C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

CISO Think Tank

SPEAKERS

David Levine
VP Corporate & CSO
Ricoh Americas Corporation

Robert Smith
Field CISO
Noname Security

Adolph Barclift
CISO
Five Star Bank

Ken Foster
VP of IT Governance, Risk and Compliance
FLEETCOR

John Wheeler
CISO
Cognizant

Mat Mathews
Vice President of Technology Services
Boys & Girls Clubs of America

Michael Owens
BISO
Equifax

Tony Hadfield
Sr Director of Solution Architects
Venafi

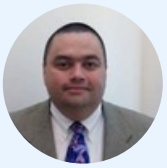
Ben Halpert
CISO
Groupon

Elizabeth Mavetz
President
ISACA - Atlanta

Bill Besinger
Director of Sales, North America
Cynet

Steve Zalewski
Former CISO
Levi Strauss & Co.

Tamar Bar Ilan
Co-founder & CTO
Cyera.io



Kelvin Arcelay
SVP, Information Security & IT Risk Management
EVO Payments International

Deena Swatzie
SVP, Corporate Cyber Strategy Leader
Truist

C VISION INTERNATIONAL

Click Here to Register

April 20, 2022

Eastern Time

Welcome & Registration

12:00 PM-12:50 PM

KEYNOTE

Application Security in a DevOps, Cloud and API World

12:50 PM-1:35 PM

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

Robert Smith
Field CISO
Noname Security

PANEL

Zero Trust Network

1:40 PM-2:35 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 2024. 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 2022 more than any other year?
As organizations race toward digital transformation, the reliance on secure machine-to-machine communications has caused an exponential increase in the number of SSL/TLS certificates organizations need to manage and protect. With InfoSec teams struggling to extend necessary certificate management and security, certificate-related outages are on the rise. When sites, services and applications fail due to expired or misconfigured certificates, these failures cause time-consuming, expensive and even job threatening challenges.

CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Co.

PANELISTS

Ken Foster
VP of IT Governance, Risk and Compliance
FLEETCOR

Adolph Barclift
CISO
Five Star Bank

Tony Hadfield
Sr Director of Solution Architects
Venafi

Elizabeth Mavetz
President
ISACA - Atlanta

Networking Break

2:35 PM-2:50 PM

PANEL

Supply Chain Technology

2:50 PM-3:35 PM

Many large enterprises in today's fiercely competitive climate look toward optimizing its supply chain to increase business scale and agility. By harnessing a combination of technologies like artificial intelligence, machine learning, and predictive analytics, companies can automate and create new customer experiences that increase satisfaction and boost sales. Gaps remain in supply chain cyber security even as digitalization accelerates. By doing so, companies are left vulnerable to the growing risk of a cyber-attack. There is no shortage of stories illustrating the dangers of lax cyber security, with the biggest attacks able to utterly paralyze an operation and cause millions in losses. Despite this obvious danger, efforts to improve cyber security are progressing slowly. Future risks to the supply chain will involve software, cloud-based infrastructures, and hyper-converged products, rather than simply hardware. Even after many years of experience, capable CISOs find they may not be equipped to overcome the cybersecurity concerns that arise from building control contractors.

CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Co.

PANELISTS

David Levine
VP Corporate & CSO
Ricoh Americas Corporation

John Wheeler
CISO
Cognizant

Deena Swatzie
SVP, Corporate Cyber Strategy Leader
Truist

DISRUPTOR

Native Vs. Open: Choosing the right XDR for your

3:40 PM-3:55 PM

organization

Extended Detection and Response (XDR) continues to be one of the most discussed technologies in cybersecurity. XDR promises far better security outcomes at a lower cost than the current security stack approaches most that most larger enterprises currently have in place. One sticky point that keeps arising in the XDR discussion has to do with the different technology approaches XDR providers rely upon to deliver platform capabilities. Most of us have heard the two primary approaches mentioned – Native XDR and Open XDR – but may be confused by all the vendor and analyst messaging. Join our discussion for an overview of these XDR approaches to better understand the benefits and shortcomings of each to help determine which option is better for your organization.

PANELISTS

Bill Besinger
Director of Sales, North America
Cynet

Networking Break

3:55 PM-4:10 PM

PANEL

Cloud Data Security

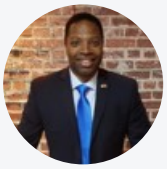
4:10 PM-5:05 PM

According to Gartner, 79% of companies have experienced at least one cloud data breach during the pandemic. But the migration of critical business data to the cloud shows no sign of slowing. In fact, it's accelerating. Yet, despite powerful trends and mounting threats, traditional data security has simply not kept pace with the cloud. Security teams still struggle to even understand the reality of what sensitive data they have in the cloud and its associated risks. This is not a sustainable status quo. Data is increasingly business' most valuable asset. And until organizations can align around a shared Data Reality, cloud security will remain several steps behind intensifying security threatens and tightening data regulations.

CHAIR

Steve Zalewski
Former CISO
Levi Strauss & Co.

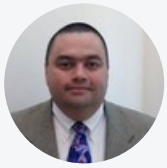
PANELISTS



Michael Owens
BISO
Equifax

Ben Halpert
CISO
Groupon

Tamar Bar Ilan
Co-founder & CTO
Cyera.io



Kelvin Arcelay
SVP, Information Security & IT Risk Management
EVO Payments International

Closing Remarks

5:05 PM-5:15 PM

Cocktail Hour

5:15 PM-6:30 PM

IN PARTNERSHIP WITH