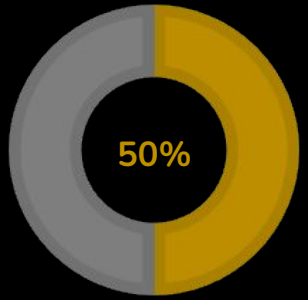
Data, AI and Cybersecurity Oversight

Together,
we're redefining data and AI guardrails in sport

TIAKI

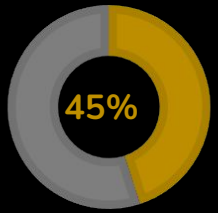
Big Tech continue to invest to win the 'AI arms race'

Data-driven, AI augmented business models hitting mainstream within 18 months

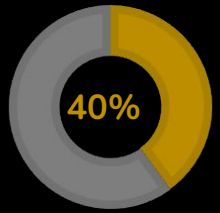


% of Nvidia revenues are with 4 Big Tech brands.
AI compute power at scale [1]

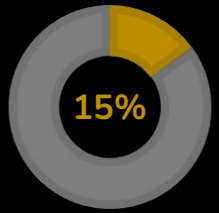
Big Tech % CAPEX spend on Nvidia chips Q3'24 [1]



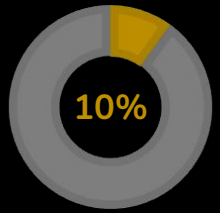
Microsoft



Meta



Alphabet



AWS

[1] Futurum Group - The relationship between Mega-Tech Capex and NVIDIA

TIAKI

Cloud, Data and AI impact all areas of the sports ecosystem

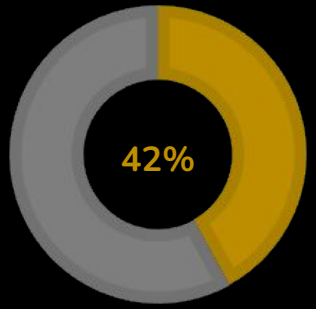
Competitive pressure is rapidly increasing

- ★ New digital revenue streams
- ★ **Hyper-personalised digital fan engagements**
- ★ Real-time, immersive streaming experiences
- ★ **Connected, digitally interactive smart venues**
- ★ Sport is now a digital, personalised entertainment business
- ★ Gen Z and Alpha sports fans expect instant, ‘sound-bite’ sporting experiences.

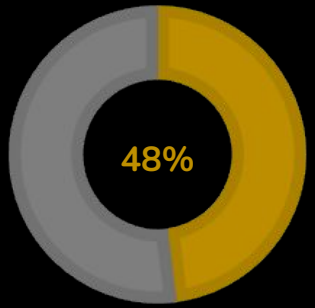
TIAKI

Oversight has become a complex issue

Governance and guard rails to power high quality data-at-scale for Gen AI projects is a challenge



% of organisations need help developing policies, governance and guard rails **for data, AI and cybersecurity to ensure regulatory compliance** [2]



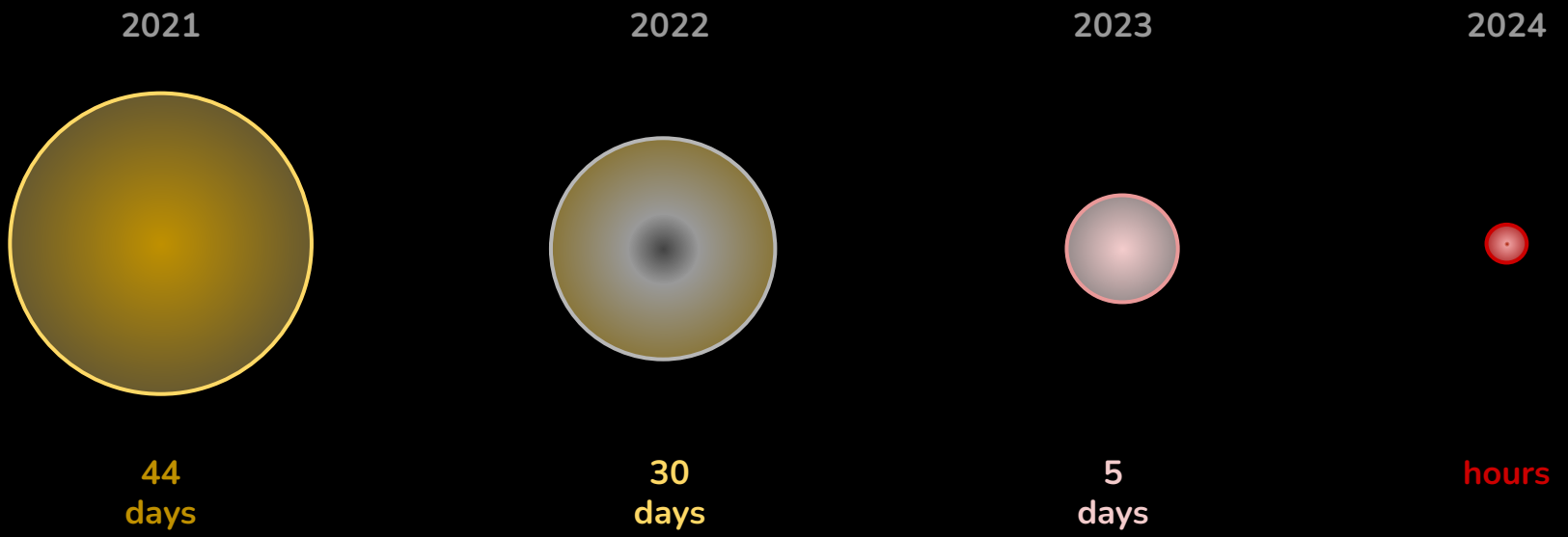
of CxOs admit their enterprises **lack enough high-quality data to operationalize their generative AI initiatives** [2]

TIAKI

[2] Data Essentials with Generative AI | Accenture

The AI-powered cybercriminal has crossed the start line:

Attacks are happening faster than organizations can respond

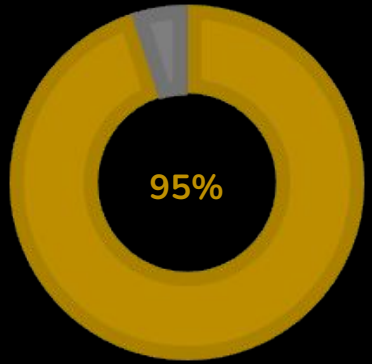


Typical number of days from ‘compromise to data breach’[3] :

[3] PaloAlto Unit 42 Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface (paloaltonetworks.com)

CEO priorities may need revision

To improve oversight focus and align with 2025 cybersecurity risk realities



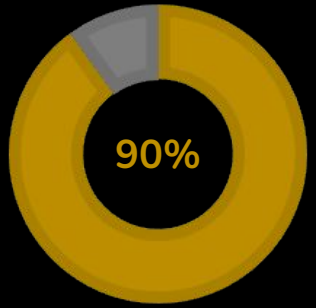
% of CEOs wrongly believe that compliance is the key driver of their Cybersecurity Strategy.
Misaligned priorities are common [4]

[4] David Andrew: The SASE-powered C-suite

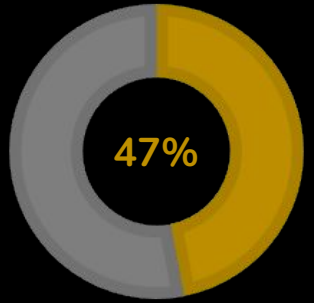
TIAKI

GenAI tools have become pervasive in the work environment

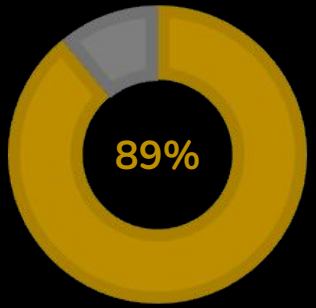
Often without adequate guardrails and governance, which increases the risk of a serious data breach



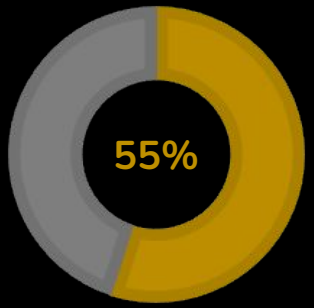
of CEOs are worried their organisation will be a victim to a catastrophic cyber attack by 2025. **CEO concerns are increasing** [5]



of enterprises are concerned about **AI-generated code risks** [6]



of organizations regard GenAI tools as a risk .... yet **95% are already using them**, and **23% admit to no monitoring of their usage** [7]



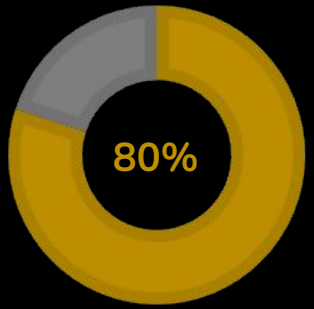
of employees have used **unapproved GenAI tools** at work and **40% have used banned GenAI tools at work** [8]

[5] David Andrew: The SASE-powered C-suite
[6] PaloAlto Unit 42 Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface (paloaltonetworks.com)
[7] Accenture, The Cyber-Resilient CEO, dated Nov'23
[8] Salesforce Survey, More than Half of Generative AI Adopters Use Unapproved Tools at Work dated 15th Nov'23

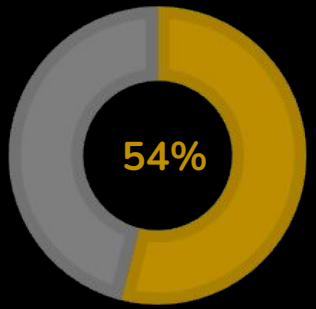
TIAKI

Cloud is the dominant attack vector for the cybercriminals

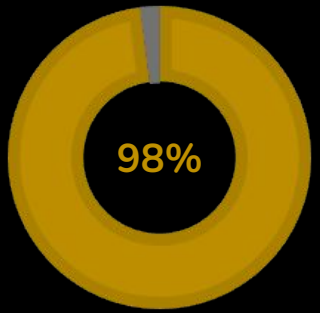
Cloud assets and supply chain risk are emerging as a critical business exposures in the sports value chain



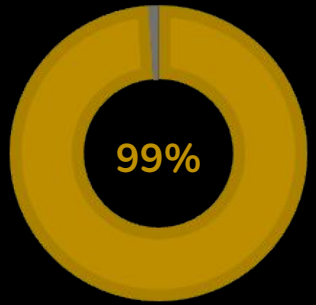
of data breaches are occurring on cloud assets in 2024.
Cloud-native vulnerabilities are a major concern [9]



of respondents highlight complexity & fragmentation of cloud environments as a major security challenge.
Fragmentation is a major issue [9]



of enterprises are storing sensitive data in multiple locations: onprem, public cloud, SaaS apps with local storage, private cloud & end points.
Spiralling security challenges [9]



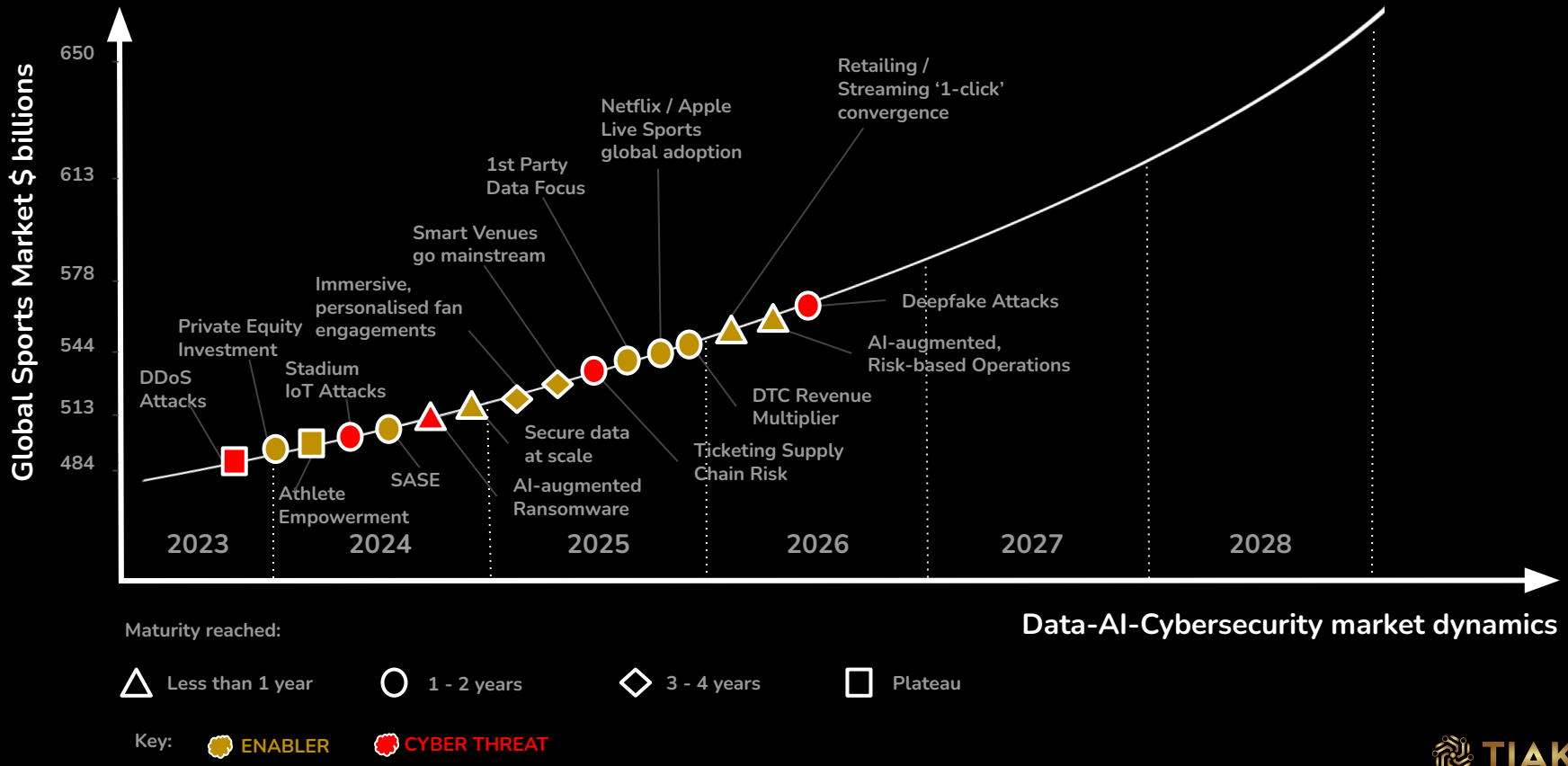
of Global 2000 companies are directly connected to a breached vendor in their supply chain.
Similar exposures are likely for sporting entities [10]

[9] PaloAlto Unit 42 Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface (paloaltonetworks.com)
[10] 99% of Global 2000 Companies Directly Connected to a Supply Chain Breach - SecurityScorecard

TIAKI

Market dynamics impacting global sports market growth

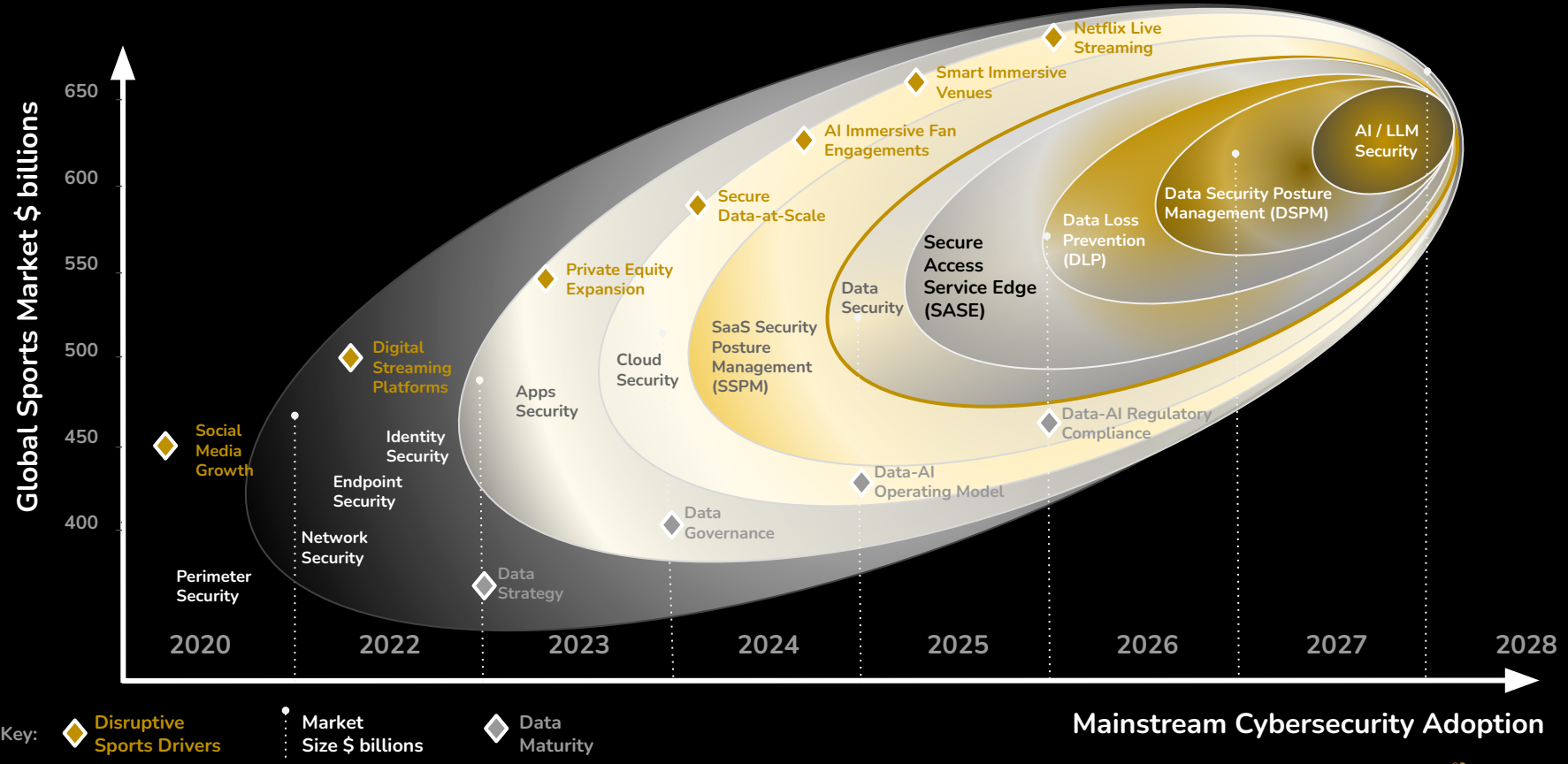
Secure data & AI maturity will be fundamental to profitable growth



Source: TIAKI

Data, AI and Cybersecurity Oversight become critical in sport in 2025

Data & AI LLM security become non-negotiable for sports leaders



Source: TIAKI

Identifying and reducing risk with Governance and Guard Rails

To empower Sports Governing Bodies to adopt data, AI and cybersecurity best practice

Benefits:

- ★ Mitigate Risks & Safeguard Reputation: protect sensitive player data, fan information, and club assets from cyber threats, data breaches, and reputational damage
- ★ **Enhance Fan Engagement: deliver personalized experiences, innovative services, and deeper fan connections through data-driven insights and AI-powered platforms**
- ★ Optimize Operations: streamline operations through efficient data utilization, automation and AI-augmentation
- ★ **Ensure Compliance & Trust: adhere to stringent data privacy regulations (e.g., GDPR, DORA) and build trust with fans, players, and stakeholders through transparent and ethical data practices**
- ★ Our guidance provides 'peace of mind' to your governing body leadership team.

TIAKI

Data, AI and Cybersecurity Oversight Framework for Governing Bodies

Current State Maturity and Compliance, Target State, Business Value Realization, Uses Cases & your Transformation Journey

I - Data, AI & Cybersecurity Current State Maturity & Benchmarking

- ★ Data & asset inventory and classification
- ★ Assess data quality, data integrity and data security across the digital ecosystem & networks
- ★ Identify critical data flows and dependencies
- ★ AI asset inventory and existing governance frameworks
- ★ Cybersecurity risk assessment including SASE review
- ★ Regulatory compliance review & identification of potential compliance gaps

II - Data, AI & Cybersecurity Target State Frameworks & Transformation Path

- ★ Co-develop data governance, policies, standards and procedures
- ★ Define robust data access controls and data retention policies for athlete and fan information
- ★ Establish data quality management processes
- ★ Co-develop AI governance framework
- ★ Define AI ethics guidelines and principles
- ★ Establish rigorous AI model development, testing and deployment processes
- ★ Co-develop risk management and monitoring procedures to mitigate risk & bias and ensure responsible AI-usage
- ★ Co-develop cybersecurity governance frameworks based on SASE best practice
- ★ Establish C-suite communication, training and governance briefs

III - Data, AI & Cybersecurity Monitoring, Reporting & Continuous Improvement

- ★ Business alignment to Oversight Frameworks
- ★ Business prioritization input to Data, AI & Cybersecurity Governance
- ★ Co-develop framework for continuous improvement of data, AI & cybersecurity best practice to respond to emerging threats
- ★ C-suite briefing on key findings, recommendations, resiliency, benchmarking results, areas for investment prioritisation & future innovation

TIAKI

Our Consulting Approach

Connecting the dots across the entire digital sports industry value chain

- We offer flexible engagement models
- **Our consultants work side by side with the governing body team to co-develop recommended governance and guard rails, covering data, AI and cybersecurity, for their specific sporting code**
- As your trusted advisors, we seek to fully understand your business objectives and the unique risks that you're facing every day
- **This can help to significantly improve overall data, AI and cybersecurity maturity across all franchises within the specific sporting code that the governing body has responsibility for**
- Our guidance provides 'peace of mind' to your governing body leadership team.

TIAKI

TIAKI bring deep expertise from our personal journeys at .....

.... which shapes our digital, data, AI and cybersecurity consulting insights in the global sports ecosystem.

TIAKI

About the Author:

David Andrew
Founder & Managing Partner
www.tiaki.ai
david.andrew@tiaki.ai

TIAKI

David is the Founder & Managing Partner at TIAKI, where he collaborates with bold and determined leaders in the sports ecosystem to define their data, AI and cybersecurity strategies to deliver sustainable value.

TIAKI is a niche consulting practice helping executive leadership in sport make confident, informed decisions on their risks, investments and business outcomes powered by secure 'data-at-scale'.

TIAKI empowers CEOs, management teams, broadcasters and investors in the global sports industry with strategic advisory frameworks to deliver secure, pioneering digital fan experiences and new ecosystem business models to achieve breakthrough returns.

David has over 20 years of strategy and technology enabled business transformation experience, providing consulting expertise in cloud native technologies, data strategy, digital business enablement and cybersecurity strategy. He is passionate about helping talented leadership teams succeed in securely growing their differentiated business models in the data-driven, digital sports economy.

Based in Stockholm, David previously worked for IBM Consulting, EY, Accenture Strategy and Orange Business. He studied Chemistry at Durham University and holds an MBA from Trinity College, Dublin Business School.