immersive

From Deepfakes to Data Breaches:

Strengthening Cyber Resilience in the Age of AI

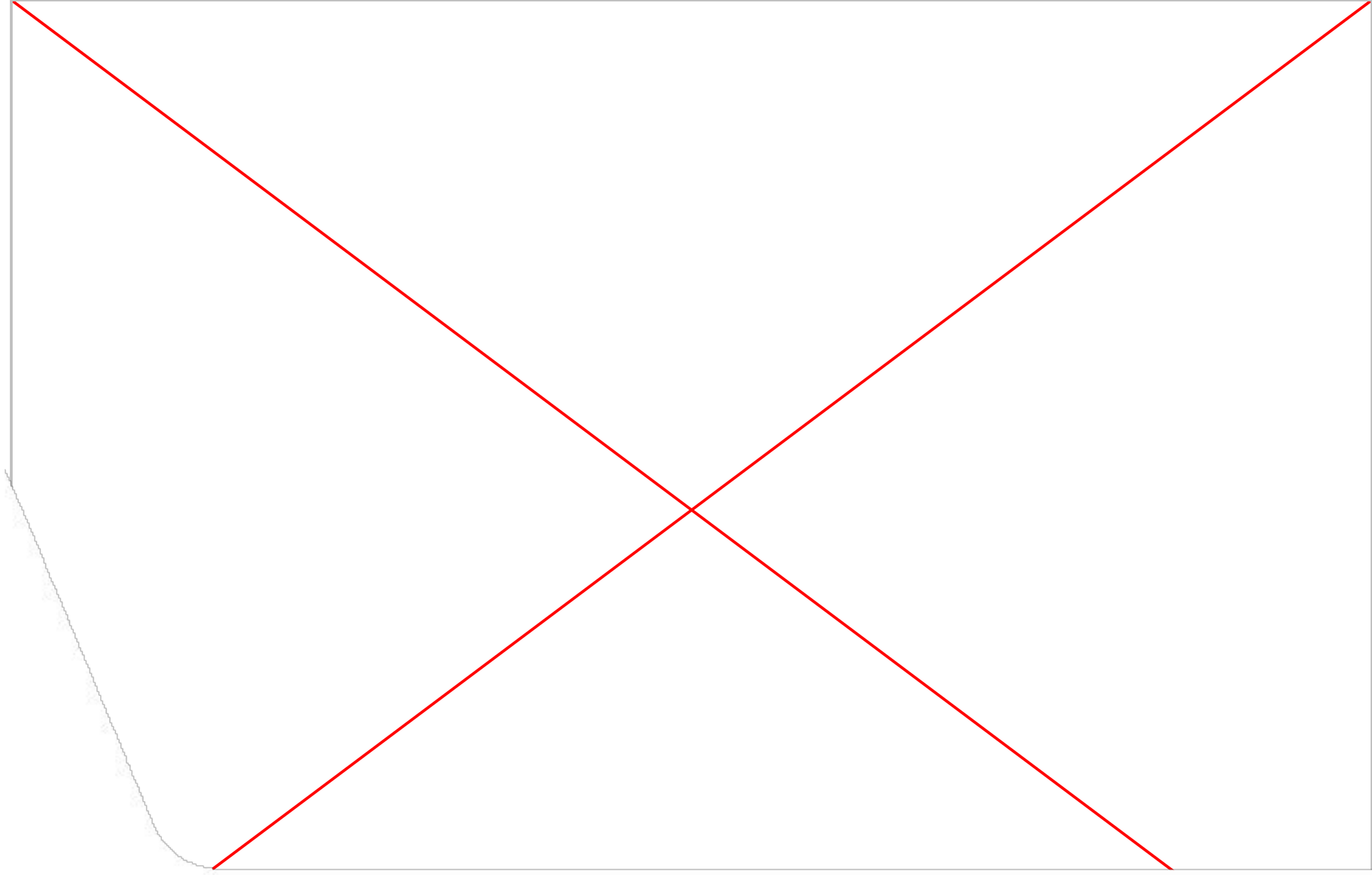
Jamie Knobles

Director, Cyber Resilience & Readiness

www.immersivelabs.com

The Evolving Threat Landscape

AI is rapidly transforming our world, but also fueling increasingly sophisticated cyberattacks. Protecting against these evolving threats, especially in the public sector, requires a new, human-centric approach to cybersecurity resilience.



The Trojan Horse of the Digital Age

01 AI-generated synthetic media that convincingly mimic real people, bypassing our defenses and exploiting trust

02 Prey on our inherent trust in audio and video, making us vulnerable to emotional manipulation and the spread of misinformation

03 Not a hypothetical threat; already being used to target public figures and manipulate public opinion

Deepfakes and Their Impact

01

Financial Loss

Can manipulate employees into fraudulent transactions, resulting in significant financial damage to organizations.

02

Reputational Damage

Can create false narratives, impacting careers, businesses, and personal relationships.

03

Societal Harm

Can spread misinformation, influence elections, and fuel social unrest, eroding public trust.

04

Security Breaches

Can manipulate security systems, granting unauthorized access to secure locations.

GenAI-Driven Cyberattacks

Personalized Phishing

Empowers highly customized phishing attacks, mimicking trusted individuals to trick users into divulging sensitive information

Adaptive Malware

AI-enhanced malware learns and adapts, evading detection and automating vulnerability exploitation at scale.

Amplified Attacks

AI increases the sophistication and scale of cyberattacks, posing a significant threat to critical infrastructure and public trust.

Who is at risk?

Cyber Resilience - More Than Just Technology

Prepare & Protect

How do you know?

Your organization has the **cyber capabilities** to prevent breaches

Cyber Incident

Detect & Respond

How do you know?

Your organization has the **decision-making skills** and muscle memory to effectively respond to an incident?

People-centric risk reduction and resilience requires:
Knowledge, Skills and Judgment

Upskilling the Workforce

01

Targeted Training

Equipping staff with specialized knowledge and skills to counter AI-powered cyberattacks, beyond general cybersecurity awareness.

02

Deepfake Defense

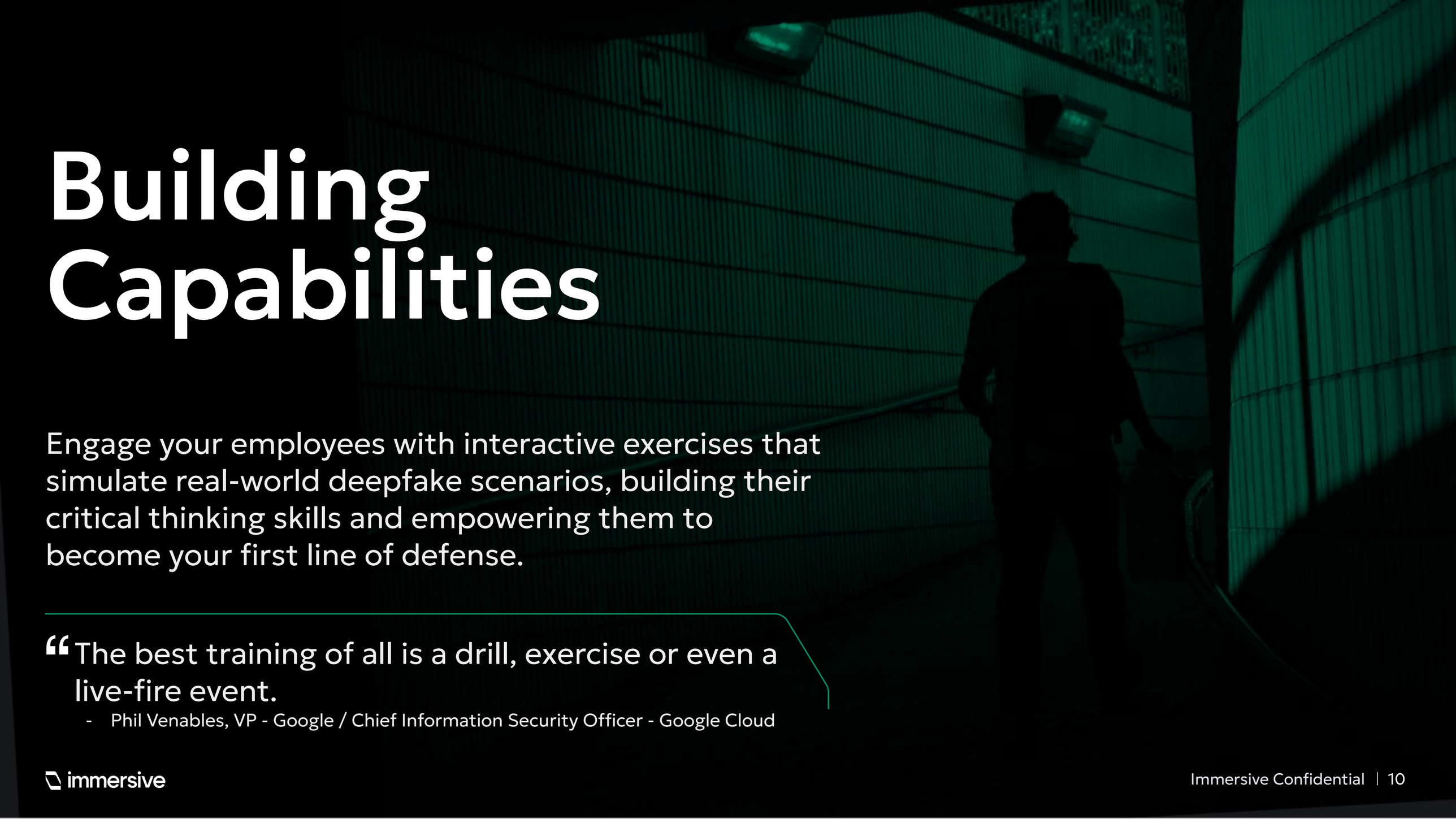
Building expertise in deepfake recognition tactics to empower employees as a crucial line of defense.

03

Resilient Workforce

Developing resilience against sophisticated, AI-driven phishing, social engineering, and other manipulative tactics.

Building Capabilities



Engage your employees with interactive exercises that simulate real-world deepfake scenarios, building their critical thinking skills and empowering them to become your first line of defense.

> “The best training of all is a drill, exercise or even a live-fire event.
>
> - Phil Venables, VP - Google / Chief Information Security Officer - Google Cloud

Cyber Drills

Cyber drills simulate real-world attacks, bridging the gap between technical and leadership teams to strengthen organizational cyber resilience. These large-scale exercises provide invaluable practical experience responding to AI-powered threats like deepfakes and adaptive malware, ultimately building a more secure digital infrastructure.

Hone the Human Edge: Build a Culture of Vigilance

01

Encourage Questioning

Promote skepticism and verification of requests and information to identify potential threats.

02

Foster Open Communication

Create a safe space for employees to share concerns and collaborate on cybersecurity initiatives.

03

Secure Leadership Buy-in

Demonstrate leadership commitment to cybersecurity through action and communication.

04

Promote Continuous Learning

Provide ongoing opportunities for employees to stay informed about evolving AI-related cyber threats.

Prevention is Key

Minimize Exposure

Implement strong access controls, data encryption, and secure storage to limit the vulnerability of sensitive information. Embed a security-first mindset in all operations, encouraging critical thinking about information consumption and AI risks.

Verify Content Integrity

Invest in tools and technologies to authenticate digital content, ensuring the reliability of information used in public sector decision-making. This includes robust authentication and continuous monitoring of AI agent activity.

Strengthen Supply Chains

Address challenges faced by Canadian organizations by promoting and supporting the adoption of robust supply chain security practices, including SBOMs and VEX, along with standardized formats.

Don’t Just Trust, Verify

01 Verification is paramount in the age of AI, requiring us to go beyond trust and implement robust protocols.

02 Multi-factor authentication and out-of-band verification of sensitive requests are crucial for preventing unauthorized access and deepfake attacks.

03 Investing in AI-powered deepfake detection tools and employee education on verification procedures are essential for a "trust, but verify" approach.

Evolving Legal Landscape

01	**Transparency**	AI systems used in the public sector must be understandable and accountable to citizens.
02	**Accountability**	Clear oversight mechanisms are essential to prevent misuse of AI, especially in surveillance.
03	**Compliance**	Adherence to existing legislation like PIPEDA is crucial for maintaining public trust and protecting privacy.
04	**Evolving Regulations**	Staying informed about emerging laws like AIDA and global AI initiatives is key for responsible AI deployment.

Key Takeaways

01 Human-Centric Resilience

Empowering public servants as the first line of defense against AI-powered threats through knowledge and skill development.

02 Culture of Vigilance

Fostering a mindset of questioning, verification, and reporting to create a human firewall against deception.

03 Proactive Prevention

Prioritizing preventative measures, including secure systems, limited exposure, and a security-first mindset.

04 Continuous Adaptation

Recognizing the evolving threat landscape and continuously updating policies, procedures, and training.

05 Strategic Collaboration

Breaking down silos and fostering open communication between agencies, partners, and citizens.

06 Urgent Action

Prioritizing cybersecurity investments in human capital and taking immediate steps to build a more resilient public sector.

Thanks!

immersive

Continuously Prove and Improve Your Cyber Resilience

Immersive Labs is trusted by the world's largest organizations and governments, including Citi, Pfizer, Daimler, Humana, HSBC, the UK Ministry of Defence, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Ten Eleven Ventures, Summit Partners, Insight Partners, Citi Ventures, and Menlo Ventures.