AGENDA

The Future of Data & AI

Data & AI Think Tank

Click Here to Register

📅 **June 16, 2026**

Central Time

Registration	8:30 AM-9:00 AM
Morning Networking	9:00 AM-9:30 AM
Opening Remarks	9:30 AM-9:40 AM

KEYNOTE   9:40 AM-10:05 AM

Rearchitecting the Enterprise for Agentic AI: Control, Collaboration, and the Next Frontier of Automation

Agentic AI, autonomous systems that perceive, reason, and act with minimal human intervention is poised to redefine how work gets done. As these intelligent agents move beyond experimentation into enterprise-scale deployments, organizations must prepare to fundamentally rearchitect their digital environments.

This panel will explore how leaders can operationalize agentic AI to drive efficiency, creativity, and strategic advantage while preserving oversight, governance, and trust. Discussion topics will include designing workflows around autonomous decision-making, managing human-agent collaboration, and navigating emerging risks such as bias, security, and operational drift. Join us as we unpack what it truly means to lead in an era of intelligent, action-oriented AI and how to ensure these agents serve both your innovation goals and core business values.

10:10 AM-10:55 AM

The Human Side of Tech: Why Soft Skills Are the Real Superpower

In a world obsessed with digital transformation, AI, and automation, it's easy to forget the power of human connection. But the truth is—technology doesn't lead, people do. As roles evolve and teams become more cross-functional, the ability to listen, influence, adapt, and collaborate has become just as critical as technical expertise.

Today's CIOs, CISOs, and tech leaders are expected not only to drive innovation, but to communicate across departments, manage diverse teams, and navigate uncertainty with empathy and clarity. Emotional intelligence, storytelling, active listening, and resilience are no longer "nice to have"—they're essential for anyone leading in a fast-moving, high-stakes environment.

Nowhere is this leadership shift more relevant than in the US particularly in NYC, a city built on creativity, reinvention, and cultural diversity. Here, the ability to connect across perspectives isn't just a professional skill—it's a way of life. As tech and business worlds converge, NYC's unique blend of innovation and human-centered thinking offers the perfect backdrop to explore how soft skills are reshaping the future of leadership.

This session dives into why the most successful executives are blending EQ with IQ to inspire trust, build alignment, and drive lasting impact.

Networking Break

10:55 AM-11:15 AM

VISION VOICES

11:15 AM-11:30 AM

Securing the Rise of Agentic AI: Trust, Control, and Resilience in Autonomous Systems

As agentic AI systems evolve from experimental tools to enterprise-grade digital workers—capable of making decisions, taking actions, and adapting in real time—they introduce a new paradigm of both possibility and risk. Unlike traditional automation, agentic AI operates with greater autonomy, raising urgent questions for security leaders: How do we ensure control? How do we manage risk when systems learn, act, and adapt independently?

This panel will explore the security implications of deploying agentic AI across business operations—from data privacy and decision integrity to real-time threat mitigation and adversarial AI risks. We'll dive into the intersection of governance, identity management, and AI observability, and how CISOs can build frameworks that safeguard both the systems and the outcomes.

DISRUPTOR

11:35 AM-11:50 AM

Cybersecurity Leadership in the Era of AI and ML: Navigating Innovation and Responsibility

In the dynamic realm of artificial intelligence (AI) and machine learning (ML), CISOs play a pivotal role in leveraging these advancements for enhanced cybersecurity. Strategic integration of AI and ML is essential for bolstering security measures, optimizing decision-making, and driving innovation. CISOs must adopt a comprehensive approach, considering the entire lifecycle of these technologies to ensure both efficiency and ethical use. Establishing robust governance frameworks becomes paramount, addressing biases, ensuring transparency, and minimizing unintended consequences.

Looking ahead, as AI and ML continue to advance, CISOs face evolving challenges and regulatory considerations. Proactive engagement involves staying informed about changing regulations, particularly in areas such as data privacy and ethical AI practices. CISOs should strive for a tech-enabled understanding of AI and ML systems, encompassing deployment, impact, and security measures. This approach positions organizations to navigate the regulatory landscape effectively, ensuring responsible and competitive integration of AI and ML into cybersecurity strategies.

FIRESIDE CHAT

11:55 AM-12:30 PM

Strategic Shifts: Reimagining Engineering Talent Deployment and Management in the Age of GenAI

Unlock insights into the evolving landscape of talent deployment and retention as board expectations drive CIOs to rethink traditional IT talent models. Explore the impact of GenAI on coding processes and the software engineering lifecycle, and discover strategies for optimizing talent allocation and headcounts. Gain actionable insights into defining new roles, cultivating essential skills, and charting GenAI-centric career paths to align with organizational goals and stay ahead in a rapidly changing technological landscape.

Lunch
12:30 PM-1:30 PM

VISION VOICES
Zero Trust Network
1:40 PM-1:55 PM

A zero trust approach to security has been steadily gaining steam for the last several years. The importance of this approach reached a new level with the May 2021 White House executive order requiring federal agencies to shift to this architecture by fall 2025.
Ransomware continues to grow and clearly as remote work became the new norm, and e-commerce increased. Leaders need to establish a mature level of cyber resilience to better handle ransomware and other potential data breaches. Luckily, zero trust can play a critical part in that strategy as more and more businesses are realizing that to build customer trust, they must establish zero tolerance for trust in their security strategy. Will Zero Tolerance for Trust redefine the state of security as government and private industry scrutinize their trusted relationships more, and re-evaluate the 'who, what, why' in 2023 more than any other year?

DISRUPTOR
Building a Resilient Digital Infrastructure
2:00 PM-2:15 PM

In the digital age, building a resilient infrastructure for business continuity is paramount. This involves redundancy and backup systems, robust cybersecurity measures, cloud solutions, and the ability to facilitate remote work. Scalability, real-time monitoring, and ongoing training are essential, as are compliance with regulatory requirements and strong vendor relationships. Effective communication strategies, continuous improvement, and the establishment of a crisis response team round out the key components. By embracing these insights, organizations can better withstand disruptions and ensure the uninterrupted operation of critical systems, all while maintaining the trust of employees, customers, and stakeholders in an increasingly dynamic business environment.

Afternoon Networking
2:15 PM-2:35 PM

PANEL
Best Practices in Data Privacy & Security
2:40 PM-3:25 PM

Implementing best practices in data privacy and security is paramount in today's digital landscape. With the ever-growing volume of sensitive information being processed and stored, organizations must adopt a proactive approach to safeguarding data. This involves classifying and controlling data access, encrypting data, and staying vigilant through regular auditing and monitoring. Employee training is a linchpin in the security chain, ensuring that all personnel understand and adhere to data protection protocols. Moreover, having a robust incident response plan and keeping software updated are crucial components of a resilient security strategy. Building a culture of security, complying with relevant privacy laws, and regularly testing for vulnerabilities complete the framework. By following these best practices, organizations can better protect their data assets and maintain the trust of their customers and partners in an era where data privacy is of paramount concern.

FIRESIDE CHAT
Monetizing Digital Platforms
3:30 PM-4:15 PM

In the digital age, monetizing digital platforms is a fundamental challenge for businesses and content creators. These online spaces offer numerous revenue-generating avenues, including advertising, subscriptions, e-commerce, affiliate marketing, and the sale of digital products or services. Effective monetization strategies require a deep understanding of the target audience, the delivery of valuable content or services, and the creation of user-friendly experiences that encourage engagement and conversions. Finding the right balance between profitability and user satisfaction is central to realizing the potential of digital platforms in the contemporary digital economy.

Closing Remarks
4:15 PM-4:25 PM

PARTNERS

We are currently accepting partnership opportunities for this event.