C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

CISO Think Tank

SPEAKERS

Cassie Crossley
VP, Supply Chain Security
Schneider Electric

Steve Zalewski
Former CISO
Levi Strauss & Company

Mark Fullbrook
CRO
RevealSecurity

Leda Muller
CISO
Stanford University, Residential and Dining Enterprises

Bharani Krish
VP Enterprise Infrastructure
Molina Healthcare

David Chun
CIO
Sonoma State University

Nancy Selph
CIO
Avellino Lab

Shadaab Kanwal
Managing Director Digital, Data and Analytics Services
Charles Schwab

Phani Burra
Director, Cloud Transformation
Albertsons

Bob Lim
CIO
San Jose State University

Arun Changamveetil
VP Data & AI Architecture
Salesforce

Gavin Grounds
CEO & Co-Founder
Mercury Risk

Aled Miles
CEO
Sauce Labs

Jim Whitehead
Chief Scientist
Sauce Labs

Bharath Nagaraj
Senior Principal Field Technical Director
Cohesity

Kaladhar Voruganti
Senior Technologist, CRO
Equinix

Chandra Sadanala
CTO
Forsys Inc

Barney Gomez
Use IT Manager, State of CA
California Department of Health Care Services

Manish Gupta
CIO
Nagarro

Prasad Suravarapu
VP Enterprise Data Management
Bank of the West

Kumar Ramachandran
SVP, Product and GTM
Palo Alto Networks

Click Here to Register

May 18, 2023

Pacific Time

Registration

9:30 AM-10:15 AM

Morning Networking

10:15 AM-11:00 AM

Opening Remarks

11:00 AM-11:05 AM

VISION KEYNOTE PANEL

Bridging the Gap Between IT and the Business

11:05 AM-11:50 AM

Bridging the gap between business and technology is not easy and requires discipline and balance between technology, people, and the business. For so many organizations today, technology is the business. Technology needs to be understood as a critical enabler in every part of the organization from the front line to the back office. It creates new value by crunching data to deliver new insights, it spurs innovation, and it disrupts traditional business models.
For business and technology leaders alike, new actions and behavioral changes can help their organizations make this shift. CIOs must take responsibility for problems, they should convey that when technology fails, many people typically share responsibility.

CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Company

PANELISTS

Nancy Selph
CIO
Avellino Lab

Barney Gomez
Use IT Manager, State of CA
California Department of Health Care Services

Prasad Suravarapu
VP Enterprise Data Management
Bank of the West

FIRESIDE CHAT

Testing the Limits of Possibility

11:55 AM-12:30 PM

We are at the ground floor of a new innovation curve—the breakthrough of modern AI—that blows past previous limits of what's possible to build with software. This, coupled with its overlap with the mobile revolution, create an unprecedented moment, and software leaders must build a new set of practices around software development to embrace exponential increases in innovation, but without sacrificing the quality of customer experience that's table stakes in a post-mobile world.
In this talk, Aled Miles, CEO of Sauce Labs, former CEO of Telesign and executive committee member at Symantec, along with Jim Whitehead, Chief Scientist, AI Research Development and Experiments (AIX) team at Sauce Labs, and a Professor of Computational Media at the University of California, Santa Cruz will leverage their expertise leading companies and research programs at the forefront of these two overlapping innovation cycles to document and explore the convergence of consumer expectations, digital transformation, and innovation in artificial intelligence.

PANELISTS

Aled Miles
CEO
Sauce Labs

Jim Whitehead
Chief Scientist
Sauce Labs

Lunch & Disruptor Showcase

12:30 PM-1:30 PM

LUNCH & DISRUPTOR SHOWCASE

Detecting Imposters and Rogue Insiders in SaaS Applications

1:15 PM-1:30 PM

The combination of rogue insiders and external attackers makes SaaS application detection a massive pain point for enterprises, particularly within core business applications. External attackers leverage stolen credentials to impersonate an insider and connect to applications, while at the same time insiders are not sufficiently monitored. Such examples could include a fraudster's takeover via social engineering, or incorrect implementation by an employee, or a doctor accessing celebrity patient medical data, or a salesperson downloading a report of all customers before switching to work for a competitor.
Even after the enterprise receives a complaint or is otherwise suspicious, detection of these breaches usually consists of manual sifting through tons of log data from multiple sources.
RevealSecurity's CRO, Mark Fullbrook, will explore the growing challenge of SaaS application detection, explain why current detection solutions are usually ineffective, and share solutions using real customer examples.

PANELISTS

Mark Fullbrook
CRO
RevealSecurity

PANEL

1:35 PM-2:20 PM

Transforming Network Security with AI-Powered SASE

Recent advancements in Artificial Intelligence (AI) have captured the imagination of the world, and the way we work right is getting transformed right in front of our eyes. It is imperative for the modern IT leaders to leverage the power of AI/ML to deliver productive and secure experiences for their organizations. Join us in this executive roundtable to hear about:
Why a unified approach to SASE is critical for leveraging AI
How AI/ML can deliver better security, networking and operational outcomes
Best practices to adopt SASE that sets you up for success

CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Company

PANELISTS

Gavin Grounds
CEO & Co-Founder
Mercury Risk

Kumar Ramachandran
SVP, Product and GTM
Palo Alto Networks

Leda Muller
CISO
Stanford University, Residential and Dining Enterprises

DISRUPTOR

Cloud Adjacent Architecture

2:25 PM-2:40 PM

In this talk we present two hybrid architecture design patterns that are allowing customers to get better cost, performance, and compliance posture:
Cloud Adjacent Storage: Customers are storing their data at a cloud adjacent location while compute still takes place in the cloud to move from a variable cost model to a fixed and more predictable cost model for storage. This is providing more flexibility with respect to a multi-cloud model and cost savings.
Distributed AI: Customers are moving from a centralized AI model where training and inference take place at the same location to a distributed AI model where training takes place at a central location and inference happens at the edge for cost, performance and compliance reasons.

PANELISTS

Kaladhar Voruganti
Senior Technologist, CRO
Equinix

Networking Break

2:40 PM-3:00 PM

PANEL

Exploring the Intersection of AI, ML, and Social Engineering: Implications and Opportunities in 2023

3:00 PM-3:45 PM

The integration of artificial intelligence (AI), machine learning (ML), and social engineering has significant implications for businesses in 2023. While AI and ML can enhance threat detection and response capabilities, threat actors are also utilizing these technologies to conduct more advanced attacks. Social engineering attacks continue to be a top concern, and AI and ML can be leveraged to create more realistic and personalized attacks.

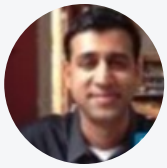
As a result, businesses must stay informed about the latest developments in AI, ML, and social engineering to protect their assets and reputation. CIOs and CISOs must work together to implement advanced security measures and ensure their employees are trained to identify and report suspicious activity. Businesses that fail to adapt to this new threat landscape risk falling behind their competitors and experiencing costly breaches.

CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Company

PANELISTS

Cassie Crossley
VP, Supply Chain Security
Schneider Electric



Arun Changamveetil
VP Data & AI Architecture
Salesforce

Manish Gupta
CIO
Nagarro

DISRUPTOR

Building a High Confidence Cyber Recovery Plan

3:50 PM-4:05 PM

Data is a differentiator in the digital economy. That's why data has simultaneously become the most valuable and the most targeted business asset. Cybersecurity Ventures expects global cybercrime costs to reach $10.5 trillion USD annually by 2025 and that companies will fall victim to a ransomware attack every 2 seconds by 2031. We have seen plenty of bad things happen due to insufficient security measures. As a species, we tend to wait for those truly significant "black swan" events before making substantial changes.
Move from waiting to anticipating, preventing and being cyber resilient. Hear from Cohesity's Senior Technical Field Director, Bharath Nagaraj, as he will speak to some of his field learnings on what C-levels of large organizations deal with and how you can learn to respond more effectively and strategically.

PANELISTS

Bharath Nagaraj
Senior Principal Field Technical Director
Cohesity

Closing Remarks & Raffle Giveaway

4:05 PM-4:10 PM

Cocktail Hour

4:10 PM-5:55 PM

TOGETHER WITH


EQUINIX
grip
REVEAL
SauceLabs
FORTRA
paloalto
NETWORKS
PRISMA SASE
COHESITY
aws