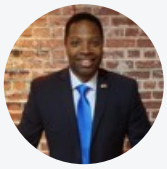
C VISION INTERNATIONAL

AGENDA

The Future of IT and Cybersecurity

CISO & CIO Think Tank

SPEAKERS



Michael Owens
BISO
Equifax



Ben Halpert
Field CISO
SHI



Charles Andry
Chief Architect
Jackson Healthcare



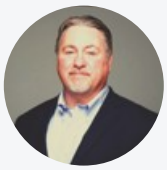
Adolph Barclift
Former CISO
Five Star Bank



Tamika Bass
Head of Cybersecurity Director (CISO)
Gannett Fleming



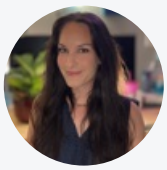
Irene Thong
Global IT & Cybersecurity Executive
Printpack Inc



Robert Sheesley
CIO
Wrench Group



Rahul Ganorkar
SVP IT
Randstad North America



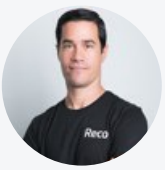
Emily Austin
Security Research Manager, Senior Researcher
Censys



Sam Krishnamurthy
CTO
Crawford



Mike Takla - NO LONGER W/ COMPANY!!!
VP of Sales
RevealSecurity



Ofer Klein
Co-Founder & CEO
Reco



Adolph Barclift
Former CISO
Mergence Global

Click Here to Register

October 19, 2023

Eastern Time

Registration

9:30 AM-10:15 AM

Morning Networking

10:15 AM-11:15 AM

Opening Remarks

11:00 AM-11:15 AM

VISION KEYNOTE PANEL
Bridging the Gap Between IT and the Business

11:10 AM-11:55 AM

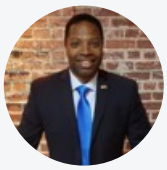
Bridging the gap between business and technology is not easy and requires discipline and balance between technology, people, and the business. For so many organizations today, technology is the business. Technology needs to be understood as a critical enabler in every part of the organization from the 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

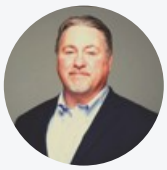


Ben Halpert
Field CISO
SHI

PANELISTS



Michael Owens
BISO
Equifax



Robert Sheesley
CIO
Wrench Group



Irene Thong
Global IT & Cybersecurity Executive
Printpack Inc



Rahul Ganorkar
SVP IT
Randstad North America

Cyversity Mentorship

11:55 AM-12:00 PM

Lunch & Networking

12:15 PM-1:15 PM

DISRUPTOR

1:15 PM-1:30 PM

Detecting Imposters and Rogue Insiders in SaaS Applications

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. In this session we will explore the growing challenge of SaaS application detection, explain why current detection solutions are usually ineffective, and share solutions using real customer examples.

SPEAKER



Mike Takla - NO LONGER W/ COMPANY!!!

VP of Sales

RevealSecurity

PANEL

Supply Chain

1:25 PM-2:10 PM

Supply chain attacks pose a significant risk to organizations that rely on third-party vendors or suppliers. These attacks can lead to data breaches, theft of intellectual property, and disruptions to the supply chain. To address this threat, companies are implementing new supply chain-specific security tools and processes. For example, they are performing risk assessments, implementing controls to mitigate vulnerabilities, and requiring vendors and suppliers to comply with specific security standards. Additionally, some companies are exploring the use of blockchain technology to track goods and prevent fraud.
Overall, securing the supply chain requires a coordinated effort from all stakeholders. By implementing best practices and innovative solutions, companies can better protect their data and systems from cyber threats.

CHAIR

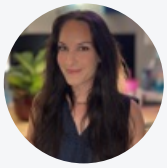


Ben Halpert
Field CISO
SHI

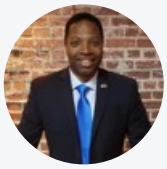
PANELISTS



Tamika Bass
Head of Cybersecurity Director (CISO)
Gannett Fleming



Emily Austin
Security Research Manager, Senior Researcher
Censys



Michael Owens
BISO
Equifax

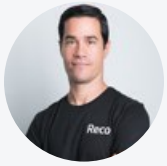
DISRUPTOR

2:15 PM-2:30 PM

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

Networking Break

2:30 PM-2:50 PM

PANEL

The Promising Future of Artificial Intelligence (AI): Opportunities and Challenges Ahead

2:50 PM-3:35 PM

The potential of Artificial Intelligence (AI) is vast, as it is now being utilized across all industries. With the combination of machine learning, AI has made significant improvements in the field of cybersecurity. Automated security systems, natural language processing, face detection, and automatic threat detection are some examples of how AI is revolutionizing cybersecurity. However, AI is also being used to create intelligent malware and attacks, which can bypass the most up-to-date security protocols, making it a double-edged sword. On the positive side, AI-enabled threat detection systems have the ability to predict new attacks and immediately notify administrators in case of a data breach.

CHAIR



Ben Halpert
Field CISO
SHI

PANELISTS



Adolph Barclift
Former CISO
Five Star Bank



Sam Krishnamurthy
CTO
Crawford

Closing Remarks & Raffle Giveaway

3:35 PM-3:45 PM

Cocktail Hour

3:45 PM-4:45 PM

TOGETHER WITH

grip REVEAL censys sentra reco