C VISION INTERNATIONAL

AGENDA

The Future of IT & Cybersecurity

CXO Think Tank

SPEAKERS

Leo Cunningham
CISO
Owkin Inc

Khadir Fayaz
VP CISO, Cybersecurity
CBRE

Adrian Leung
Group DPO
Equifax

William Davies
Head of Information Security and Assurance
Government Shared Services

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

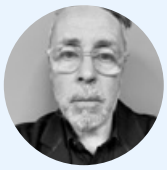
Leo Cunningham
Former CISO
Flo Health Inc.

Jimmy Jones
Head Of Security
ZARIOT

Deepak Uniyal
Head of Risk Domains
BNP Paribas

Philip Hoyer
CTO Software BU
Videojet Technologies

Steven Gillham
Cyber Security Specialist
Capital One



Simon Gooch
CIO Director of Security
Accenture

Thomas Kinsella
Co-Founder & COO
Tines

Dr. David Movshovitz
Co-Founder & CTO
RevealSecurity

Lino Gambella
Chief Technology Officer
Defenx

Richard Meeus
Director, Security Technology & Strategy
Akamai Technologies

James Hughes
Vice President - Sales Engineering & Enterprise CTO EMEA
Rubrik

Nana-Ampofo A.
Enterprise Security Architect - SecOps
Cortex - Palo Alto Networks

David Lomax
Senior Systems Engineer
Abnormal Security

Click Here to Register

www.cvisionintl.com

October 18, 2022

United Kingdom Time

Welcome & Registration

12:30 PM-1:00 PM

KEYNOTE

The Future of SecOps?

1:20 PM-1:45 PM

What to Expect

Artificial Intelligence, Machine Learning, Automation - these terms get bandied about a *lot* in modern technology circles. At Palo Alto Networks we believe it will be the rise of the Centaurs [Humans augmented by Machine technology] and *not only* The Rise Of the Machines that will reshape Security Operations.

Join our speaker on this 30 minute tour of the world of AI, ML and automation and learn how the rise of the centaurs will change everything in SecOps as we know it

PANELISTS

Nana-Ampofo A.
Enterprise Security Architect - SecOps
Cortex - Palo Alto Networks

DISRUPTOR

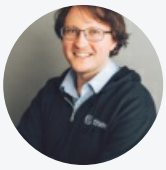
Staff Shortages

1:40 PM-1:55 PM

We have always suffered from a shortage of good security employees. Is it any wonder we have trouble recruiting and motivating good security people?

The shift to work from home that was accelerated by the start of the COVID pandemic has resulted in a sharp increase in cyberattacks. Companies of all sizes were simply unprepared for the sudden and massive switch to remote work. As a result, data exfiltration and leakage has increased most sharply. Phishing, ransomware, VPN breaches and other security events have all shot up as well. Inevitably the sheer persistence of these attacks led to more hours of work needed leading to staff burnout, often more severe at organizations that are still trying to fight present battles with yesterday's tools. Many believe that a new approach is needed to prevent cybersecurity staff burnout increasing the demand for more automated solutions since yesterday's tools are not nearly as successful at stopping attacks as state-of-the-art methods, in addition to increasing the workload for cybersecurity staff, using them also exposes organizations to major losses.

PANELISTS



Thomas Kinsella
Co-Founder & COO
Tines

Networking Break

1:55 PM-2:10 PM

FIRESIDE CHAT

Have You Been Breached Yet?

2:15 PM-3:00 PM

Preventing and Protecting Your Organisation against an Inevitable Cyber Security Breach.
Fallen victim to a data breach yet? If not, your organisation is one of the lucky ones - for now. Cyber attackers are using ever more sophisticated attempts to execute cyber-attacks on a daily basis. Realistically, it's unlikely that an organisation can swerve an attack without robust cyber security measures already in-place to prevent, detect and mitigate cyber threats.
Hear from Akamai's EMEA Director of Security Technology and Strategy Richard Meeus and Defenx's Chief Technology Officer:
From DDoS & Zero Day vulnerabilities to phishing - understand the common attacks in the cyber threat landscape.
Discover cyber security models and strategies to protect your organisation should it fall victim to an attack.
Learn how you can provide your users with risk-free access to applications and services.

CHAIR

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

PANELISTS

Richard Meeus
Director, Security Technology & Strategy
Akamai Technologies

Lino Gambella
Chief Technology Officer
Defenx

PANEL

Ransomware/Extortionware

3:05 PM-4:00 PM

CISOs face a huge headache trying to understand how to know when they were attacked, what data attackers have corrupted? How quickly can they recover from the attack? And do they have to pay a ransom to get the data back?
Ransomware remains a significant challenge for companies, not simply because it has become ubiquitous, but also because of the significant impact a single ransomware attack may have on a company and every other company or customer that relies on that company. Cybersecurity and risk management have always been vital for the flow of any business. However, the current condition of the global supply chain makes it exceptionally vulnerable to severe damage from an attack more so than usual. When the supply chain is barely getting by, criminals are more likely to assume they have leverage over businesses. A ransomware attacker may be more brazen and

exercise higher demands than they might have a few years ago.

CHAIR

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

PANELISTS

James Hughes
Vice President - Sales Engineering & Enterprise CTO EMEA
Rubrik

Leo Cunningham
Former CISO
Flo Health Inc.

William Davies
Head of Information Security and Assurance
Government Shared Services

Networking Break

4:00 PM-4:15 PM

PANEL

Monitoring Authenticated Users in Business Applications to Detect Imposters and Rogue Insiders

4:15 PM-5:10 PM

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. External attackers leverage stolen credentials to impersonate an insider and connect to applications, while at the same time insiders are not sufficiently monitored in SaaS and home-grown 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. Current detection solutions are application-specific and in most cases ineffective, therefore requiring a new approach. However, the problem goes beyond detection itself, because even after the enterprise receives a complaint or is otherwise suspicious, investigating these suspicions usually consists of manual sifting through tons of log data from multiple sources, which is time consuming and ineffective in many cases.
This panel will explore the growing need for application detection and the problems with current rule-based techniques for application monitoring. Panelists will discuss potential solutions using real examples, such as the analysis of user journeys within the application and across applications to accurately detect malicious activities performed by authenticated users.

CHAIR

Cameron Brown
Director - CyberSecurity - Risk Advisory
Deloitte

PANELISTS

Dr. David Movshovitz
Co-Founder & CTO
RevealSecurity

Steven Gillham
Cyber Security Specialist
Capital One

Adrian Leung
Group DPO
Equifax

Jimmy Jones
Head Of Security
ZARIOT

Philip Hoyer
CTO Software BU
Videojet Technologies

DISRUPTOR

Key Considerations for Choosing the Right Cloud Email Security Platform

5:15 PM-5:30 PM

Email is both a necessary communication medium, and the most vulnerable area for an attack. Year after year, adversaries find success in abusing email to gain a foothold into an organization—deploying malware, leaking valuable data, or stealing millions of dollars. Unfortunately, email threats are only growing in number. Business email compromise accounts for 35% of all losses to cybercrime, and the Verizon Data Breach Investigations Report holds that phishing remains the top entry point for breaches - a position it has held for years. Does that mean email is doomed, and we should give up? Quite the opposite. But the shift to cloud email requires one major thing: a shift to cloud email security.

Attend the Abnormal Security session for answers to your most pressing questions, including:

What are modern email threats, and how are they different from legacy attacks?

Which email threats are most concerning, and how can we defend against them in the cloud environment?

Which technical capabilities are required when protecting cloud email?

How can cloud email security platforms detect the most dangerous attacks?

PANELISTS

David Lomax
Senior Systems Engineer
Abnormal Security

Closing Remarks

5:30 PM-5:35 PM

Cocktail Hour

5:35 PM-6:35 PM

IN PARTNERSHIP WITH

tines · DEFENX BV TECHGROUP · Akamai · rubrik · paloalto NETWORKS · CORTEX BY PALO ALTO NETWORKS · Panorays · Reveal security · Infoblox · Abnormal