C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

CISO Think Tank

SPEAKERS

Neil Thacker
CISO (EMEA) & DPO
Netskope

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

Khadir Fayaz
SVP Digital & Technology
CBRE

Dorian Skeete
Head, Information Security
boohoo

Steven Gillham
Infrastructure Security Manager
TSB

Roben Leonard
CISO
Thames Technology

Adrian Leung
Group DPO
Equifax

Mike Backinsell
Global Deputy CISO
ManpowerGroup

Shikha Hornsey
CDIO
Crown Commercial Service

Lorraine Dryland
Global CISO
First Sentier Investors

Mike Bray
CISO
Monzo

Florian Jörgens
CISO
Vorwerk SE & Co. KG

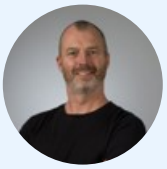
Ludwig Keyser
CISO
Rothesay

Sadiq Sani
Adviser and Senior Lecturer in Cybersecurity
University of Greenwich

Zac Warren
Chief Security Advisor, EMEA
Tanium

Bogdan Grigorescu
Senior Technical Lead, Automation
Direct Line Group

Neil Thacker
CISO (EMEA) & DPO
Netskope



Charlie Howe
VP EMEA
Cribl

Phil Scully
VP Digital & EMEA Technology
RS Group plc

Shweta Gupta
VP IT
Deutsche Bank

Saul Williams
Regional Director
Safebreach

Click Here to Register

March 30, 2023

United Kingdom Time

Welcome & Registration

10:00 AM-11:05 AM

THOUGHT LEADERSHIP

The Human Firewall: How to Create a Culture of Cyber Security?

11:05 AM-11:20 AM

When it comes to information security, many companies still focus on IT security and the technical protection of systems. Employees are often seen as the weakest link in a very complex chain, as 70% of all attacks today are aimed at people and only 30% at systems. However, this is a fallacy. Properly trained, employees can make an essential and valuable contribution to raising the overall level of security and are the most important building block of an all-encompassing security strategy. Therefore, all companies should focus on increasing the awareness of their employees. But how to build a successful awareness campaign that sensitizes employees to the topic of information security in the long term is presented in this session.

PANELISTS

Florian Jörgens
CISO
Vorwerk SE & Co. KG

VISION KEYNOTE PANEL

CXO's Role in Employee Retention

11:25 AM-12:10 PM

Over the last decade, the ability to understand and utilise existing, new and upcoming technologies has been a critical enterprise success factor. As a result, the need for capable and qualified leaders, whether front-line Analysts, mid-level Managers, or top level CXO's is at an all-time high. However, the availability of personnel with the necessary skills is sinking to an all-time low. There simply is not enough expertise to go around, or is there? In this environment, senior leaders must express creativity in their pursuit of the people, performance, and passion necessary to address this capability shortfall.

CHAIR

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

PANELISTS

Shikha Hornsey
CDIO
Crown Commercial Service

Lorraine Dryland
Global CISO
First Sentier Investors

Shweta Gupta
VP IT
Deutsche Bank

LUNCH & DISRUPTOR SHOWCASE
Lunch & Innovation Showcase

12:10 PM-1:10 PM

DISRUPTOR
The Role of Breach and Attack Simulation in Cybersecurity

12:45 PM-1:00 PM

Security control validation is a key component of compliance requirements for many organizations. But there are differing opinions about the best way to test controls, including when it should be done, how often, and what tools are most effective to support the process.

In this presentation, SafeBreach Regional Director Saul Williams makes the case for integrating continuous breach and attack simulation (BAS) as a practical approach for programmatic remediation. This presentation will explore:
BAS fundamentals and objectives
How to get the most benefit from your security controls
How BAS can inform and enhance communications with key stakeholders

PANELISTS

Saul Williams
Regional Director
Safebreach

DISRUPTOR
In Cyber Security, is Prevention Better Than The

1:05 PM-1:20 PM

Cure?

How can organisations stay ready to defend against cyber threats, so they don't have to respond in a rush?
In a world of increasingly damaging cyber attacks, organisations need effective strategies to stay ahead of threats and drive a proactive security posture. But the nature of the threats can be hard to measure. How can you manage what you don't know? How can you secure what you don't manage?
Organisations need to ask key questions. What assets do we have? What is running on our IT estates? What goes in and out of our network? These are hard questions to answer. But to keep safe, visibility is key. We need to know what we look like to an attacker if we are to defend ourselves. Only with this knowledge can we maintain readiness to respond to new and unexpected dangers.

PANELISTS

Zac Warren
Chief Security Advisor, EMEA
Tanium

PANEL

How to Optimize your Security Data and reduce SOC TCO with Data Pipelines

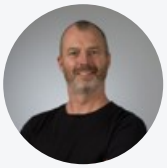
1:25 PM-2:10 PM

Securing your organisation no longer comes down to acquiring the right tools and building the best policies. Additionally, managing the flood of noisy, high volume security data means the difference between detecting a breach and missing a critical alert. Join this session to learn how data pipelines put choice and control over data back into the hands of security teams, helping get the right data, in the right formats, to the right places, all while reducing your SOC TCO

CHAIR

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

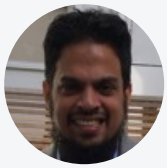
PANELISTS



Charlie Howe
VP EMEA
Cribl

Roben Leonard
CISO
Thames Technology

Florian Jörgens
CISO
Vorwerk SE & Co. KG



Khadir Fayaz
SVP Digital & Technology
CBRE

Networking Break

2:10 PM-2:30 PM

PANEL

Zero Trust Network

2:35 PM-3:20 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 2023 more than any other year?

CHAIR

Florian Jörgens
CISO
Vorwerk SE & Co. KG

PANELISTS

Neil Thacker
CISO (EMEA) & DPO
Netskope

Dorian Skeete
Head, Information Security
boohoo

Bogdan Grigorescu
Senior Technical Lead, Automation
Direct Line Group

Steven Gillham
Infrastructure Security Manager
TSB

PANEL
Bridging the Gap Between IT and the Business

3:25 PM-4:00 PM

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

Amjad Khan
VP Customer Success and Growth
NewPage Solutions

PANELISTS

Sachin Gaba
Managing Director, Head of Software Development
State Street

Sadiq Sani
Adviser and Senior Lecturer in Cybersecurity
University of Greenwich

Phil Scully
VP Digital & EMEA Technology
RS Group plc

Jon Townsend
CIO
National Trust

Networking Break

4:00 PM-4:20 PM

PANEL
The Greatest Fears?

4:25 PM-5:10 PM

The biggest fear for CISOs is often human error, typified by a distracted user that falls for a well-crafted social engineering email. Secure email gateways fail to catch business email compromises and security analysts struggle to keep up with the flood of user-reported suspicious emails. How can we truly create a culture of security while also making the best use of a cybersecurity leader's most precious resource – people?

CHAIR

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

PANELISTS

Ludwig Keyser
CISO
Rothesay

Mike Backinsell
Global Deputy CISO
ManpowerGroup

Adrian Leung
Group DPO
Equifax

PANEL
Promoting & Enabling Women in Tech to Succeed

5:15 PM-6:00 PM

How do we come together, as a group of professionals, to create and foster an inclusive tech world where all women have a role to play? We know that a major part of this is attracting and retaining talent at every level but how exactly do we do that and where can we use technology to help? Our panelists will discuss how their companies are creating more inclusive environments, the use AI tools to help uncover hidden biases, what flexibility looks like for all team members and how they are advancing women earlier and signing them up for long term success.

CHAIR

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

PANELISTS

Shweta Gupta
VP IT
Deutsche Bank

Adrian Leung
Group DPO
Equifax

Lorraine Dryland
Global CISO
First Sentier Investors

Closing Remarks & Raffle Giveaway

6:00 PM-6:05 PM

Cocktail Hour

6:05 PM-7:05 PM

IN PARTNERSHIP WITH


TANIUM
opentext™
Cybersecurity
SafeBreach
Cribl™
RED BUTTON
DDoS Experts
netskope