

Post event report



The 12th e-Crime & Cybersecurity Congress in Abu Dhabi

21st September 2022 | Abu Dhabi, UAE

Principal Sponsor



Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



“ I would like to thank you all for organising this very successful conference. ”

Cyber Security Manager, International Media Investments Holdings

“The conference was more than wonderful, and the speakers had a lot of experience in the areas they handled. ”

Legal Translator, Abu Dhabi Police GHQ

“Thank you for the opportunity to attend e-Crime Cybersecurity Congress. It was very informative, great place to meet industry experts and share knowledge. ”

Fraud Prevention Officer, Etihad Aviation Group

“ Very well organised and pleasant to attend from the beginning till end. The seminar exceeded my expectations in terms of AI/ML cybercrime threats and how to deal with it. I have a complete new understanding of cybersecurity, innovation and technologies. All presenters were really knowledgeable and gave us amazing information in only 20 minutes. It was a terrific use of my time. Thank you very much! ”

AML and Compliance Officer, Lari Exchange

Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



Speakers

Abdulla Al Dhaheri, Cybersecurity Specialist, **UAE Government**

Khaled Al Tenejji, Cybersecurity Head, **ENOC**

Ramy AlDamati, Co-founder/Chief Strategy Officer (CSO), **AlBrza**

Hussain Alkhalsan, CISO, **Zand**

Bilal Baig, Technical Director, MEA, **Trend Micro**

Nabil Bousseham, Team Lead Solutions Architecture, EMEA North & Middle East, **Veracode** on behalf of **Green Method**

Michael Byrnes, Director, Solutions Engineer iMEA, **BeyondTrust**

Aloysius Cheang, Chief Security Officer, **Huawei UAE**

Sam Clever, CEO & Founder, **Nostraverse**

Peter Craig, Director of Product Marketing – Cybersecurity, **Human Security**

Renato de Castro, Executive Director, **RMA Advisory**

Andrew de Lange, Solutions Consultant, **Anomali**

Alaa Abu Gharbieh, Regional Sales Manager – META, **Cofense**

Abhi Ghosh, Sales Director UAE, **Synack**

Cumai A. Housn, Co-founder, **Biennale.io**

Shafiullah Ismail, CISO, **Mubadala Capital**

Ayoub Jaouani, Sales Engineer – MEA, **Malwarebytes**

Thabet Khamis, Director of Information Security, **Central Bank of the UAE**

Ben Kite, Senior Defence and Intelligence Adviser, **Kearney**

Philippe Lopez, Regional Chief Security Officer, Eastern Europe, Middle East & Africa, **Mastercard**

Tom McVey, Solution Architect, **Menlo Security**

Aditya Modha, Security Researcher & Cloud Security Consultant, **Safe Security**

Parthasarathy Pillairkulam, GCISO, **Leading Bank MENA**

Hamid Qureshi, Territory Sales Manager, Middle East and Africa, **Entrust**

Dee Richartz, VP of Sales EMEA, **Binalyze**

Ensar Seker, VP of Research, Advisory Information Security Officer (CISO), **SOCRadar**

Bader Shaath, Solutions Engineer, **Cloudflare**

Hussein Shafik Bahgat, Regional Information Security Risk Officer (CISRO), Africa and Middle East & UAE, **Standard Chartered Bank**

Zaheer Shaikh, Chief Information Security Officer, **Al Maryah Community Bank LLC**

Shawn (Shakthi Shankar RM), Business Development & Customer Success, **ManageEngine**

Vikalp Shrivastava, Global CISO, **Kerzner International**

Gopan Sivasankaran, General Manager – META, **Secureworks**

Adnan Taha, Director – Middle East, **CybelAngel**

Rajesh Yadla, Head of Information Security, **Al Hilal Bank**

Key themes

Securing the technologies of the future

Reining in BigTech

Embracing risk management

From cybercrime to cyberwar

From smart machines to smart cities – securing the IoT

The perimeter is dead – that is not just hype

Securing digital currencies

Getting real about automation, AI and the rest

Keeping citizens safe

All aboard the Cloud

Developing the next generation of security leaders

The rise and rise of effective cybersecurity regulation

Who attended?



Cyber-security

We have a 15-year track record of producing the events cyber-security professionals take seriously



Risk Management

We attract senior risk officers with responsibility for information risk assessment and mitigation



Fraud, Audit, Compliance

We provide the go-to events for fraud prevention and compliance owners at the world's key corporates



Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority

Agenda					
08:00	Registration & networking				
08:50	Chairman's welcome				
09:00	Cybersecurity in Fintech Thabet Khamis , Director of Information Security, Central Bank of the UAE <ul style="list-style-type: none"> • UAE regulation development • CBUAE Cybersecurity Center of Excellence • Information sharing lesson learned and best practices • Banking sector cybersecurity simulation exercises 				
09:20	Defence-in-Concert: Evolving your SecOps strategy to ensure a robust cyber-defence through context and collaboration Gopan Sivasankaran , General Manager – META, Secureworks What you'll learn: <ul style="list-style-type: none"> • Why 'more security layers' doesn't necessarily equal a stronger defence for your organisation • How to gain better visibility, context, and collaboration across your IT ecosystem • Ways to modernise your security operations and improve threat detection and response 				
09:40	Zero Trust: Getting least privilege right, finally Michael Byrnes , Director, Solutions Engineer iMEA, BeyondTrust <ul style="list-style-type: none"> • What is behind the concept of Zero Trust • The goals of Zero Trust • Roadblocks to Zero Trust (legacy architectures and technologies) • How Privileged Access Management aligns with and enables Zero Trust 				
10:00	Cybersecurity attacks on new web 3 technologies Abdulla Al Dhaheri , Cybersecurity Specialist, UAE Government <ul style="list-style-type: none"> • Metaverse cybersecurity threats • The blockchain ecosystem and ways to secure new technologies • Transformation of attacks from web 2 to web 3 				
10:20	Education Seminars Session 1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%; vertical-align: top;"> Cloudflare Mantis – the most powerful botnet to date Bader Shaath, Solutions Engineer, Cloudflare </td> <td style="width: 25%; vertical-align: top;"> Entrust Securing digital transformation Hamid Qureshi, Territory Sales Manager, Middle East and Africa, Entrust </td> <td style="width: 25%; vertical-align: top;"> ManageEngine Embracing Zero Trust security: Privileged Access Management deep dive Shawn (Shakthi Shankar RM), Business Development & Customer Success, ManageEngine </td> <td style="width: 25%; vertical-align: top;"> Menlo Security The next class of browser-based attacks Tom McVey, Solution Architect, Menlo Security </td> </tr> </table>	Cloudflare Mantis – the most powerful botnet to date Bader Shaath , Solutions Engineer, Cloudflare	Entrust Securing digital transformation Hamid Qureshi , Territory Sales Manager, Middle East and Africa, Entrust	ManageEngine Embracing Zero Trust security: Privileged Access Management deep dive Shawn (Shakthi Shankar RM) , Business Development & Customer Success, ManageEngine	Menlo Security The next class of browser-based attacks Tom McVey , Solution Architect, Menlo Security
Cloudflare Mantis – the most powerful botnet to date Bader Shaath , Solutions Engineer, Cloudflare	Entrust Securing digital transformation Hamid Qureshi , Territory Sales Manager, Middle East and Africa, Entrust	ManageEngine Embracing Zero Trust security: Privileged Access Management deep dive Shawn (Shakthi Shankar RM) , Business Development & Customer Success, ManageEngine	Menlo Security The next class of browser-based attacks Tom McVey , Solution Architect, Menlo Security		
11:00	Networking break				
11:30	FINANCIAL INSTITUTIONS PANEL DISCUSSION Hussain Alkhalsan , CISO, Zand; Hussein Shafik Bahgat , Regional Information Security Risk Officer (CISRO), Africa and Middle East & UAE, Standard Chartered Bank; Rajesh Yadla , Director Head of Information Security, Al Hilal Bank; Zaheer Shaikh , Chief Information Security Officer, Al Maryah Community Bank LLC; Parthasarathy Pillairkulam , GCISO, Leading Bank MENA <ul style="list-style-type: none"> • What are the most worrying threats you see against financial institutions? • How do new resilience regulations help in the battle against cybercriminals? • Does cybersecurity fit naturally into the three lines of defence model? • How secure are the market infrastructures upon which the financial institutions rely (e.g. payment systems like SWIFT or Fedwire or CHAPs or even central banks)? • Third-party dependency • Should the industry be collaborating much more to strengthen the entire system, as well as themselves? In particular, given the shared dependence on unregulated providers (Cloud, telco, core internet infrastructure etc.), and given shared exposure to new risks coming from digital assets, isn't collaboration almost more important than individual action? 				
11:50	Securing the modern enterprise using a cloud-native security platform Nabil Bousselham , Team Lead Solutions Architecture, EMEA North & Middle East, Veracode on behalf of Green Method In this talk, you will learn how a cloud-native security platform can help you manage the security programme of a growingly complex modern enterprise. This session will cover: <ul style="list-style-type: none"> • How a unique approach to continuously scanning cloud native applications real estate can enable your development teams to rapidly deliver new value and business outcomes • The importance of customised architecture – because no two DevSecOps programmes are the same • How to get cloud-native security easily integrated into your existing workflow 				
12:10	What the 'hack' is going on? Bilal Baig , Technical Director, MEA, Trend Micro <ul style="list-style-type: none"> • An overview of the threats in the pandemic and predictions for 2022 				

Agenda

12:30	How sophisticated bots are impacting your digital transformation		
	<p>Peter Craig, Director of Product Marketing – Cybersecurity, HUMAN Security</p> <p>Sophisticated bots can mimic human behaviour and are used in three out of four cyber-attacks, but they work differently from conventional threats. In this session, we'll explore:</p> <ul style="list-style-type: none"> How bot attacks contaminate digital transformation trends including automation, data analytics, and application architectures How you can optimise your security and bot management strategy and adopt new approaches to detect and counter sophisticated bots The limitations of WAFs and CAPTCHAs Case studies where organisations solved these challenges 		
12:50	Education Seminars Session 2		
	<p>Anomali King of the jungle Andrew de Lange, Solutions Consultant, Anomali</p>	<p>Cofense Adaptive email security architecture: Moving from incident response to continuous response Alaa Abu Gharbieh, Regional Sales Manager – META, Cofense</p>	<p>CybelAngel Exposed doors and lost keys: Gaining visibility across your digital footprint Adnan Taha, Director – Middle East, CybelAngel</p>
			<p>Synack Hacking for the greater good: Using hackers to beat hackers Abhi Ghosh, Sales Director UAE, Synack, and Aditya Modha, Security Researcher & Cloud Security Consultant, Safe Security</p>
13:30	Lunch break		
14:30	EXECUTIVE PANEL DISCUSSION CISO priorities for 2023		
	<p>Aloysius Cheang, Chief Security Officer, Huawei UAE; Khaled Al Teneiji, Cybersecurity Head, ENOC; Philippe Lopez, Regional Chief Security Officer, Eastern Europe, Middle East & Africa, Mastercard; Shafiullah Ismail, CISO, Mubadala Capital; Vikalp Shrivastava, Global CISO, Kerzner International</p> <ul style="list-style-type: none"> Data privacy or security? How will companies view 'security' in the post-pandemic world? Hybrid working: problem solved or problem postponed? The issue of 'basic' cyber-hygiene (or 'why can't we stop ransomware?') Have the security implications of Cloud been exaggerated? The future of the security stack: insource/outsource/reduce number of solutions/rely on large application and infrastructure providers more Reining in the costs of cybersecurity 		
14:50	Lessons learned from multibillion-dollar ransomware empires		
	<p>Ensar Seker, VP of Research, Advisory Information Security Officer (CISO), SOCRadar</p> <ul style="list-style-type: none"> How ransomware groups evolved and built multi-billion-dollar crime 'business' ecosystems What percentage of the million-dollar ransom request is paid after negotiations (w/ real-life examples) TTPs of most active ransomware groups How to mitigate ransomware risk with early-warning cyber-threat intelligence methodologies 		
15:10	Education Seminars Session 3		
	<p>Binalyze The growing role of enterprise forensics in resilient incident response strategies Dee Richartz, VP of Sales EMEA, Binalyze</p>	<p>HUMAN Security The phases of account takeover (ATO) and how to stop them Peter Craig, Director of Cybersecurity Product Marketing, HUMAN Security</p>	<p>Malwarebytes Incident response in the age of ransomware and data protection Ayoub Jaaouani, Sales Engineer – MEA, Malwarebytes</p>
15:50	Networking break		
16:20	Organisational approaches to cybersecurity		
	<p>Ben Kite, Senior Defence and Intelligence Adviser, Kearney</p> <p>In the new digital world, our livelihoods are getting more dependent and digital than ever before. Our critical resources, including public services, healthcare, energy, and transportation are all online. And threat actors know this; taking down a large supply chain or critical power grid can cause significantly more chaos than cyber-attacks of the past. By creating a sustainable pipeline of cybersecurity talent we might change the world.</p> <ul style="list-style-type: none"> Defining cybersecurity skills Bridging the widening cybersecurity skills gap How to cultivate cybersecurity talent Lessons from the global response 		
16:40	Benefits of DevSecOps		
	<p>Rajesh Yadla, Head of Information Security, Al Hilal Bank</p> <ul style="list-style-type: none"> Automation suitable for modern development A repeatable and robust process Cost-effective software development process Proactive security approach Identify and fix security vulnerabilities while coding 		
17:00	EXECUTIVE PANEL DISCUSSION Securing the metaverse		
	<p>Cumai A. Housn, Co-founder, Biennale.io; Sam Clever, CEO & Founder, Nostraverse; Ramy AlDamati, Co-founder/Chief Strategy Officer (CSO), AlBrza; Renato de Castro, Executive Director, RMA Advisory</p> <p>A world in which VR and AR merge to create a version of the web in which we, in the form of avatars, can work, play, shop and socialise as if you're actually there sounds great. Or not. But it creates a host of cybersecurity issues and businesses like banks are already there. So, this panel will look at:</p> <ul style="list-style-type: none"> Identity and access management – securing the avatar The implications of payment mechanisms and blockchain inside the metaverse Social engineering in the metaverse Biometric hacking and securing biometric data Securing AR and VR headsets Privacy without a perimeter or geographic borders: relying on the platform? 		
17:20	Conference close		

Education Seminars	
<p>Anomali</p> <p>King of the jungle</p> <p>Andrew de Lange, Solutions Consultant, Anomali</p>	<p>It is a well-known fact that the lion is the king and the apex predator of its domain. For the king to remain in control of their kingdom, they need a strong pride and knowledge of their surroundings. The same applies for SOC teams today.</p> <p>Join Andrew de Lange, Technical Director for Anomali to hear more about:</p> <ul style="list-style-type: none"> • The job of the SOC, and the size of the digital jungle they need to be the Kings of, is often unmanageable • The several factors that take the role of king away from SOC teams. Things like MTD (Mean time to Detect), MTR (Mean time to Respond), network blind spots, and many more factors create too much noise to resolve a problem effectively • A demonstration on how SOC teams can take back control of their jungle, to act, resolve, and continuously defend against the predators, not in weeks, days, hours, or minutes, but in mere seconds by operationalising threat intelligence in the most effective manner with Anomali tools
<p>Binalyze</p> <p>The growing role of enterprise forensics in resilient incident response strategies</p> <p>Dee Richartz, VP of Sales EMEA, Binalyze</p>	<p>There is a new breed of digital forensics solutions that are lightning fast, remote, scalable, automated and integrated. They are dramatically changing when, where and how forensic visibility can be leveraged, in traditional investigations, but also for proactive threat hunting and incident response.</p> <p>During the session, you will learn:</p> <ul style="list-style-type: none"> • How enterprise forensics is disrupting the traditional digital forensics landscape and delivering forensic capability to the centre of the security stack • How speed, automation and integration can dramatically reduced incident response dwell times and improve SOC productivity by 50% • Why assisted compromise assessment will help to reduce your skills shortage by allowing analysts to focus on high-value actions • Why proactive forensic diffing is a game-changer for cyber-resilience and vulnerability management
<p>Cloudflare</p> <p>Mantis – the most powerful botnet to date</p> <p>Bader Shaath, Solutions Engineer, Cloudflare</p>	<p>Join this session to learn more on the evolution of malicious botnets and how they produce severe attacks that overwhelm organisations and take them out of service. Cloudflare has visibility over almost 20% of Internet traffic and has many technologies to detect and control a wide range of devastating cybersecurity attacks.</p> <p>Bader Shaath will be discussing:</p> <ul style="list-style-type: none"> • The effect of cybersecurity attacks on the IT space • The anatomy of new threats and BOT networks • Mitigating complex cybersecurity attacks with the Orange Cloud • Demonstration of Cloudflare security platform
<p>Cofense</p> <p>Adaptive email security architecture: Moving from incident response to continuous response</p> <p>Alaa Abu Gharbieh, Regional Sales Manager – META, Cofense</p>	<p>With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation.</p> <p>Join us for this informative session that walks through the benefits of implementing an adaptive security architecture and risk framework, and how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity.</p> <p>This session will cover:</p> <ul style="list-style-type: none"> • What is adaptive security architecture? • Objectives of adaptive security architecture • Risk framework • The current situation in email and phishing security • Implementing adaptive security architecture and risk framework with Cofense

Education Seminars	
<p>CybelAngel</p> <p>Exposed doors and lost keys: Gaining visibility across your digital footprint</p> <p>Adnan Taha, Director – Middle East, CybelAngel</p>	<p>Remember the Colonial Pipeline attack? Or how an exposed password combined to a publicly accessible VPN led to a \$2.4m ransom attack. Mundane, but deadly. Join CybelAngel's experts, as they share real-life examples of how shadow assets, lost creds, and fake websites easily add up to costly attacks unless you regain full visibility across your extended digital footprint.</p> <p>In this presentation, you will:</p> <ul style="list-style-type: none"> • Understand the threats caused by unsanctioned digital assets in your supply chain • See your digital footprint through the eyes of attackers • Spot opportunities to reduce your external attack surface
<p>Entrust</p> <p>Securing digital transformation</p> <p>Hamid Qureshi, Territory Sales Manager, Middle East and Africa, Entrust</p>	<p>The value of data puts a target on all enterprises. In order to thrive against such constant threats, enterprises require a full complement of digital and physical solutions to address today's key security challenges, meet compliance regulations, protect the post-Covid remote workers and realise digital transformation initiatives.</p> <p>Join this session where we'll discuss today's security challenges and how to overcome them:</p> <ul style="list-style-type: none"> • Protecting corporate and consumer data • Meeting compliance mandates like GDPR, PSD2, KYC, etc. • Securing virtualised and cloud infrastructure • Enabling a secure, productive workforce
<p>HUMAN Security</p> <p>The phases of account takeover (ATO) and how to stop them</p> <p>Peter Craig, Director of Cybersecurity Product Marketing, HUMAN Security</p>	<p>For any online business, account takeover (ATO) attacks are one of the fastest growing threats facing retailers, especially those that collect, store and process customer information. ATO presents a big risk to the business, one that can cost millions of dollars, force unpleasant public disclosures, damage a brand, and upset customers and investors.</p> <p>ATO fraud attempts rose 307% from April 2020 to June 2021, averaging 82% of all login attempts in the second half of 2021. The 2022 Cyberthreat Defense Report found that credential stuffing and ATO were the #2 most concerning threat to web apps in 2022, up from #4 in 2021.</p> <p>Sophisticated bots can quickly and easily create large numbers of fake new user accounts. These accounts are either completely fake or are created using details where the real human is unaware of the fraud.</p> <p>In this session, we'll explore:</p> <ul style="list-style-type: none"> • Why and how fraudsters takeover and create fake accounts • How to spot and stop ATO attacks without introducing unnecessary friction to the customer experience • Why sophisticated bots are different and the limitations of your existing defences
<p>Malwarebytes</p> <p>Incident response in the age of ransomware and data protection</p> <p>Ayoub Jaaouani, Sales Engineer – MEA, Malwarebytes</p>	<p>Recent trends – current industry situation and ransomware NIST Framework and ransomware incident response automation lever for next gen SOC Malwarebytes Value Proposition</p> <p>Key takeaways:</p> <ul style="list-style-type: none"> • Specific pre-attack events that indicate behaviour of ransomware in your environment • Incident response strategy to clean your environment on an ongoing basis – automated/orchestrated. • Organisations standing on NIST Cybersecurity Capability Maturity Model • NIST Framework best practices to prevent ransomware

Education Seminars	
<p>ManageEngine</p> <p>Embracing Zero Trust security: Privileged access management deep dive</p> <p>Shawn (Shakthi Shankar RM), Business Development & Customer Success, ManageEngine</p>	<p>Threat actors are proving to be increasingly effective at breaching corporate networks and gaining footholds. Since the start of the pandemic, we have already seen an incredible number of breaches/public hacks due to the hybrid work culture. In this talk, learn more about the emerging threats in cybersecurity space and how embracing Zero Trust through an effective PAM strategy can help organisations mitigate those threats.</p> <p>This session will cover:</p> <ul style="list-style-type: none"> • A snapshot of recent data breaches • How organisations can protect against cyber-threats using PAM • How organisations can embrace Zero Trust security through PAM
<p>Menlo Security</p> <p>The next class of browser-based attacks</p> <p>Tom McVey, Solution Architect, Menlo Security</p>	<p>There are two distinct characteristics that all threat actors tend to share. First, they focus on avoiding detection by any means. Second, while some go after specific targets, many opt to aim their tactics at the vectors that will reap the greatest rewards. After all, a big pond with many fish increases everyone’s chances of success.</p> <p>Between July and December 2021, there was a 224% increase in highly evasive adaptive threats (HEAT) attacks – a class of cyber-threats targeting web browsers as the attack vector. While malware once had to be downloaded to pose a real risk, now, it’s a dynamically-generated threat toolkit built in the web where employees are productive.</p> <p>In this session, you will:</p> <ul style="list-style-type: none"> • Discover the anatomy of recent browser-based attacks • Learn why network security today is broken • Experience a live demo that enables you to discover the technology approach proven to eliminate these threats
<p>Synack</p> <p>Hacking for the greater good: Using hackers to beat hackers</p> <p>Abhi Ghosh, Sales Director UAE, Synack, and Aditya Modha, Security Researcher & Cloud Security Consultant, Safe Security</p>	<p>For cybersecurity professionals, the rate of modern software development and infrastructure change are outpacing security testing capacity and capability. As organisations have gone remote and increasingly digital, they increase risk of introducing new vulnerabilities and put additional strain on security teams. In this session, Synack’s Abhi Ghosh will discuss the security challenges CISOs are facing in today’s business climate and how Synack’s innovative security model and continuous pen testing offering address these challenges.</p> <p>Attendees will learn:</p> <ul style="list-style-type: none"> • Why diverse perspectives in security testing are essential to hardening systems against the full spectrum of cyber-threats • How to secure your organisation while managing a remote workforce from the executive’s perspective • How agile businesses are able to respond quickly to opportunities or threats • How security researchers are playing a pivotal role in securing company’s assets