technical capabilities of SentinelOne's security solutions, focusing on how Singularity XDR integrates AI-powered threat hunting, automated remediation, and forensic analysis to ensure a zero-touch security approach. He explained that SentinelOne’s Behavioral AI continuously monitors all processes, detecting even the most subtle indicators of compromise. Sareen also showcased how Automated EDR (Endpoint Detection and Response) enables organizations to contain threats in real-time, isolate compromised systems, and even roll back endpoints to their pre-infected state. By leveraging autonomous security operations, businesses can significantly reduce response times, minimize human intervention, and maintain operational continuity even in the face of sophisticated cyberattacks.

In conclusion, the session reinforced that AI-driven, autonomous cybersecurity solutions like SentinelOne’s Singularity XDR are critical in modern cyber defense. By integrating behavioral AI, real-time automation, and proactive threat response, organizations can achieve a future-ready security posture that is resilient against evolving cyber threats.

Rule 1
This is a WORKSHOP fpr LEARNING EXERCISE.
Try your best, but ASK FOR HELP!
I’ve got your back

05

Workshop by CHECK POINT

Stop Phishers in Their Tracks: Become Zero Trust & Qishing Defense SuperHero

Presented by:
Vikas Rajpal, Head of Cloud & Harmony business, India & SAARC, Check Point Software Technologies

The session, led by Vikas Rajpal, Head of Cloud & Harmony Business, India & SAARC at Check Point Software Technologies, focused on the imperative of adopting a pre-emptive cybersecurity posture in today's rapidly evolving threat landscape. Rajpal began by highlighting the increasing sophistication of cyberattacks, which necessitates that organizations move beyond reactive measures and embrace proactive security strategies. He emphasized the importance of integrating advanced threat intelligence to stay ahead of potential threats. Rajpal introduced Check Point's Infinity architecture, a consolidated cybersecurity framework designed to provide comprehensive protection across networks, cloud environments, and mobile infrastructures. This architecture leverages real-time threat intelligence and AI-driven analytics to detect and mitigate threats before they can inflict damage.

Rajpal also delved into the technical aspects of Check Point's CloudGuard and Harmony solutions, which are integral components of the Infinity architecture. CloudGuard offers advanced security for cloud assets, ensuring continuous compliance and automated threat prevention across multi-cloud deployments. It employs AI and machine learning to adapt to emerging threats, providing robust protection for dynamic cloud environments. Harmony, on the other hand, secures remote workforces by protecting endpoints, emails, and collaborative applications from sophisticated cyber threats. Rajpal highlighted that both solutions are designed to seamlessly integrate with existing infrastructures, offering scalable and efficient security without compromising performance.

In conclusion, the session underscored the necessity for organizations to transition towards a proactive cybersecurity stance. By implementing comprehensive solutions like Check Point's Infinity architecture, CloudGuard, and Harmony, businesses can effectively anticipate and neutralize threats, ensuring robust protection in an increasingly complex digital landscape.

Plenary & Special Sessions

Plenary Session 1

Charting the future of digital identities
... Examining the future of authentication and zero trust

Plenary Session 2

Building Cyber Resilience through ESG Integration

Special Session 1

Cyber Risk Quantification... Thinking risk beyond compliance

Special Session 2

Decade of Authentication ... Cryptography enabling new digitization possibilities

01

Plenary Session 1

Charting the future of digital identities

... Examining the future of authentication and zero trust

The plenary session focused on the critical issue of cybersecurity and the launch of a groundbreaking $100 million cybersecurity venture fund, designed to foster innovation in the Indian-American cybersecurity corridor. The discussion was led by Mr. Siddharth Gandhi (Co-founder, 1 Kosmos Technology Pvt. Ltd.), Mr. H. Vimadalal (CEO, 1 Kosmos Technology Pvt. Ltd.), and industry veteran Mr. Nandkumar SV (Ex-CEO, ReBIT). The speakers highlighted the alarming rise in cybercrime, the urgent need for stronger digital authentication, and the role of venture funding in accelerating cybersecurity advancements.

A key concern raised was the exponential growth of cybercrime losses, which reached $8 trillion in 2023 and are projected to rise to $10 trillion by 2025. However, the global cybersecurity market remains significantly undervalued at just $285 billion, covering less than 15% of total cybercrime losses. Interestingly, Indian Americans dominate nearly 65% of the global cybersecurity market, underscoring their influence in the industry.

In response to these challenges, Mr. Vimadalal announced the launch of an $830 crore ($100 million) cybersecurity fund aimed at supporting Indian and American startups through investments, talent acquisition, and research collaborations with leading universities. The initiative draws inspiration from the Israeli-American corridor, where 13 out of 14 recent cybersecurity acquisitions involved Israeli firms.

The discussion also emphasized the need for mentorship and industry collaboration in the cybersecurity space. Mr. Nandkumar SV stressed that while many entrepreneurs possess strong technical skills, they often lack market insights, agility, and product usability knowledge. To bridge this gap, the new fund will provide not just capital, but also strategic mentorship, ensuring startups have the guidance needed to succeed.

Another key focus area was digital identity and authentication trends. The panel discussed the limitations of SMS-based OTP authentication, citing regulatory bodies like RBI and SEBI, which are now encouraging passwordless authentication and biometric-based security. 1Kosmos positioned itself as a leader in this space, offering advanced authentication solutions powered by blockchain and biometrics.

A case study on Union Digital Bank (Philippines) demonstrated the effectiveness of 1Kosmos' biometric authentication solutions in customer onboarding and secure fund transfers. Instead of traditional OTPs, users authenticate transactions using facial recognition and biometric gestures. Additionally, a hardware-based biometric authentication key was introduced for shared workstations, enabling a seamless passwordless login experience for employees in call centers and BFSI sectors.

The session concluded with an invitation for cybersecurity professionals to invest in the fund and contribute their industry expertise. Attendees were also encouraged to visit the 1Kosmos booth for a live demonstration of their passwordless authentication solutions.

Moderator: Vinayak Godse, CEO, DSCI

Speakers:

- Nandkumar Saravade, EX - CEO, ReBIT
- Deepak Sharma, EX - CDO, Kotak Mahindra Bank
- Mathan Babu Kasilingam, CTSO & DPO, Vodafone Idea Limited
- Hemen Vimadalal, CEO, One Kosmos Technology Pvt Ltd
- Anuj Gupta, CEO, Hitachi Systems India

02

Plenary Session

Building Cyber Resilience through ESG Integration

The session, moderated by Mr. Vinayak Godse, CEO of DSCI, brought together industry leaders Ritesh Thosani (Senior Vice President, Marsh McLennan), Anurag Nalawade (Global Head - India GSIs, Blancco Technology Group), Pravin Kumar (Chief Market Information Security Officer and Data Protection Officer – NPCI), and A R Nithiyanantham (ED, IRDAI) to discuss the intersection of cybersecurity, quantum computing, and Environmental, Social, and Governance (ESG) principles. The session began with an introduction to the topic, emphasizing the growing importance of ESG in cybersecurity discussions.

The panellists included senior representatives from financial institutions, regulatory bodies, and technology firms, all contributing their insights on how cyber resilience intersects with ESG principles. The panel underscored the increasing role of governance in cybersecurity, particularly the regulatory push for enhanced oversight and accountability at the board level. The speakers noted that cybersecurity risks were no longer confined to individual organizations but had systemic implications, affecting investors, policyholders, and the broader digital ecosystem.

They emphasized that cybersecurity should not be seen as the sole responsibility of Chief Information Security Officers (CISOs) but as an integral part of business strategy at all levels.

One of the key points addressed was the evolving landscape of cyber risk management. Regulators were shifting from rule-based to principle-based governance, encouraging organizations to implement self-regulatory mechanisms. The discussion also highlighted the financial implications of cyber resilience, particularly in relation to insurance. It was revealed that insurers were becoming increasingly hesitant to cover organizations that lacked a well-defined ESG strategy. Companies demonstrating strong ESG compliance were more likely to secure better cyber insurance terms.

Technical advancements and solutions tailored for ESG and cybersecurity were key focal points of the discussion. Anurag Nalawade from Blancco Technology Group talked about secure data erasure solutions that minimize electronic waste while ensuring regulatory compliance, particularly in industries handling sensitive financial and personal data. Pravin Kumar from NPCI emphasized the necessity of quantum-resistant security measures in financial transactions, advocating for early adoption of cryptographic agility frameworks in digital payment infrastructures.

Ritesh Thosani of Marsh McLennan outlined risk assessment models that incorporate ESG factors, demonstrating how organizations can measure cybersecurity resilience while reducing their environmental footprint. A R Nithiyanantham from IRDAI provided insights into regulatory policies that encourage businesses to align their cybersecurity strategies with ESG principles, ensuring transparency, compliance, and sustainability. AG Giridharan from RBI highlighted the Reserve Bank of India's initiatives to incorporate quantum-safe security measures into the country’s financial ecosystem, ensuring resilience against next-generation cyber threats.

The session got concluded by underscoring the importance of a unified approach, where enterprises integrate ESG-driven cybersecurity solutions with quantum-safe technologies to future-proof digital ecosystems while meeting regulatory and sustainability objectives.

Speakers:

· Ritesh Thosani, Senior Vice President, Marsh McLennan
· Vinayak Godse, CEO, DSCI
· Anurag Nalawade, Global Head - India GSIs, Blancco Technology Group
· Pravin Kumar, Chief Market Information Security Officer and Data Protection Officer – NPCI
· A R Nithiyanantham, ED, IRDAI
· A G Giridharan, GM, RBI

DSCI
FINSEC CONCLAVE 2024
Plenary Session
Building Cyber Resilience through ESG Integration
A Regulator Investor dialogue
PICUS

03 Special Session

Cyber Risk Quantification... Thinking risk beyond compliance

The session focused on Cyber Risk Quantification (CRQ) and its growing significance in cybersecurity management. It was moderated by Vinayak Godse, CEO of DSCI. The speakers introduced FAIR (Factor Analysis of Information Risk), a methodology that helped organizations measure cybersecurity risks in financial terms. They emphasized the importance of moving beyond traditional risk assessments, which often relied on vague scoring methods and compliance checklists. Instead, CRQ provided measurable financial impact analysis, making it easier for security leaders to justify cybersecurity investments to boards, CFOs, and regulators. Decision-makers were more likely to approve security budgets when risks were presented in dollar-value reductions rather than technical risk scores.

The FAIR model translated cybersecurity threats into quantifiable financial risks, allowing organizations to estimate the probability of breaches and potential financial losses. Large corporations, including Netflix and major financial institutions, used FAIR to predict security risks and prioritize security investments.

The speakers highlighted how FAIR enabled CISOs to communicate cybersecurity risks more effectively, ensuring leadership understood the financial implications rather than being overwhelmed by technical jargon. Instead of requesting a security tool with a broad justification, a CISO could have framed it in financial terms. For example, “A $300,000 investment in EDR would reduce cyber risk by $6 million.” This shift in approach aligned cybersecurity with business objectives and regulatory expectations.

CRQ also played a crucial role in business decision-making, helping organizations prioritize security investments based on their return on investment (ROI). For example, a FAIR analysis determined whether a $1 million cybersecurity investment was better allocated to Endpoint Detection & Response (EDR) or Data Loss Prevention (DLP). This enabled CISOs to negotiate security budgets with a data-driven approach rather than relying on fear-based justifications.

The session introduced new FAIR-based risk management models, including FAIR-CAM (Control Analytics Model) for measuring security control effectiveness, FAIR-MAM (Materiality Analysis Model) for estimating breach costs and cyber insurance needs, and FAIR-TAM (Third-Party Analysis Model) for evaluating risks from third-party vendors. These models helped organizations improve their cybersecurity posture through structured, data-driven insights.

FAIR gained global recognition, with the country of Jordan officially adopting it as its national cybersecurity standard. Many Fortune 1000 companies integrated FAIR into their risk management strategies, reinforcing its credibility. Since the methodology was open-source, organizations worldwide could leverage it to enhance risk assessments and cybersecurity governance.

To further expand expertise in Cyber Risk Quantification, a new FAIR certification program was launched in collaboration with DSCI. This initiative helped security teams, CISOs, and financial analysts develop skills in cyber risk measurement, ensuring they could apply FAIR methodologies effectively.

Recognizing the need for localized risk quantification in India, the speakers highlighted plans to develop India-specific cybersecurity risk models. Industry collaboration was crucial in refining these frameworks, ensuring they aligned with Indian market conditions and regulatory expectations.

The session concluded with a discussion on the future of cyber risk management, emphasizing the growing regulatory pressure on organizations to report breaches and risk exposure in financial terms. The shift from reactive cybersecurity responses to proactive risk planning became essential, and Cyber Risk Quantification (CRQ) was expected to become a mandatory component of financial and regulatory reporting.

Speakers:

- Vinayak Godse, CEO, DSCI

- Rahul Tyagi, Co-founder, Safe Security and Technical Advisor, FAIR Institute

- Gowdhaman Jothilingam, Global CISO, Head of Information Technology, Latentview Analytics

Cyber Risk Quantification
Thinking risk beyond compliance
GBR
Vinayak Godse
CEO
DSCI
Rahul Tyagi
Co-founder, Safe Security and
Gowdhaman Jothilingam
Global CISO, Head of Information
Technology
DSCI

04

Special Session

Decade of Authentication … Cryptography enabling new digitization possibilities

The session explored how cryptography had been redefining authentication in fintech, addressing key challenges such as identity fraud, digital trust, and post-quantum cryptography (PQC). Experts from academia, cybersecurity, and digital certification authorities shared insights into the evolution of authentication—from password-based security to multi-factor authentication (MFA), digital signatures, and cryptographic verification—all critical for securing financial transactions in an increasingly complex threat landscape.

“Digital trust was no longer just about verifying people; fintech firms now had to authenticate machines and software to prevent fraud,” said Ajit Hatti, Founder of PureID. The discussion on biometrics vs. cryptographic authentication was a key highlight, with Dr. Ashok Kumar Nanda, Associate Professor at BV Raju Institute of Technology, emphasized that “Unlike biometric data, cryptographic keys could be revoked and replaced, making them a stronger security choice.” The consensus among panellists was that a hybrid model—biometrics for user convenience and cryptography for security—was the ideal approach.

Identity fraud remained a major concern, with banks facing significantly higher financial losses per breach than fintech companies—some incidents costing up to $500,000 per breach. To address this, blockchain-based authentication was emerging as a reliable solution, offering tamper-proof identity verification mechanisms.

The panel also discussed the growing quantum computing threat to cryptographic security. “Quantum computers could potentially break widely used encryption methods like RSA and ECC, rendering current security models obsolete,” opined Manoj M Prabhakaran, Professor at IIT Bombay. In anticipation of this risk, NIST had already selected four PQC algorithms, and panellists urged financial institutions to start assessing their cryptographic assets and transitioning to quantum-safe encryption before it became an urgent necessity.

Balancing security and usability was another critical themes. Strict authentication protocols in digital banking, such as India's multi-layered security frameworks, had often led to friction in customer experience. “Security should never come at the expense of usability—fintech firms needed to strike the right balance,” the panel stressed.

The role of Certificate Authorities (CAs) in digital trust was also examined, particularly in the context of geopolitical tensions like the Russia-Ukraine conflict, which had affected CA trust levels and access restrictions. The panel debated whether decentralizing CAs could offer a more resilient and politically neutral approach to digital identity verification.

A significant concern raised was India's cybersecurity talent gap. “With most students opting for AI/ML over cybersecurity, the shortage of cryptography professionals was becoming a serious challenge,” emphasized Dr. Nanda. The session emphasized the need for stronger industry-academia collaboration and greater investment in cryptographic research and training programs to bridge this gap and build local expertise.

The panel also stressed upon cryptographic security in fintech - expected to evolve with innovations like Secure Multi-Party Computation (MPC) and Zero-Knowledge Proofs (ZKP), which aimed to enhance privacy, security, and efficiency in financial transactions. However, for widespread adoption, increased funding, standardization, and a skilled workforce were necessary.
Conclusion: Cryptography remained at the heart of secure digital finance, but with growing identity fraud, usability concerns, and quantum threats, fintech firms, banks, and regulators needed to collaborate to create a future-proof authentication ecosystem.

Speakers:
Ajit Hatti, Founder, PureID
Manoj M Prabhakaran, Computer Science and Engineering, IIT Bombay
Dr. Ashok Kumar Nanda, Associate Professor, BV Raju Institute of Technology

Industry Keynotes

Platformization in Cybersecurity - Power of Integrated AI Platforms

Speaker:
Tarique Ansari, Senior Manager - Systems Engineering, Palo Alto Networks

Charting the future of identities

Speaker:
Siddharth Gandhi, COO - APAC, One Kosmos Technology Pvt Ltd Hemen Vimadalal, CEO, One Kosmos Technology Pvt Ltd

Ensuring Trust in the Digital Economy ... Thales' Approach to Protecting Applications, Data, and Identities

Speaker:
Nishant Rana, Senior Solution Sales, Thales Group

Data Sanitization: The Unsung Hero of Cybersecurity

Speaker:
Anurag Nalawade, Global Head - India GSIs, Blancco Technology Group

Industry Keynotes

Cybersecurity Redefined: AI vs AI in the Battle against Breaches

Speaker:
Kushagra Kaushik, Regional Sales Director - South Enterprise, Sentinelone

Security Operations of the Future

Speaker:
Derek Whigham, Chief Product Owner, Group COO, Lloyds Banking Group

CISO Evolution in BFSI ... Strategic Influence and Leadership in Navigating Organizational Change

Speaker:
Vishal Salvi, Chief Executive Officer - Quick Heal Technologies Limited

Data Sanitization for FINSEC

Speaker:
Ashwin Mittal, Regional Head at OPSWAT

Industry Keynotes

The Intersection of AI Powered , Cloud Delivered Cyber Security

Speaker:

- Alok Pradhan, Director & Head - Commercial Business, India & SAARC, Check Point Software Technologies
- Rajesh Pillai, Senior Technical Architect, NTT DATA

Unveiling AI powered DSPM for Data Security Everywhere

Speaker:
Aman Thareja, Managing Director, Forcepoint India

Continuously Validated Security Operations Leveraging BAS to shift from Activities to Outcomes

Speaker:
Harmeet Kalra, Regional Sales Director - India & SAARC, PICUS Security

Special Keynote: Future of Cyber Security in Banking

Speaker:
Sameer Ratolikar, Senior Executive Vice President & CISO, HDFC Bank

Track Sessions - Day 1

Track Session 1

Generative AI to Augment Cyber Defense ... Experiments & use cases of Gen AI for security operations

Product Security and Financial Product

Track Session 2

New in Ransomware ... Specifically, from Financial Sector Perspective

Track Session 3

B2B Transaction & DPDP Act ... Compliance Challenges and probable approach

Track Session 4

Emerging Technologies and Transaction Security 2027

Track Session 5

Navigating the Future of Mobile App Security

Track Sessions - Day 2

Track Session 6

Time for OTP and Password Less Authentication is now

BFSI Cyber Security Roles

Track Session 7

Board and Security Governance

Track Session 8

Compliance: Automation is the way

Track Session 9

Fraud Management and Customer Digital Journey

Track Session 10

DevSecPrivaOps

FINSEC - DSCI Innovation Box 2024

The DSCI Innovation Box remained a key highlight within the prestigious DSCI Excellence Awards 2024, dedicated to celebrating startup excellence and innovation, now in its 14th year. Specifically tailored for FINSEC 2024, this marked the 15th edition of the Innovation Box, spotlighting cutting-edge cybersecurity product companies addressing security challenges in the Financial Sector Security landscape.

This edition aimed to honor and reward individuals and organizations that demonstrated strategic, proactive, and innovative FinTech security solutions, significantly contributing to risk mitigation, resilience-building, and trust enhancement in the BFSI & FinTech sectors.

The DSCI Innovation Box took place during the two-day DSCI Financial Security Conclave 2024, which was held in-person at Westin, Mumbai, on June 4-5, 2024. The event provided deep insights into the security and privacy concerns emerging from the rapid digitization of the financial sector, bringing together industry experts, policymakers, developers, and innovators to share best practices and explore new opportunities for strengthening cybersecurity in BFSI.

Startups underwent a rigorous selection process, meeting specific eligibility criteria before advancing to the final evaluation stage. Shortlisted participants had the unique opportunity to pitch their products on June 5, 2024, before a distinguished jury and a live audience. The judging process combined jury scores (70%) and audience polling (30%), ensuring a fair and transparent evaluation. Winners and runners-up were recognized for their groundbreaking contributions to cybersecurity in financial services.

Winner of the
DSCI Innovation Box FINSEC Edition
Most Innovative Product – Zeron

1st Runner Up
WhizHack Technologies

2nd Runner Up
AppSentinels

Event Speakers

A R Nithiyanantham
ED, IRDAI

Adv. Puneet Bhasin
Founder
Cyberjure Legal Consulting

Air Commodore Nitin Sathe
Veteran

Akhil Kumar
Senior Vice President
Mizuho Global Services
India Private Limited

Alok Pradhan
Director & Head,
Commercial Business, India
& SAARC, Check Point
Software Technologies

Aman Thareja
Managing Director,
Forcepoint India

Aniket Karekar
Director, PayU

Animesh Chauhan
District Manager
Financial Services,
Palo Alto Networks

Anitha Ravindran
Director, Data Management
and Privacy, Standard
Chartered Bank

Ankit Goenka
Senior Vice President &
Head Customer Experience,
Bajaj Allianz General Insurance

Anooradha Goel
Senior Manager,
DSP Mutual Fund

Anuj Gupta
CEO, Hitachi Systems India

Anurag Nalawade
Global Head - India GSIs,
Blancco Technology Group

Arindam Roy
Country Director
India and South Asia,
SANS Institute

Ashish Chalke
SASE Solution Architect,
Palo Alto Networks

Ashwin Mittal
Regional Head
at OPSWAT

Basil Dange
CISO, Aditya Birla Capital

Bhaskar Rao
CISO, Bharat Co-op
Bank (Mumbai) Ltd

Bishakha Bhattacharya
Head - Public Policy, AWS

Chandra Prakash
Partner and Co-Head
Cyber Defense and Incident
Response, KPMG in India

Deepak Sharma
EX - CDO,
Kotak Mahindra Bank

Deepti George
Deputy ED and Head
of Strategy, Dvara Research

Derek Whigham
Chief Product Owner,
Group COO,
Lloyds Banking Group

Deval Mazmudar
Cybersecurity Advisor,
TJSB Bank

Dharshan Shanthamurthy
Founder & CEO, SISA

Event Speakers

Dinesh Purushothaman
Head - Digital Forensics & Corporate Investigations, GMR Group

Divya K
Senior Manager (IT), Indian Public Sector Bank

Dr. Jay Prakash
Co-Founder & CEO, Silence Laboratories

Dr. Rajarshi Pal
Assistant Professor, IDRBT

Dr. Sumit Kr Yadav
Dy. Director Income Tax, CBDT

Fal Ghancha
Head Technology and CISO, Jio BlackRock AMC

Gireesh Kumar N
Quantum Technology Consultant, Independent Consultant

Gowdhaman Jothilingam
Global CISO, Head of Information Technology, Latentview Analytics

Gowree Gokhale
Leader, Nishith Desai Associates

Gunjan Patel
Director & Head Philanthropies, Microsoft India

Hakimuddin Wadlawala
Founder of Aquila

Harish Soni
Practice Leader Cyber Resiliency, Kyndryl India

Harmeet Kalra
Regional Sales Director - India & SAARC, PICUS Security

Hemen Vimadalal
CEO, One Kosmos Technology Pvt Ltd

Jeevan Joseph Sakhre
Global Head - IAM, Barclays

Kalpesh Doshi
Group CISO, HDFC Life

Kinjal Shah
Chief Technology Officer, Yes Securities Ltd.

Kunal Pande
National Co-Head for Digital Risk and Cyber National leader for Digital Trust financial services sector, KPMG in India

Kushagra Kaushik
Regional Sales Director - South Enterprise, Sentinelone

Mahendran Chandramohan
VP-Managed Extended Detection & Response (MXDR), SISA

Makesh Chandramohan
CISO, Aditya Birla Capital Limited

Mandar Kulkarni
National Security Officer, Microsoft India

Manish Mimani
Founder & CEO, Protectt.ai Labs Pvt. Ltd.

Manisha Singh
Head of IF&IS Automation & Integration, Allianz Technology

Manoj Kumar Shrivastava
CISO, Future Generali India Insurance Company Limited

Event Speakers

Mathan Babu Kasilingam
CTSO & DPO,
Vodafone Idea Limited

Mayur Vijay Desai
Head of station -
Global Security, Invesco

Mohan Jindal
CEO, Chipspirit

Mrutyunjay Mahapatra
Independent Consultant

Munish Gupta
President & Global Cyber
Security Advisory Head,
Inspira Enterprise Private Limited

Nandkumar Saravade
EX - CEO, ReBIT

Nasser Prakash
Head of Risk & Infosec,
Lloyds Technology Centre

Navaneethan M
Sr. Cybersecurity Expert

Navaneetharangan Chakravarthy
Executive Director,
JPMorgan Chase & Co.

Navin Raju Roselin
CISO, CredAble

Nishant Rana
Senior Solution Sales,
Thales Group

Pavithra Santhanam Iyengar
Group Data Privacy Manager,
Emirates NBD Bank

Pavithra Shwetha
Executive Director,
Wells Fargo Technology

Pawan Chawla
Industry Evangelist,
TATA AIA Life Insurance
Company Ltd.

Prasanna Ravi
RESEARCH FELLOW, NANYANG
TECHNOLOGICAL UNIVERSITY,
SINGAPORE

Prateek Bhajanka
APJ Field CISO,
SentinelOne

Pravin Kumar
Chief Market Information
Security Officer and Data
Protection Officer - NPCI

Rahul Tyagi
Co-founder,
Safe Security and Technical
Advisor, FAIR Institute

Raj Rao
Co-Founder and
Chief Product Officer,
Aldefi

Rajesh Pillai
Senior Technical Architect,
NTT DATA

Rajsri Rengan
Head of Product
Development, EdgeVerve,
an Infosys subsidiary

Rakesh Maheshwari
Former Sr. Director and
Group Coordinator, MeitY

Ram Shanmugam
Co-founder and CEO,
Aldefi

Ramesh Gurram
CISO, MCX India

Ritesh Thosani
Senior Vice President,
Marsh McLennan

Event Speakers

Romharsh Razdan
Director, KPMG in India

Ruma Dey
DMD GCO

Rumit Shah
Director, JISA Softech Pvt. Ltd.

Sabyasachi Dhal
VP, Wells Fargo

Saikumar M
SASE - Sales Specialist, Palo Alto Networks

Sameer Ratolikar
Senior Executive Vice President & CISO, HDFC Bank

Samir Aksekar
Cybersecurity Director, EQT

Samuel Sathyajith
Senior Vice President - Enterprise Sales, Quick Heal Technologies Limited

Sandeep Mehra
Chief Vigilance Officer, Yes Bank

Satyanandan Atyam
Chief Risk Officer, Tata AIG General Insurance Co. Ltd.

Senthil Vellaichamy
Senior Director of Engineering at PayPal

Shanker Ramrakhiani
CISO, IIFL Group

Shanker Sareen
Director-Marketing, SentinelOne

Shashank Shekhar
Co-Founder, Future Crime Reserach Foundation (FCRF)

Shilpa Konkar
DPO and General Manager, SBI

Shinto Joseph

Shivani Arni
Deputy CISO, Mahindra Group

Shri. Shaji K V
Chairman, NABARD

Shubham Majumder

Siddharth Gandhi
COO - APAC, One Kosmo Technology Pvt Ltd

Srihari Kotni
Sr. Director - Chief Information Security Officer, Pine labs

Steve Dsouza
Vice President - Enterprise Risk Management & CRO, ICICI Lombard

Tarique Ansari
Senior Manager - Systems Engineering, Palo Alto Networks

Tejasvi Addagada
Senior Vice President, Head - Enterprise Data Management at HDFC bank

Venugopal Parameswara
CISO, CSB BANK

Event Speakers

Vikas Murli Kyatsandra

Principal Engineer, Solutions Engineering, Arm

Vikas Rajpal

Head of Cloud & Harmony business, India & SAARC, Check Point Software Technologie

Vinay Kesari

Director - Operations and Strategy, Setu AA

Vinayak Godse

CEO, DSCI

Vinayak Srimal

Senior VP, Kotak Mahindra Bank

Vishal Salvi

CEO, Quick Heal Technologies Limited

Yash Vartak

Director, Cyber Security Partnerships - (Channels & Alliances) - Asia Pacific & Japan, Mastercar

Zubin Tafti

Managing Director, PricewaterhouseCoopers Private Limited

Sponsors, Partners & Exhibitors

POWERED BY

paloalto NETWORKS

EXCLUSIVE PARTNERS

1KOSMOS | HITACHI Inspire the Next

SentinelOne

THALES Building a future we can all trust | TECHNOBIND

PLATINUM SPONSORS

blancco

LLOYDS BANKING GROUP

OPSWAT. | HITACHI Inspire the Next

SEQRITE

GOLD SPONSORS

Forcepoint

PICUS

SILVER SPONSOR

secpod

Sponsors, Partners & Exhibitors

PARTNERS

appsealing

AQUILA I

ProTechmanize

CHECK POINT

NTT DATA

CYBERARK
The Identity Security Company

FORTRA

KPMG

threatcop

KRATIKAL

Protectt.ai

SANS | GIAC CERTIFICATIONS

SISA
Forensics-driven Cybersecurity

EXHIBITORS

eCAPS

riskrecon by | inspira

KLASSIFY
Discover . Classify . Protect

NETWORK INTELLIGENCE
The Digital Security Company

Pearson VUE

PrivaSapien
Evolution for the Privacy & AI Era

stellar

vehere

GIVEAWAY PARTNERS

True Elements ®

CAMPA
THE GREAT INDIAN TASTE

natch
delicious. naturally.

paper KAITE
www.paperkaite.com

CHIYA LEAF

Sponsors, Partners & Exhibitors

NCoE Innovation Arcade

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

Watch out for the Start-ups at NCoE Innovation Arcade

AppSentinels

ATTACKFENCE
Autonomous Cyber Defense Platform

CryptoBind®
By JISA Softech

privEzi

SECONIZE

TechBridge
Making the World Smarter

haltdos

innspark

ATHENIAN TECH

3rd Eye
Techno Solutions Pvt. Ltd.

DOMDOG
Page Security & Privacy Platform

MATISOFT CYBER SECURITY LABS
INTELLIGENTLY PROTECTING

Optimized Cyber Security Solutions

PROGIST®

Saptang Labs

SEQURETEK
SIMPLIFY SECURITY

DEEP ALGORITHMS
Fostering AI, Connecting Minds

DocChain.io
by Print2Block

THANK YOU

From Team DSCI for being a part of
the 6th edition of FINSEC CONCLAVE 2024
and making it a huge success.

DATA SECURITY COUNCIL OF INDIA (DSCI)
NASSCOM CAMPUS, 3rd Floor, Plot. No. 7-10,
Sector 126, Noida, UP - 201303

For any queries contact:
P: 0120-4990262 | E: events@dsci.in | W: www.dsci.in