CVISION INTERNATIONAL

AGENDA

The Future of IT & Cybersecurity
CXO Summit

SPEAKERS

Kenn Kern
CIO, CISO Special Assistant
City of New York

Amit Basu
VP, CIO & CISO
International Seaways

Peter Dentico
Managing Director Security Operations
Omnicom Group

Susan Koski
CISO
PNC

Devon Bryan
Global CIO
Carnival Corporation

Ibrahim Jackson
Founder
Ubiquitous Preferred Services

Anthony Gonzalez
CISO NA
QBE North America

Adam Fishman
COO US Investment Banking
RBC Capital Markets

Nick Diieso
Director, Global Head of Operational Risk
Citi

Leo Cunningham
Former CISO
Flo Health Inc.

Vic Ventura
Global CIO
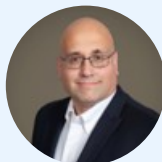Novolex

Scot Miller
SVP & CISO
Mr. Cooper

Laura Deaner
CISO
Northwestern Mutual

Martin Howard
EVP/IT & IS
Fortium Partners

Michael Gross
Manager, Cybersecurity Intelligence
Cleveland Clinic

Avishai Avivi
CISO
Safebreach

Anna Thomas
Director Operations & Technology Transformation
Citibank

Shamla Naidoo
Head of Cloud Strategy & Innovation
Netskope

Scott Dillon
CEO, Digital Evangelist, Board Advisor & Investor

Kathleen Hurley
CIO
Sage Inc

Cecilia Li
CIO
Urban Edge Properties

Alex Shulman
Managing Director, Cloud Security
Ernst & Young

Jim Routh
CSO, Board Member, Advisor & Investor
Transmit Security

Charles Blauner
CISO
Cyber Aegis

Viktoria Levay
Corporate Health Coach & Resilience Trainer
Nourish With Viktoria

Amy Aiello
Amy Aiello Photography

Michael Woodson
Director of Information Security
Sonesta International Hotels Corporation

Ben Cody
SVP Product Management
SailPoint Technologies Inc

Karl Mattson
CISO
Noname Security

Anne Marie Zettlemoyer
CSO
CyCognito

Anand Raghavan
Co-Founder & CPO
Armorblox

Ben Halpert
Founder & CEO
CISO Horizon

Aruna Ravichandran
SVP, CMO, Webex by
Cisco

Doron Hendler
CEO & Co-Founder
RevealSecurity

Jason Stutt
CRO
ArmorCode

Gabi Reish
Chief Product Officer
Cybersixgill Ltd.

Todd Dekkinga
CISO
Zluri

David Geevaratne - NO LONGER W/ COMPANY!!!
SVP of Sales
Uptycs

Martin Howard
EVP/CIO
Avesis

Anthony Gonzalez
Principal, Strategic Advisor
Innervision Services LLC

Leo Cunningham
CISO
Owkin Inc

Karl Mattson
CISO
Endor Labs

Click Here to Register

📅 November 09, 2022

Eastern Time

Registration & Breakfast
8:45 AM-9:30 AM

Opening & Welcome
9:30 AM-9:45 AM

Viktoria Levay
Corporate Health
Coach & Resilience
Trainer
Nourish With
Viktoria

PANEL

The "New" Workspace

In the post pandemic era, remote employment is the new status quo. Employers are forced to implement and improve the digital workplace by providing productivity tools and accessibility to company resources. In this session, we will share case studies of successful digital workplace implementations, including how to deal with the inherent security risks of expanded accessibility to company resources.

CHAIR

PANELISTS

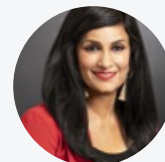**Ibrahim Jackson**
Founder
Ubiquitous Preferred
Services

Adam Fishman
COO US Investment
Banking
RBC Capital Markets

Martin Howard
EVP/IT & IS
Fortium Partners

Kathleen Hurley
CIO
Sage Inc

Aruna Ravichandran
SVP, CMO, Webex by
Cisco

KEYNOTE

Application Security in a DevOps, Cloud and API World

Security teams are challenged to modernize application security practices in light of accelerating shifts to DevOps delivery models and rapid adoption of cloud-native application designs. Applications built on microservices (e.g. serverless, containers, APIs) and delivered continuously are outpacing application security teams ability to secure them. CISOs need to consider new skills, new touch points and new platforms to maintain a strong security posture in light of these trends and the speed at which they are re-shaping IT.

PANELISTS

Karl Mattson
CISO
Noname Security

Networking Break

PANEL

Operationalization: Bridging the Divide between Knowledge and Action

Knowledge is power, and yet, knowing is not enough. Security teams are well aware of the vital role played by threat intelligence within the modern security stack. Too often, TI is underutilized, funneled through manual processes to the desks of security analysts and researchers, and not operationalized to drive automated cybersecurity processes and actions.

Why is this knowledge lost in translation on the way to action? Is it due to the overwhelming quantities of data? Is it because of conflicting information? Is it related to concerns about false positives? If we succeeded in operationalizing sensor-driven telemetry data in vehicles to autonomously drive cars, why aren't we as successful in operationalizing threat intelligence data to drive autonomous cybersecurity actions?
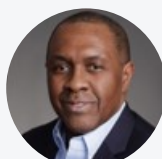
CHAIR

Gabi Reish
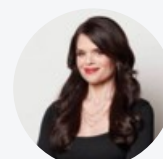Chief Product Officer
Cybersixgill Ltd.

PANELISTS
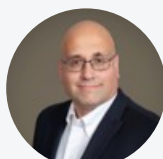
Avishai Avivi
CISO
Safebreach

Michael Woodson
Director of Information Security
Sonesta International Hotels Corporation

Cecilia Li
CIO
Urban Edge Properties

Anne Marie Zettlemoyer
CSO
CyCognito

FIRESIDE CHAT

Lunch & Fireside Chat

BEC - FBI calls it the $43B* heist. How to tame this beast?

According to the FBI's recent IC3 report in 2022, exposed business loss due to BEC accounts for > $43B. Why? At the heart of it, the biggest fear is not the technology, it is the potential of human error that could expose your organization to a cyberattack. The majority of CISOs agree that an employee carelessly falling victim to a BEC/phishing scam is the most likely cause of a security breach. Most also agree that they will not be able to reduce the level of employee disregard for information security. How do we guard against human error without limiting employee efficiency and productivity?
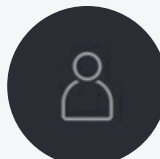
CHAIR
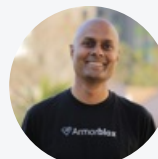
Ibrahim Jackson
Founder
Ubiquitous Preferred Services

PANELISTS

Devon Bryan
Global CIO
Carnival Corporation

Scott Dillon
CEO, Digital Evangelist, Board Advisor & Investor

Anand Raghavan
Co-Founder & CPO
Armorblox

PANEL

Building Security into DevSecOps

Many organizations struggle with how and where to introduce automation and integrations efficiently. Conventional approaches to application security can't keep pace with cloud-native environments that use agile methodologies and API-driven architectures, microservices, containers, and serverless functions. Application security testing is evolving to meet the speed at which DevOps teams operate. DevSecOps teams are challenged with how to make sense of the noise their AppSec tools generate once they've been automated into DevOps pipelines.

Processes and tools are more fast-paced and rely on integration and automation to maintain efficiency throughout the software development life cycle. A new approach to DevSecOps is required addressing a change in the security mindset. How do CISOs achieve this without the buy-in from stakeholders?

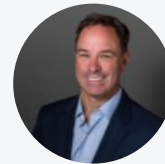| CHAIR	PANELISTS			
Jim Routh CSO, Board Member, Advisor & Investor Transmit Security	**Leo Cunningham** Former CISO Flo Health Inc.	**Anthony Gonzalez** CISO NA QBE North America	**Nick Diieso** Director, Global Head of Operational Risk Citi	**Jason Stutt** CRO ArmorCode

---

PANEL   2:55 PM-3:45 PM

The Greatest Fears?

The biggest fear is not the technology, it is the potential of human error that could expose your organization to a cyberattack. The majority of CISOs agree that an employee carelessly falling victim to a phishing scam is the most likely cause of a security breach. Most also agree that they will not be able to reduce the level of employee disregard for information security. Identity security is business essential for modern enterprises, but the ability to do it effectively has moved well beyond human capacity. How do we guard against human error without limiting employee efficiency and productivity?

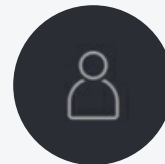| CHAIR	PANELISTS			
Jim Routh CSO, Board Member, Advisor & Investor Transmit Security	**Shamla Naidoo** Head of Cloud Strategy & Innovation Netskope	**Ben Cody** SVP Product Management SailPoint Technologies Inc	**Anna Thomas** Director Operations & Technology Transformation Citibank	**Scott Dillon** CEO, Digital Evangelist, Board Advisor & Investor

---

Networking Break   3:50 PM-4:05 PM

PANEL   4:15 PM-5:10 PM

Security Controls: Measuring Efficacy for the Business Growth

The industry is spending record amounts on cybersecurity tooling, but somehow CISOs still are at times left scrambling to respond to the vulnerabilities like Log4j. Assuming that these types of critical and far-reaching events are inevitable, how can CISOs further improve their organization's preparedness for future cyberattacks?

This panel will discuss potential strategies for determining the critical security controls - both technology and behavioral - that can minimize cyber-risks and give the organization the competitive advantage to grow and innovate. We will explore frameworks for measuring the efficacy of cybersecurity investments, and KPIs that show the board the investment is safeguarding the company's digital infrastructure for the long term.

CHAIR

Ben Halpert
Founder & CEO
CISO Horizon

PANELISTS

Scot Miller
SVP & CISO
Mr. Cooper

Susan Koski
CISO
PNC

Alex Shulman
Managing Director,
Cloud Security
Ernst & Young

**David Geevaratne -
NO LONGER W/
COMPANY!!!**
SVP of Sales
Uptycs

PANEL

5:15 PM-6:10 PM

Detect Imposters and Rogue Insiders in Business Applications

The risks posed by rogue insiders and external attackers make application detection a massive pain point for enterprises, especially in regards to core business applications. Examples are a fraudster's takeover of a checking account via social engineering, or a customer service agent modifying an insurance policy to add themselves as a beneficiary, or a salesperson downloading a report of all customers before switching to work at a competitor. This panel will explore the growing need for application detection and the challenges posed by current rule-based techniques.
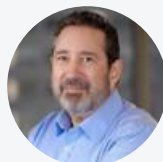
CHAIR

Ben Halpert
Founder & CEO
CISO Horizon

PANELISTS

Michael Gross
Manager,
Cybersecurity
Intelligence
Cleveland Clinic

Laura Deaner
CISO
Northwestern Mutual

Charles Blauner
CISO
Cyber Aegis

Doron Hendler
CEO & Co-Founder
RevealSecurity

DISRUPTOR

6:15 PM-6:30 PM

The Road to SaaS Governance: Centralize & secure application management

The acceleration of cloud adoption has reached a point where today, 39% of all applications are SaaS. Because of decentralization and a low-friction model of payment and usage, SaaS applications will continue to replace on-prem software rapidly. But with decentralization comes chaos. Governance & management around SaaS is still largely lagging behind. CIOs and CISOs currently don't have visibility or control, leading to Shadow IT & disjointed IT (SaaS) Ops.

To help IT leaders get a hold of their SaaS stack, we'll present a full-fledged discovery and management framework that seamlessly integrates control systems for SaaS within the modern IT technology landscape.

PANELISTS

Todd Dekkinga
CISO
Zluri

Reception

6:30 PM-7:30 PM

TOGETHER WITH