C VISION INTERNATIONAL

AGENDA

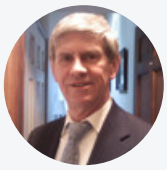
Future of Cybersecurity

CISO Summit

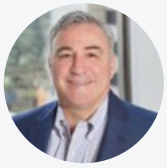
SPEAKERS



Richard Rushing
CISO
Motorola Mobility



Ivan Durbak
CIO
BronxCare Health System



Tony Parrillo
Global Head of Security
Schneider Electric



Rick Patterson
EVP CISO
Clear



Hans Vargas
Cyber
MPCLP



Damon Becknel
CISO
ID.me



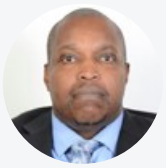
Prabha Jha
Director, Security
Verizon



Edmond Mack
CISO
Cencora



Peter Tse
Information Security Officer
CTBC Bank



John Whiting
Global CSO
Omnicom



Tim Swope
CISO
Catholic Health System



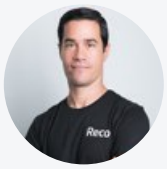
John Savini
CISO, Optum Insight & Analytics
Optum



Kenneth Townsend
Global CISO
Ingredion



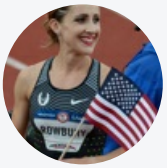
Wade Lance
Field CISO
Synack, Inc.



Ofer Klein
Co-Founder & CEO
Reco



Marcus Merrell
VP of Technology
Sauce Labs



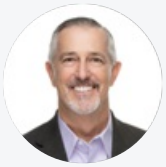
Shannon Rowbury
US Olympian & WSG
US Olympics



Anthony Gonzalez
Former CISO
Innervision Services LLC



Demond Waters
CISO
NYC Public Schools



Tim Woods
VP of Technology Alliance
FireMon



Kathleen Hurley
CIO
Sage Inc



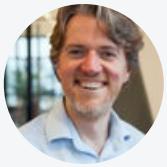
Rohit Agrawal
SVP IT, Global Head of Hybrid Cloud
Siemens Healthineers



Kish Galappatti
Senior Sales Engineer
CardinalOps



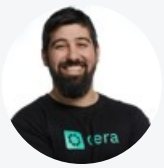
Bob West
Chief Security Officer, Prisma Cloud
Palo Alto Networks



Ky Nichol
CEO
Cutover.



Rahul Bhardwaj
Deputy CISO
Kroll



Yotam Segev
Co-Founder & CEO
Cyera US Inc.



Keith Donnelly
VP, Global Head of Risk & Compliance
Broadridge



Matthew Martin
Founder
Two Candlesticks



Wes Kussmaul
CISO
Authenticity Institute



Todd Carroll
CISO/VP of Global Cyber Operations
CybelAngel



Justin Conza
Technical Product Specialist
KnowBe4

Click Here to Register

November 16, 2023

Eastern Time

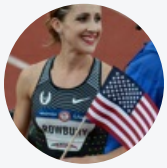
Welcome & Registration	**8:00 AM-8:30 AM**
Morning Networking	**8:30 AM-9:00 AM**
Opening Remarks	**9:00 AM-9:15 AM**

My Olympic Mindset

9:15 AM-9:30 AM

Dissecting the career of a 3xOlympic Athlete and translating sports performance principles to unlock business success.

SPEAKER



Shannon Rowbury
US Olympian & WSG
US Olympics

KEYNOTE
Testing the Limits of Possibility

9:35 AM-10:00 AM

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, In this talk, Marcus Merrell, Vice President of Technology Strategy at Sauce Labs, and executive committee member of the Selenium project, will leverage his expertise leading teams 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. Culminating in a "call to arms," a rally cry, for other executives across all industries and categories to think hard about their software development philosophy and how they will deliver quality customer experiences in an uncharted environment, or suffer the consequences of irrelevance.

SPEAKER



Marcus Merrell
VP of Technology
Sauce Labs

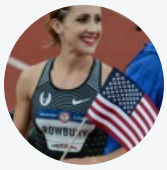
FIRESIDE CHAT

Synergy of Leadership, Athlete Mindset, Cybersecurity, and Technology for Business Success

10:05 AM-10:45 AM

In today's dynamic business landscape, the fusion of leadership principles and the athlete mindset, combined with a strong focus on cybersecurity and technology, offers a potent approach to meet evolving demands. Leadership qualities like adaptability, resilience, and vision complement the discipline, determination, and performance focus inherent in athletes. This connection is particularly relevant in the realm of cybersecurity and technology, where leaders must navigate constant change and cyber threats. Integrating athlete mental skills into technology leadership roles and fostering a culture of cybersecurity resilience is essential. By recognizing this synergy, businesses can equip their leaders to thrive in the face of technological disruptions and security challenges, ultimately ensuring sustainable success in the digital age.

SPEAKERS



Shannon Rowbury
US Olympian & WSG
US Olympics



Bob West
Chief Security Officer, Prisma Cloud
Palo Alto Networks

Coffee Break

10:45 AM-10:55 AM

Poor Cyber Hygiene

10:55 AM-11:10 AM

In the digital age, practicing good cyber hygiene is essential to maintaining the security and integrity of personal and business data. However, in 2023, the lack of basic cyber hygiene practices will continue to be a major cause of cyber incidents. Cybercriminals exploit these vulnerabilities to gain unauthorized access to sensitive information, steal data, and launch damaging cyber attacks. It's crucial for individuals and businesses to prioritize basic cyber hygiene practices, such as using strong passwords, regularly updating software, and backing up data. Additionally, individuals and businesses must educate themselves and their employees on cybersecurity best practices and the latest threats to stay ahead of the evolving threat landscape. By taking these proactive steps, individuals and businesses can protect themselves from cybercriminals who prey on poor cyber hygiene practices.

SPEAKER



Richard Rushing
CISO
Motorola Mobility

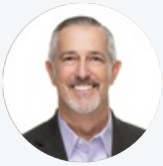
DISRUPTOR

11:15 AM-11:30 AM

Compliance: What Can be Done Today about Tomorrow's Challenges

In the dynamic landscape of cybersecurity and compliance, 2024 looms as a pivotal year. CISOs and cybersecurity leaders are focused on safeguarding not just data, but the future of your business. For this intimate, virtual gathering we bring together industry experts to delve into the upcoming compliance challenges, including the formidable PCI DSS 4.0, and explore how proactive preparation can be a catalyst for business resilience.
Join us for an insightful journey that transcends checkboxes and audits, focusing on aligning compliance with broader business objectives. Discover strategies to enhance organizational agility, reduce risks, and ensure that compliance not only meets regulatory mandates but also fuels your business growth.

SPEAKER



Tim Woods
VP of Technology Alliance
FireMon

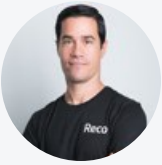
DISRUPTOR

11:35 AM-11:50 AM

Leveraging Artificial Intelligence for SaaS Discovery

In today's interconnected business world, companies rely on SaaS applications as the operating system of business, which can pose significant cybersecurity risks. This makes it critical for companies to have effective security measures in place to properly secure their entire SaaS environment. Failure to do so can result in data breaches, financial losses, and reputational damage. To mitigate this risk, companies must ensure they are monitoring not only the SaaS applications that are managed and known to the IT team, but their entire SaaS environment. Application discovery provides a comprehensive view into the entire SaaS ecosystem, including what managed applications have access to data, connected third-party apps, and even shadow apps, as well as who has enabled them, and the level of access they've been granted. Using a combination of graph algorithms, anomaly detection, NLP, and GenAI tools, solutions leveraging AI can provide a complete picture of interactions and activities across users. This insight can be used to pinpoint common causes of a breach such as misconfigurations, overly permissioned users, and compromised accounts. In this session, we'll explore the importance of investing in SaaS discovery, how AI can add the context needed to protect against common causes of breaches, and how organizations can secure their SaaS from the most common risks that can lead to a breach in 2023 and beyond.

SPEAKER



Ofer Klein
Co-Founder & CEO
Reco

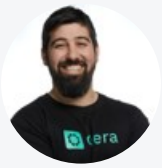
DISRUPTOR

11:55 AM-12:10 PM

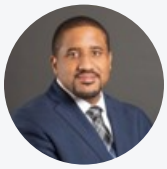
Your Most Important Asset: Data - Is It Really Secure?

Boosting data security posture is a top priority for organizations in 2023 and beyond. In a recent Forrester Research study commissioned by Cyera, 71% of security leaders said legacy technologies and manual processes inhibit business success. Join this deep dive discussion on why today's security executive expects the most transformational business benefits to come from automating data security, specifically risk assessments, data discovery, and classification.
Session topics will include:
The struggle to meet security goals while enabling the business to use data and advanced technologies
New approaches to data security that keep pace in the era of cloud and AI
Generative AI - risk versus reward
Embracing automation and rapid time are critical capabilities in cybersecurity

SPEAKERS



Yotam Segev
Co-Founder & CEO
Cyera US Inc.



Edmond Mack
CISO
Cencora

Lunch & Networking

12:15 PM-1:15 PM

PANEL

Ransomware and Cyber Readiness

1:15 PM-2:00 PM

Ransomware attacks are becoming increasingly prevalent and sophisticated, affecting businesses and individuals in all sectors. In 2023, these attacks are expected to continue to grow, resulting in significant financial losses, data theft, and reputational damage. Businesses should implement comprehensive security measures, including regular backups, employee training, and endpoint security, to minimize the risk of a ransomware attack. Additionally, because cyber attacks are unpredictable and complex it's important to have cyber recovery plans in place to orchestrate both teams and technology to minimize the impact of an attack. Businesses must develop recovery plans detailing the tasks to restore systems, manage data integrity, keep stakeholders informed of progress and meet regulatory requirements.

CHAIR

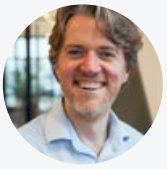


Anthony Gonzalez
Former CISO
Innervision Services LLC

PANELISTS



John Savini
CISO, Optum Insight & Analytics
Optum



Ky Nichol
CEO
Cutover.

DISRUPTOR

Using Strategic Security Testing to Transform Your Security Posture

2:05 PM-2:20 PM

Most security testing today is purely tactical- we find vulnerabilities and sometimes fix them. We use this process to satisfy compliance requirements and report point-in-time status to regulators, but we rarely learn anything about our overall security posture and use that information to change our strategy and priorities. Strategic, transformational security testing is the solution.

Strategic security testing uses aggregated data from individual penetration tests to reveal the root cause of persistent weaknesses in security posture due to broken processes and overwhelmed staff. Security and IT management can use that data to invest in training and solutions that are specifically targeted at organizational deficiencies. Moreover, a strategic security testing program will track improvements in overall security posture over time so those improvements can be communicated to senior leadership and the board.

SPEAKER



Wade Lance
Field CISO
Synack, Inc.

Networking Break

2:20 PM-2:50 PM

DISRUPTOR

2:25 PM-2:40 PM

Enhancing the Resilience of Your Organization's Final Barrier: The Human Firewall

In today's digital landscape, social engineering attacks like phishing, Business Email Compromise (BEC), and Ransomware are increasingly prevalent. These cunning tactics rely on manipulating humans to gain unauthorized access to protected systems and sensitive data. As the frequency of such cyber-attacks rises, it is crucial to fortify your organization's last line of defense: the human firewall.
In this session we will look into case studies around:
Regular, tailored security awareness training to educate employees about social engineering threats.
Foster a reporting culture for prompt identification of suspicious activities.
Strengthen password policies and use multi-factor authentication (MFA) to reduce risks.

SPEAKER



Justin Conza
Technical Product Specialist
KnowBe4

DISRUPTOR

2:50 PM-3:05 PM

The Current and Future State of your External Attack Surface

Today's threat landscape is growing two fold every year due to a growing cyber ecosystem with partners, third parties and vendors. Add the technically "savvy" remote employee workforce with an increase in remote services use, the threats to IP, data and operations has significantly grown.
In this session we will:
Review key data from the CybelAngel EASM report and current data trends
Show visibility into this attack vector is possible to help identify high risk areas and help prioritize threats before they become front page news.

SPEAKER



Todd Carroll
CISO/VP of Global Cyber Operations
CybelAngel

CISO Evolution: Adopting a Risk Mindset

3:10 PM-3:25 PM

In today's complicated cyber environment, the significance of a risk-centric approach is paramount. Explore the importance of adopting a risk mindset as a core in building your security strategy and ensuring buy-in from senior leaders. In this talk, I will discuss my journey over the last 30 years, lessons learned, and mistakes made. As well as the urgency to get this right in light of the evolving cybersecurity landscape and heightened CISO liability.

SPEAKER



Rick Patterson
EVP CISO
Clear

PANEL
Cloud Vulnerabilities

3:30 PM-4:15 PM

Cloud computing services have become a cornerstone of modern business operations, providing organizations with the agility and scalability needed to thrive in the digital age. However, in 2023, the threat of cloud vulnerabilities will continue to grow as more companies adopt cloud services. Cybercriminals are constantly finding new ways to exploit vulnerabilities in cloud infrastructure, which can result in data breaches, unauthorized access, and financial losses. To mitigate the risks of cloud-related security incidents, businesses must prioritize implementing robust security measures such as multi-factor authentication, encryption, and regular penetration testing. Additionally, businesses must develop comprehensive incident response plans that take into account the unique challenges of cloud-based attacks. By taking these steps, businesses can protect themselves and their customers from the growing threat of cloud vulnerabilities in the digital age.

CHAIR



Matthew Martin
Founder
Two Candlesticks

PANELISTS



Kish Galappatti
Senior Sales Engineer
CardinalOps



Hans Vargas
Cyber
MPCLP



John Whiting
Global CSO
Omnicom



Demond Waters
CISO
NYC Public Schools

Networking Break

4:15 PM-4:25 PM

Building a Cyber Resilient Culture

4:25 PM-4:40 PM

The ability of an organization to prepare for, respond to, and recover from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges.

SPEAKER



Kenneth Townsend
Global CISO
Ingredion

PANEL
Internet of Things

4:45 PM-5:30 PM

The Internet of Things (IoT) is a network of physical devices that communicate and exchange data, creating new opportunities for businesses and consumers alike. However, in 2023, the increasing adoption of IoT devices will pose new security risks. Cybercriminals are becoming more adept at exploiting vulnerabilities in IoT devices, which can result in data breaches, unauthorized access, and privacy violations. It's essential for businesses to prioritize security measures such as strong authentication protocols, regular software updates, and network segmentation to minimize the risk of an IoT-related security incident. Additionally, businesses should implement comprehensive incident response plans to quickly and effectively respond to a potential IoT-related attack.

CHAIR

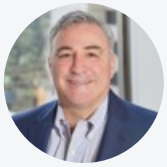


Tim Swope
CISO
Catholic Health System

PANELISTS



Edmond Mack
CISO
Cencora



Tony Parrillo
Global Head of Security
Schneider Electric



Prabha Jha
Director, Security
Verizon



Peter Tse
Information Security Officer
CTBC Bank

Closing Remarks & Raffle Giveaway

5:30 PM-5:45 PM

Cocktail Reception

5:45 PM-6:45 PM

TOGETHER WITH

chronosphere KnowBe4 Human error. Conquered. RegScale


Synack
SauceLabs
reco
CYERA
CybelAngel
FIREMON
CARDINALOPS
Gem
cutover
paloalto
NETWORKS
valence
Scribe