DSCI and SANS Institute launch the Indian Cyber Security Skilling Landscape Report 2025-26

New Delhi, 1st May 2026: The Data Security Council of India (DSCI) and SANS Institute have jointly launched the 'Indian Cyber Security Skilling Landscape Report', which examines the state of cyber security skilling and workforce readiness in the country. The report was officially launched by Mr. Vinayak Godse, CEO, DSCI, and Mr. James Lyne, CEO, SANS Institute. The partnership was further strengthened through the signing of a Memorandum of Understanding (MoU) for cybersecurity training, awareness and talent development initiatives for Government of India agencies.

The study examines the demand for the cyber security workforce in the country, driven by a structural shift in digital architecture as enterprises move from static networks to distributed environments such as cloud-native platforms, API-driven systems, and Artificial Intelligence (AI). It further analyses the impact of these shifts on roles and skill requirements and assesses critical gaps between digital transformation and workforce readiness.

Report Key Highlights

Organizational operations are adapting to technologies such as AI, leading to a reduction in entry-level job roles. While automation and advanced tooling are decreasing reliance on operational positions, advanced and decision-critical roles continue to remain persistently understaffed.

Talent Availability and Hiring Struggles

- 73% of enterprises and 68% of providers report a limited availability of skilled cyber security candidates.
- 84% of organizations report that it takes between one to six months to fill cyber security roles.

Capability and Hands-On Skill Gaps

- 63% of enterprises and 59% of providers report limited hands-on practical skills among job candidates.

- 58% of enterprises and 60% of providers lack professionals with cross-domain capability, reflecting difficulty in finding talent that can integrate cloud, applications, and identity systems.

The AI and Emerging Technology Impact

- 83% of organizations identify AI and GenAI security skills as a critical requirement.
- 78% of organizations report high demand specifically for AI Security Engineers.
- 73% of cyber security providers report growing client demand for AI and GenAI security services.
- 62% of surveyed enterprises report running active AI and GenAI projects within their digital environments, thereby expanding the attack surface.

Specific Roles that are Hardest to Hire

- 49% of providers and 40% of enterprises report difficulty hiring Security Architects.
- 41% of providers and 23% of enterprises report difficulty hiring OT/ICS (Operational Technology / Industrial Control Systems) security specialists.
- 35% of organizations report significant difficulty recruiting professionals capable of conducting advanced threat intelligence.

Attrition and Retention

- 70% of providers and 42% of enterprises report losing talent primarily because employees move to other organizations for higher compensation.
- 32% of providers and 8% of enterprises identify insufficient upskilling opportunities as a driver of talent attrition.

Sharing his perspective, **Mr. Vinayak Godse, CEO, DSCI** said, "*The world today is marked by rapid evolution in both threats and technologies amid rising geopolitical tensions and AI led interventions with cyber security emerging as a critical area requiring specific talent. Supported by the SANS Institute, this report highlights a key dimension of the current cyber security skills landscape in the country, set against growing volatility in recruiter expectations and trends that must keep pace with the unprecedented speed of technological advancements.*"

At the report launch, **Mr. James Lyne, CEO SANS** said, *"India's cyber security challenge is no longer about headcount; it is about skills and depth. This report makes clear that the gap between enterprise readiness and attacker trends is widening at the moment due to rapid technological developments and it matters the most. SANS is committed to closing that gap through world-class training and certifications that*

produce professionals who are ready to operate from day one. Our partnership with DSCI is a meaningful step in the right direction."

Left to right: Hemang Vivek Prakhar, Assistant Manager - Cyber Security Technology; Atul Kumar, Director, DSCI; Tulika Pandey, Scientist 'G' and Group Coordinator (R&D in Cybersecurity), Ministry of Electronics & Information Technology, Government of India; Vinayak Godse, CEO, DSCI; James Lyne, CEO, SANS, Suresh Mustapha, Managing Director, APAC & LATAM; Arindam Roy, Country Director, South Asia, SANS

Vinayak Godse, CEO, DSCI and James Lyne, CEO, SANS with Atul Kumar, Director, DSCI; Suresh Mustapha, Managing Director, APAC & LATAM and Arindam Roy, Country Director, South Asia, SANS at the MoU exchange

About Data Security Council of India

The Data Security Council of India (DSCI), a Nasscom initiative, is a premier think tank on data protection, cyber security and emerging tech in India. DSCI engages with governments, regulators, industry, and academia to build a secure and trusted cyberspace through policy advocacy, thought leadership, and capacity-building initiatives.

About SANS

Founded in 1989, the SANS Institute is the world's leading provider of cyber security training and certification for professionals across government and industry. Its expert instructors deliver over 85 courses through in person, virtual, and OnDemand formats. In India, more than 6,000 courses have been completed and over 3,000 certifications earned. Its affiliate, GIAC, offers over 50 hands on technical certifications, while the SANS Technology Institute provides accredited degree and certificate programs in cyber security. SANS also supports the global InfoSec community through research, webcasts, podcasts, newsletters, and the Internet Storm Center, fostering collaboration among security practitioners worldwide.