C VISION INTERNATIONAL

AGENDA

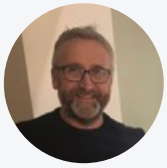
The Future of IT & Cybersecurity

CIO & CISO Think Tank

SPEAKERS

Anders Jaegerskou
Country Manager Mandiant Denmark & Norway
Google Cloud

Allan Andersen Christensen
Group VP Data Analytics & AI
DEAS Group



Roy Matthews
VP Cyber Security
Pandora

Bruno Mariano da Cunha
Director IT Architecture, Infrastructure and Operations
Getinge

Carsten Falshøj
Owner of Cyber Security Consulting and former CISO
Hempel A/S

Kasper Adelhøj
CTO, Audit & Assurance Denmark
Deloitte

Rami El Outa
Regional IT Director - Infrastructure, Solutions and Cybersecurity
Grupo Eurofins

Patrick Morgan Rudbøg
CISO
Dansk Sundhedssikring

Janni Lee Bang Brodersen
CISO
University of Southern Denmark

Sharon Givskov
Head Of Security
Coor

Jacob-Steen Madsen
CIO
University of Southern Denmark

Dado Dizdar
Regional Enterprise Account Manager
KnowBe4

Thomas B. Zuliani
Sr Director, Global Chief IT Security Services Officer
GEA Group

Bo Falk
BISO
ISS

Tom Hornung
Lead Solutions Architect, EMEA
Synack, Inc.

Kristoffer H?g
Head of Customer Engineering
Google Cloud

Jason Stutt
CRO
ArmorCode

Dirk-Jan van Helmond
Director of Solutions Engineering EMEA
Cloudflare

Neil Thacker
CISO (EMEA) & DPO
Netskope

Click Here to Register

October 26, 2023

Central European Time

Registration	**8:30 AM-9:00 AM**
Morning Networking	**9:00 AM-9:30 AM**
Opening Remarks	**9:30 AM-9:40 AM**

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

9:40 AM-10:10 AM

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

SPEAKER

Allan Andersen Christensen

Group VP Data Analytics & AI

DEAS Group

Poor Cyber Hygiene

10:10 AM-10:25 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

Rami El Outa

Regional IT Director - Infrastructure, Solutions and Cybersecurity

Grupo Eurofins

VISION KEYNOTE PANEL

Bridging the Gap Between IT and the Business

10:30 AM-11:15 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

Rami El Outa
Regional IT Director - Infrastructure, Solutions and Cybersecurity
Grupo Eurofins

PANELISTS

Jacob-Steen Madsen
CIO
University of Southern Denmark

Allan Andersen Christensen
Group VP Data Analytics & AI
DEAS Group

Bo Falk
BISO
ISS

Networking Break

11:15 AM-11:40 AM

DISRUPTOR

Enable Cloud Innovation at Speed with Continuous Security Testing

11:40 AM-11:55 AM

Many cloud migration projects struggle to deliver on project objectives, and most cloud migration teams aren't confident in their security posture during the transition.
Even fewer teams can communicate measurable security metrics and trends from their programs to leadership in a way that creates confidence and trust in the new solution.
Join us for a discussion on leveraging continuous security testing for cloud migration projects, and the challenges and requirements for effective continuous testing.

SPEAKER

Tom Hornung
Lead Solutions Architect, EMEA
Synack, Inc.

DISRUPTOR

12:00 PM-12:15 PM

The Most Important Shift for Cybersecurity in a Generation

We live in a fully hybrid world. The mix between personal and corporate devices and private and public services is evolving and exposes organisations to both new challenges and new risks. The pressure to converge legacy controls and do “more with less” is now at peak levels. We must therefore approach this challenge with the right strategy that fully optimises our investment in securing web and cloud whilst protecting against new threats and securing sensitive information...whilst ensuring a great user experience for our remote workforce.

Join this session to learn:

- How to build a strong plan for network and security transformation...without adding to the chaos
- Prioritisation and rationalisation tactics that can help quickly reduce and report on risk
- Critical use cases to prioritise that deliver tactical value and efficiency today

SPEAKER

Neil Thacker

CISO (EMEA) & DPO

Netskope

Lunch

12:15 PM-1:10 PM

DISRUPTOR

1:10 PM-1:25 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

Dado Dizdar
Regional Enterprise Account Manager
KnowBe4

FIRESIDE CHAT

1:30 PM-2:05 PM

A Culture of Innovation and Smarter Use of Data? That’s Digital Leadership.

Data and AI help create competitive advantage, enable agility, and can even create new business opportunities in times with fast changes. Listen to how Google Cloud enables their customers to take the next step in their digital transformation journey.

CHAIR

Rami El Outa
Regional IT Director - Infrastructure, Solutions and Cybersecurity
Grupo Eurofins

SPEAKERS

Kristoffer H?g
Head of Customer Engineering
Google Cloud

Anders Jaegerskou
Country Manager Mandiant Denmark & Norway
Google Cloud

PANEL

Ransomware

2:10 PM-2:55 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, it's important to have a response plan in place to minimize the impact of an attack if it does occur.

CHAIR

Carsten Falshøj

Owner of Cyber Security Consulting and former CISO

Hempel A/S

PANELISTS

Patrick Morgan Rudbøg

CISO

Dansk Sundhedssikring

Thomas B. Zuliani

Sr Director, Global Chief IT Security Services Officer

GEA Group

Janni Lee Bang Brodersen

CISO

University of Southern Denmark

Networking Break

2:55 PM-3:15 PM

DISRUPTOR

Streamlining Vulnerability Management for Faster Risk Reduction

3:15 PM-3:30 PM

In today's fast-evolving digital landscape, achieving comprehensive control over your organization's cybersecurity vulnerabilities is imperative. This necessitates a holistic approach that consolidates all vulnerability management efforts. By unifying your vulnerability management, you can gain a clear and comprehensive view of all potential security weaknesses across your digital assets. This comprehensive visibility enables you to apply effective risk scoring and prioritization strategies, ensuring that your limited resources are allocated to address the most critical threats first. In turn, this unification allows for more efficient and streamlined remediation processes, accelerating your efforts to reduce risk, bolster security, and safeguard your digital infrastructure from emerging threats.

SPEAKER

Jason Stutt

CRO

ArmorCode

DISRUPTOR

3:35 PM-3:50 PM

A Resilient Internet: Stronger, Leaner, Greener, Open and Interconnected

Cloud migration and sustainability goals are intrinsically linked in today's digital landscape. As organisations increasingly transition their IT infrastructure to the cloud, they not only gain operational efficiencies and scalability but can also contribute to a more sustainable future. As businesses are expanding their operations beyond geographical boundaries, global interconnectivity faces significant risks due to legislative actions and policies adopted by various countries. One of the most pressing concerns is the proliferation of data localisation laws, which require companies to store data within the borders of a specific jurisdiction. While such regulations are often enacted for reasons of data sovereignty and national security, they can hinder the smooth flow of information across borders and disrupt global interconnectivity. Compliance with these laws can lead to increased operational costs, data fragmentation, and reduced flexibility for businesses that rely on global cloud services

SPEAKER

Dirk-Jan van Helmond
Director of Solutions Engineering EMEA
Cloudflare

FIRESIDE CHAT

3:55 PM-4:30 PM

Social Engineering: New in 2023

Social engineering attacks are a growing concern for businesses and individuals alike, as cybercriminals continue to use advanced techniques to trick people into divulging sensitive information or performing actions that can lead to data breaches. In 2023, these attacks are expected to become even more sophisticated, making it increasingly challenging for individuals and businesses to identify and prevent them. To protect themselves, individuals and businesses must be vigilant and aware of these tactics. They must also implement comprehensive security measures, such as security awareness training, anti-phishing software, two-factor authentication, and access controls. Additionally, businesses must establish policies and procedures for responding to social engineering attacks, including incident response plans, data backup and recovery, and regular security assessments. By taking these proactive steps, businesses and individuals can better protect themselves from the risks associated with social engineering attacks in 2023 and beyond.

CHAIR

Rami El Outa
Regional IT Director - Infrastructure, Solutions and Cybersecurity
Grupo Eurofins

SPEAKERS

Sharon Givskov
Head Of Security
Coor

Roy Matthews
VP Cyber Security
Pandora

Closing Remarks & Raffle Giveaway	**4:30 PM-4:35 PM**
Cocktail Hour	**4:35 PM-5:35 PM**

TOGETHER WITH