

# Post event report



## Strategic Sponsors



## Education Seminar Sponsors



“ The virtual conference in general and topics covered were well organised. The content provided insight in critical areas for internal audit consideration, value adding truly. ”

Vice President-Internal Audit,  
Fly Dubai

“ I attended e-Crime Middle East and it was wonderful. Surely looking forward to attending in person the upcoming event in March. ”

Head of Fraud Investigations,  
RAK Bank

“ Thank you for the excellent event. ”

Head of Information Security – Bahrain,  
Gulf International Bank

“ I found the event to be very informative, and all topics discussed were so relatable to today's information security & integrity challenges and threats. I found the event management to be very efficient and well controlled. Thank you for yet another successful event and looking forward to the next in-person conference next March 2022 in Dubai. ”

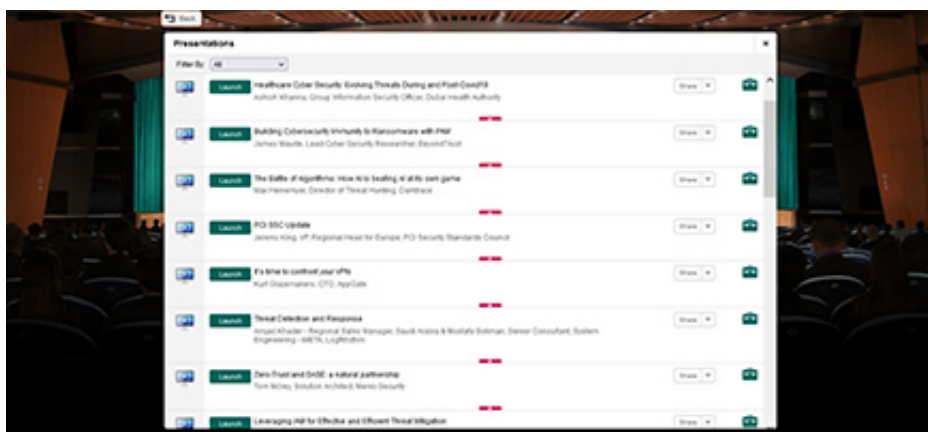
Chief of Internal Audit,  
Dubai Healthcare City Authority

“ Thanks for the wonderful sessions, looking forward to the next e-Congress. ”

Head of IT and Innovation,  
Index Exchange

Inside this report:

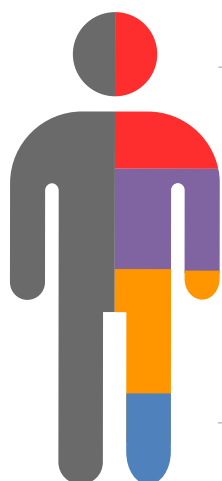
- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



### Key themes

- Moving to Cloud Native?
- Re-engineering the SOC: from logs to automated XDR
- From smart machines to smart cities – securing the IoT
- Cybersecurity for business resilience
- Building better Cloud governance
- Closing the cybersecurity skills gap
- Too little time for implementation?
- Building-in security: from DevOps to SecDevOps?
- Are criminals winning the ransomware war?
- Securing digital currencies
- Securing the citizen

### 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

### Speakers

- Hatem Ali, Global Services and Intelligence Lead, MEA, **FireEye**
- Jeevan Badigari, Director of Information Security and Governance, **DAMAC Properties**
- Lonnie Benavides, Head of Infrastructure and Application Security, **OneLogin**
- Ali Beshara, Head of Information Security and Risk Management, **BENEFIT Company – Bahrain**
- Steve Brown, Director, Cybersecurity, **Mastercard**
- Graham Cluley, Security Analyst, **grahamcluley.com**
- Ozgur Danisman, Vice-President of Sales Engineering, EMEA, **Forcepoint**
- Amr El-Hatter, Regional Sales Manager, EMEA, **FireMon**
- Kurt Glazemakers, CTO, **Appgate**
- Max Heinemyer, Director of Threat Hunting, **Darktrace**
- Mr A Karthik, Chief Technical Evangelist, **ManageEngine**
- Amjad Khader, Regional Sales Manager, Saudi Arabia, **LogRhythm**
- Muhammad Rizwan Khan, General Manager, **Al Dhahery Exchange**
- Ashish Khanna, Group Information Security Officer, **Dubai Health Authority**
- Jeremy King, VP, Regional Head for Europe, **PCI Security Standards Council**
- Maurits Lucas, Director of Intelligence Solutions, **Intel 471**
- James Maude, Lead Cyber Security Researcher, **BeyondTrust**
- Tom McVey, Solution Architect, **Menlo Security**
- Ahmed Nabil, Regional Information Security and Risk Manager, **Standard Chartered Bank**
- Hamid Qureshi, Territory Sales Manager, Middle East and Africa, **Entrust**
- Mark Richmond, Senior Solutions Engineer EMEA, **Stealthbits**
- Mostafa Soliman, Senior Consultant, System Engineering – iMETA, **LogRhythm**
- Jason Steer, Director of EMEA Presales, **Recorded Future**
- Kamel Tamimi, Director of Engineering, META/APAC, **Cofense**

Agenda					
08:00	Login and networking				
08:55	Chairman's welcome				
09:00	<p><b>Healthcare cybersecurity: Evolving threats during and post-Covid-19</b></p> <p><b>Ashish Khanna</b>, Group Information Security Officer, Dubai Health Authority</p> <ul style="list-style-type: none"> <li>• How hackers rapidly evolved tactics to exploit the public's pandemic fears</li> <li>• The rapid adoption of cybersecurity best practices for keeping pace with evolving threats</li> <li>• How threats to the health system from nation-states and criminals are a growing concern at a time when the pandemic has increased our reliance on technology</li> </ul>				
09:20	<p><b>Building cybersecurity immunity to ransomware with PAM</b></p> <p><b>James Maude</b>, Lead Cyber Security Researcher, BeyondTrust</p> <ul style="list-style-type: none"> <li>• 6 things to know about ransomware</li> <li>• Realistic security practices you can implement to protect against ransomware</li> <li>• The role of PAM (privileged access management) in mitigating the risks of ransomware and other cyber-threats with a powerful, blended defence</li> </ul>				
09:40	<p><b>The battle of algorithms: How AI is beating AI at its own game</b></p> <p><b>Max Heinemyer</b>, Director of Threat Hunting, Darktrace</p> <ul style="list-style-type: none"> <li>• How cybercriminals are leveraging AI tools to create sophisticated cyber-weapons</li> <li>• What an AI-powered spoofing threat may look like, and why humans will not be able to spot them</li> <li>• Why defensive AI technologies are uniquely positioned to fight back</li> </ul>				
10:00	<p><b>PCI SSC update</b></p> <p><b>Jeremy King</b>, VP, Regional Head for Europe, PCI Security Standards Council</p> <ul style="list-style-type: none"> <li>• PCI DSS V4.0 latest news</li> <li>• PA DSS migration to Software Security Framework</li> <li>• Software Security Framework latest news</li> <li>• Training</li> <li>• Informational training</li> <li>• Work from home</li> <li>• Remote assessments</li> <li>• PCI at a glance</li> </ul>				
10:20	<p><b>Education Seminars   Session 1</b></p> <table border="1"> <tr> <td> <p><b>Appgate</b></p> <p><b>It's time to confront your VPN</b></p> <p><b>Kurt Glazemakers</b>, CTO, Appgate</p> </td> <td> <p><b>LogRhythm</b></p> <p><b>Threat detection and response</b></p> <p><b>Amjad Khader</b>, Regional Sales Manager, Saudi Arabia, and <b>Mostafa Soliman</b>, Senior Consultant, System Engineering – iMETA, LogRhythm</p> </td> <td> <p><b>Menlo Security</b></p> <p><b>Zero-Trust and SASE: A natural partnership</b></p> <p><b>Tom McVey</b>, Solution Architect, Menlo Security</p> </td> <td> <p><b>OneLogin</b></p> <p><b>Leveraging IAM for effective and efficient threat mitigation</b></p> <p><b>Lonnie Benavides</b>, Head of Infrastructure and Application Security, OneLogin</p> </td> </tr> </table>	<p><b>Appgate</b></p> <p><b>It's time to confront your VPN</b></p> <p><b>Kurt Glazemakers</b>, CTO, Appgate</p>	<p><b>LogRhythm</b></p> <p><b>Threat detection and response</b></p> <p><b>Amjad Khader</b>, Regional Sales Manager, Saudi Arabia, and <b>Mostafa Soliman</b>, Senior Consultant, System Engineering – iMETA, LogRhythm</p>	<p><b>Menlo Security</b></p> <p><b>Zero-Trust and SASE: A natural partnership</b></p> <p><b>Tom McVey</b>, Solution Architect, Menlo Security</p>	<p><b>OneLogin</b></p> <p><b>Leveraging IAM for effective and efficient threat mitigation</b></p> <p><b>Lonnie Benavides</b>, Head of Infrastructure and Application Security, OneLogin</p>
<p><b>Appgate</b></p> <p><b>It's time to confront your VPN</b></p> <p><b>Kurt Glazemakers</b>, CTO, Appgate</p>	<p><b>LogRhythm</b></p> <p><b>Threat detection and response</b></p> <p><b>Amjad Khader</b>, Regional Sales Manager, Saudi Arabia, and <b>Mostafa Soliman</b>, Senior Consultant, System Engineering – iMETA, LogRhythm</p>	<p><b>Menlo Security</b></p> <p><b>Zero-Trust and SASE: A natural partnership</b></p> <p><b>Tom McVey</b>, Solution Architect, Menlo Security</p>	<p><b>OneLogin</b></p> <p><b>Leveraging IAM for effective and efficient threat mitigation</b></p> <p><b>Lonnie Benavides</b>, Head of Infrastructure and Application Security, OneLogin</p>		
10:50	Refreshments and networking break				
11:20	<p><b>Securing a remote workforce</b></p> <p><b>Jeevan Badigari</b>, Director of Information Security and Governance, DAMAC Properties</p> <ul style="list-style-type: none"> <li>• Balancing security and productivity</li> <li>• Enabling business beyond the perimeter</li> <li>• Continuous risk assessment and adoption of new ways of working</li> </ul>				
11:40	<p><b>Risk-adaptive data security for today's hybrid workforce</b></p> <p><b>Ozgur Danisman</b>, Vice-President of Sales Engineering, EMEA, Forcepoint</p> <ul style="list-style-type: none"> <li>• What to prioritise between WHO accesses your business systems and WHAT is stored inside</li> <li>• Adapting existing infrastructures for evolving workplace models</li> <li>• The healthy balance between being compliant and having necessary threat protection technology in place</li> </ul>				
12:00	<p><b>How to increase incident response efficiency with security intelligence</b></p> <p><b>Jason Steer</b>, Director of EMEA Presales, Recorded Future</p> <ul style="list-style-type: none"> <li>• Learn why incident response teams are overwhelmed with too many events to analyse every day</li> <li>• Working on the front lines of cyber-defence require security intelligence to help cut through the noise and respond quickly to 'real' threats</li> <li>• Understand why intelligence needs to be embedded into your tools and workflows to save time</li> </ul>				

## Agenda

<b>12:20</b>	<b>Education Seminars   Session 2</b>			
	<b>Cofense</b> <b>Is something missing from your email security architecture?</b> <b>Kamel Tamimi</b> , Director of Engineering, META/APAC, Cofense	<b>Entrust</b> <b>Encryption strategies to protect customer and enterprise data against insider and outsider attacks</b> <b>Hamid Qureshi</b> , Territory Sales Manager, Middle East and Africa, Entrust	<b>FireMon</b> <b>What do the Special Forces and cybersecurity have in common?</b> <b>Amr El-Hatter</b> , Regional Sales Manager, EMEA, FireMon	<b>Intel 471</b> <b>Big game hunting in the Middle East</b> <b>Maurits Lucas</b> , Director of Intelligence Solutions, Intel 471
<b>12:50</b>	Refreshments and networking break			
<b>14:00</b>	<b>Cloud security 2021 – what's new?</b>			
	<b>Ahmed Nabil</b> , Regional Information Security and Risk Manager, Standard Chartered Bank <ul style="list-style-type: none"> <li>• What are the most significant challenges in Cloud security in this new hybrid era?</li> <li>• Building a comprehensive Cloud security plan, policies and processes</li> <li>• Combining humans and automation to optimise Cloud security</li> <li>• Controlling costs while maintaining security in the Cloud</li> </ul>			
<b>14:20</b>	<b>To resiliency and beyond!</b>			
	<b>Steve Brown</b> , Director, Cybersecurity, Mastercard <ul style="list-style-type: none"> <li>• Increasingly complex networks of business relationships are exposing participants to systemic operation risk</li> <li>• As a result, our national security, public safety and economic growth are being exposed to major disruption</li> <li>• In this session, see how Mastercard is delivering trust through an approach that quantifies, automates and prioritises risk to build cyber-resilience and trust throughout the connected digital economy</li> </ul>			
<b>14:40</b>	<b>Education Seminars   Session 3</b>			
	<b>FireEye</b> <b>Edge of tomorrow: Is cyber-resilience a fairytale?</b> <b>Hatem Ali</b> , Global Services and Intelligence Lead, MEA, FireEye	<b>ManageEngine</b> <b>The dynamic shift in the digital world – focus on IT security</b> <b>Mr A Karthik</b> , Chief Technical Evangelist, ManageEngine	<b>Netwrix</b> <b>Secure access to the data and infrastructure: Active Directory security and management</b> <b>Mark Richmond</b> , Senior Solutions Engineer EMEA, Stealthbits	
<b>15:10</b>	Refreshments and networking break			
<b>15:30</b>	<b>Closing the security skills gap</b>			
	<b>Ali Beshara</b> , Head of Information Security and Risk Management, BENEFIT Company – Bahrain <ul style="list-style-type: none"> <li>• Identifying the skills first, highlight the SFIA Foundation revised IT skills</li> <li>• Can all security skills be easily acquired? What is the case in Bahrain?</li> <li>• Available resources in the market, what works and what are the challenges</li> <li>• Get into their shoes: A look at security skills gap from the perspective of the candidate and from the employer's perspective</li> </ul>			
<b>15:50</b>	<b>How robust compliance can prevent e-Crime</b>			
	<b>Muhammad Rizwan Khan</b> , General Manager, Al Dhahery Exchange <ul style="list-style-type: none"> <li>• Financial crime, identification of key factors that should be reported as suspicious</li> <li>• Identification of areas where due diligence inquiries need to be made for e-Crimes</li> <li>• Areas of susceptibility and vulnerability to employee collaboration in e-Crimes</li> <li>• Establishment of Risk Assessment Model</li> <li>• Prevention of unauthorised access</li> <li>• Consumer Data Protection regulation</li> </ul>			
<b>16:10</b>	<b>Ghosts in the machine</b>			
	<b>Graham Cluley</b> , Security Analyst, grahamcluley.com In a series of real-life stories, computer security veteran Graham Cluley takes a look at the threats that should be giving you sleepless nights. <ul style="list-style-type: none"> <li>• Cyber-extortion and the future of ransomware</li> <li>• From fakes to deepfakes: pretending to be the government</li> <li>• Do you even know who your third parties are?</li> <li>• An employee spurned is a big security problem</li> </ul>			
<b>16:30</b>	Closing remarks			
<b>16:35</b>	Final refreshments and networking break			
<b>17:00</b>	Conference close			

Education Seminars	
<p><b>Appgate</b></p> <p><b>It's time to confront your VPN</b></p> <p><b>Kurt Glazemakers, CTO,</b> Appgate</p>	<p>Legacy business VPN remote access solutions weren't designed to handle the security challenges of today's distributed workforce and escalating threat landscapes. Zero Trust Network Access (ZTNA) is the new industry standard for secure access to anything, from anywhere, by anyone.</p> <p><b>Join this session to find out how you can easily migrate your business from VPN to ZTNA:</b></p> <ul style="list-style-type: none"> <li>• Best practises for moving from VPN to ZTNA</li> <li>• Explore a variety of use cases that can be addressed by ZTNA</li> <li>• How replacing VPN can strengthen security and reduce your attack surface</li> </ul>
<p><b>Cofense</b></p> <p><b>Is something missing from your email security architecture?</b></p> <p><b>Kamel Tamimi, Director of Engineering, META/APAC,</b> Cofense</p>	<p>Tune in to gain insight into the latest best-practice security architecture, the inadequacy of traditional solutions, the costs of inadequacy in a modern cyber-stack, and what to do about it.</p> <p>The (so called) secure email gateways that businesses depend upon to filter out malicious email are simply failing, as polymorphic attacks and social engineering increase. These traditional solutions are proving – on a daily basis – inadequate to prevent breaches.</p> <p>New security layers are needed – and thankfully, Cofense is able to provide the answer.</p> <ul style="list-style-type: none"> <li>• An Adaptive Security Architecture, and why you need one</li> <li>• The true costs of an incomplete cyber-stack</li> <li>• Why prevention is not enough</li> <li>• Real life attacks – a walk through some real attacks</li> <li>• How to do effective phishing detection and response</li> </ul>
<p><b>Entrust</b></p> <p><b>Encryption strategies to protect customer and enterprise data against insider and outsider attacks</b></p> <p><b>Hamid Qureshi, Territory Sales Manager, Middle East and Africa,</b> Entrust</p>	<p>Cyber-attacks targeting organisations continue to increase in both volume and sophistication. Security-conscious enterprises need to prepare for threats that emanate from external cybercriminals as well as employee errors and malicious insiders. While detection, threat intelligence and other techniques have come into vogue in recent years, encryption continues to play a foundational role in protecting sensitive customer data and enterprise assets.</p> <p><b>Join this session to learn:</b></p> <ul style="list-style-type: none"> <li>• The role that encryption plays in defending sensitive data</li> <li>• The strategies for implementing strong encryption with a HSM as a root of trust</li> <li>• Real-world case studies to address challenges</li> </ul>
<p><b>FireEye</b></p> <p><b>Edge of tomorrow: Is cyber-resilience a fairytale?</b></p> <p><b>Hatem Ali, Global Services and Intelligence Lead, MEA,</b> FireEye</p>	<p>Criminality has been part of human experience since the dawn of existence, and it gets transformed as we evolve as a species. Technology today is a foundation for civilisation development, but is also an opportunity for cybercriminals.</p> <p><b>In this session we shall:</b></p> <ul style="list-style-type: none"> <li>• Review the state of cybersecurity</li> <li>• Outline how criminals are using our growing dependency on digital infrastructure against us</li> <li>• Try to envision what tomorrow could look like when it comes to advancing a cyber-defence mission</li> </ul>



<b>Education Seminars</b>	
<p><b>FireMon</b></p> <p><b>What do the Special Forces and cybersecurity have in common?</b></p> <p><b>Amr El-Hatter</b>, Regional Sales Manager, EMEA, FireMon</p>	<p>A Special Forces team is a well-oiled machine. Their extensive training ensures that when faced with risk, they know exactly what to do and when. They are programmed to identify and assess every single risk and ensure that their response complies with their superior's clearly defined orders and commands. So what is the secret to their success? Join us as we explore why automation is fundamental to the success of every single organisation globally, including yours.</p> <p><b>This session will cover:</b></p> <ul style="list-style-type: none"> <li>The challenges facing Middle Eastern organisations right now from new regulations through to skill gap shortages</li> <li>How automation is used by enterprises and Special Forces alike to overcome risk and compliance challenges</li> <li>A Special Forces mindset – why your security approach should mirror their thinking</li> <li>Real life examples of how automation transformed a number of businesses</li> </ul>
<p><b>Intel 471</b></p> <p><b>Big game hunting in the Middle East</b></p> <p><b>Maurits Lucas</b>, Director of Intelligence Solutions, Intel 471</p>	<p>In a little over a year, the number of breaches has more than tripled. And the Middle East is no exception, far from it actually! 'Big game hunting' ransomware attacks are a threat that is top of mind for many CISOs who are determined to protect their organisation from falling victim to this threat. The question is how?</p> <p>In this session, we will look at the broad range of products and services in the underground that have sprung up to facilitate and scale up this type of attack. Because the deployment of ransomware is actually the last step in a multi-stage process.</p> <p>To effectively protect the organisation against attack, it is key to understand these steps and services so you can stop an incident from becoming a full blown crisis.</p> <p><b>What attendees will learn</b></p> <ul style="list-style-type: none"> <li>How stolen credentials and vulnerabilities play a key role in ransomware attacks</li> <li>The role of access brokers and affiliates</li> <li>The surprising role of Iranian actors in selling access to company networks</li> <li>Why the underground is hiring business analysts to help with attacks</li> <li>Measures you can take that make a difference</li> </ul>
<p><b>LogRhythm</b></p> <p><b>Threat detection and response</b></p> <p><b>Amjad Khader</b>, Regional Sales Manager, Saudi Arabia, and <b>Mostafa Soliman</b>, Senior Consultant, System Engineering – iMETA, LogRhythm</p>	<p>Detecting malware, network intrusion, social engineering, and anomalous user behaviour are just a few of today's threat challenges. In this session, discover how LogRhythm uses hybrid analytics to detect threats by identifying and monitoring actors and their actions.</p> <p><b>The LogRhythm team will provide an overview of hybrid analytics, including:</b></p> <ul style="list-style-type: none"> <li>How machine learning (ML) and rule-based detection work hand-in-hand to detect known and unknown threats</li> <li>How hybrid analytics use threat intelligence and identity data to help speed incident response</li> <li>How integrations with endpoint detection and response (EDR) and firewalls expand visibility</li> <li>In addition, you'll learn how network detection and response (NDR) integrates with your security information and event management (SIEM)</li> </ul>

<b>Education Seminars</b>	
<p><b>ManageEngine</b></p> <p><b>The dynamic shift in the digital world – focus on IT security</b></p> <p><b>Mr A Karthik</b>, Chief Technical Evangelist, ManageEngine</p>	<p>In today's world, the security threat is at an all-time high. Unregulated endpoints is a serious concern faced by IT admins and organisations all over the world. To evade any security breach, your organisation must deploy modern-day solutions to your IT infrastructure.</p> <p>To optimise your IT security, it is essential to automate your day-to-day IT activities and utilise the latest digital transformation trends such as ML, AI, IAM, etc., for improved security management. At ManageEngine's webinar, we'll explore topics to ensure better endpoint and network security with new digital transformations for seamless business continuity.</p> <p><b>The seminar will highlight the following:</b></p> <ul style="list-style-type: none"> <li>• Introduction to the shift in digitalisation</li> <li>• Infographics related to IT security and other technology trends</li> <li>• How do you overcome the security threats to stay higher up in the ladder?</li> </ul>
<p><b>Menlo Security</b></p> <p><b>Zero-Trust and SASE: A natural partnership</b></p> <p><b>Tom McVey</b>, Solution Architect, Menlo Security</p>	<p>A SASE approach shifts security to the cloud – closer to apps, users and data – but it will not fulfil its promise without a fundamental change to an organisation's detect-and-remediate controls. In order to outsmart threats and liberate users, cybersecurity teams are seeking to fundamentally change the way they protect the enterprise from malicious threats on the Internet.</p> <ul style="list-style-type: none"> <li>• SASE – modernising detection and response</li> <li>• New visibility at speed and scale</li> <li>• Isolation – eliminating phishing and ransomware while driving productivity</li> <li>• How to combine Zero-Trust and SASE to transform end-user protection</li> </ul>
<p><b>Netwrix</b></p> <p><b>Secure access to the data and infrastructure: Active Directory security and management</b></p> <p><b>Mark Richmond</b>, Senior Solutions Engineer EMEA, Stealthbits</p>	<p>While most organisations focus on analysing and controlling access to the data and resources Active Directory is facilitating access to, they often lack visibility into the security of AD itself and the myriad of tactics, techniques, and procedures attackers have developed to compromise this beating heart of any organisation's IT infrastructure.</p> <p>Active Directory is secure and efficient when it's clean, understood, configured properly, monitored closely, and controlled tightly.</p> <p><b>In our session you can learn, how to:</b></p> <ul style="list-style-type: none"> <li>• Inventory all objects, policies, &amp; configurations to obtain a complete view of your AD footprint</li> <li>• Analyse relationships between objects, permissions, access rights, and toxic conditions to prioritise risks and remediation efforts</li> <li>• Clean up stale and unneeded objects to limit risk and unnecessary exposure while alleviating administrative burden</li> <li>• Monitor changes to critical objects signifying attacker attempts to compromise credentials and circumvent security controls in order to achieve persistence</li> <li>• Protect critical objects from unauthorised change or access, remediate vulnerabilities, prevent credential abuse &amp; privilege escalation</li> </ul>
<p><b>OneLogin</b></p> <p><b>Leveraging IAM for effective and efficient threat mitigation</b></p> <p><b>Lonnie Benavides</b>, Head of Infrastructure and Application Security, OneLogin</p>	<p>There's no question that the current cybersecurity landscape is constantly shifting and evolving as new threats and security solutions emerge. Increased cyber-attacks and distributed workforces have created new challenges that require innovative solutions.</p> <p>Faced with the challenge of managing identities and securing access to data and applications from a growing number of endpoints, what are the fundamental controls organisations need to maintain business continuity and secure their remote and hybrid workforce?</p> <p>Hear from Lonnie Benavides – Head of Infrastructure and Application Security, Onelogin – for a discussion on practical information and advice regarding the utilisation of identity and access management solutions to effectively mitigate modern cyber-threats to your business.</p> <p><b>Key takeaways:</b></p> <ul style="list-style-type: none"> <li>• Understanding the key fundamentals of a strong cloud security posture</li> <li>• Why passwords alone are not enough</li> <li>• Best practices for building a cybersecurity strategy at scale</li> </ul>