Post event report

Strategic Sponsors

BeyondTrust
DARKTRACE
illumio
Pulse Secure Acquired by Ivanti
Recorded Future
SentinelOne
Synack

Education Seminar Sponsors

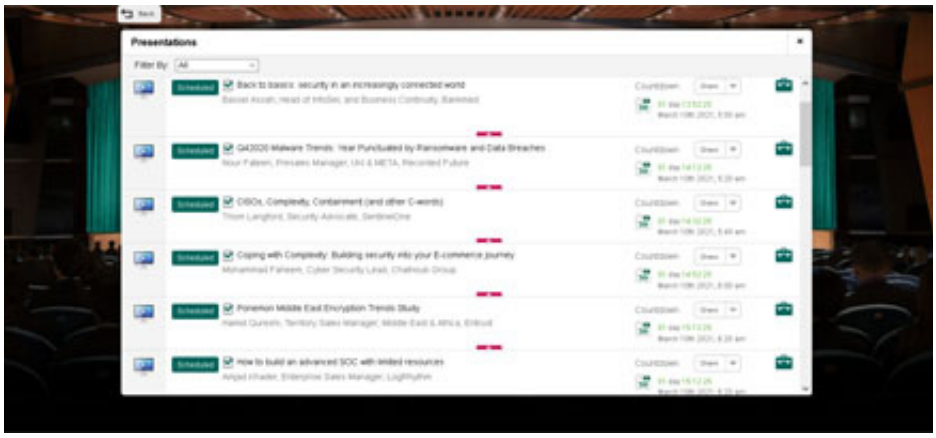
ENTRUST SECURING A WORLD IN MOTION
FIREEYE
FIREMON
LogRhythm
onapsis
onelogin
ThreatConnect

Networking Sponsors

BULWARK Technologies
corelight
emt TECHNOLOGY DISTRIBUTION
Green Method
Gulf IT Network Distribution
GO ANYWHERE A HelpSystems Solution
ManageEngine
OPSWAT.
tripwire

Inside this report:

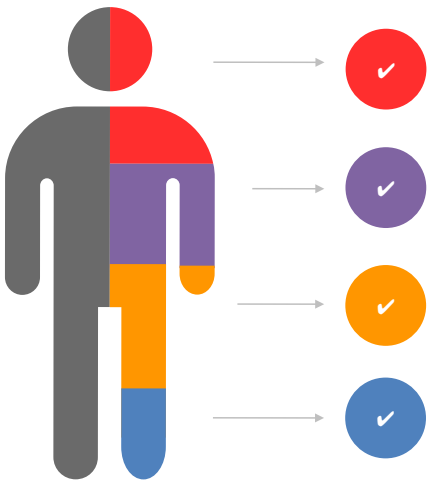
Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars



Key themes

- Security for the 5G revolution
- Securing digital currencies
- Cybersecurity for business resilience
- Stuck in the Cloud
- Building in security: easier said than done?
- Securing the enterprise of sensors
- Securing the citizen
- Securing and protecting remote employees
- Cybersecurity by remote control

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

Wissam Abed, Leader – Financial Intelligence Unit – Middle East & South Asia, Western Union

Shakeel Ahmed, Head of Infrastructure & IT Security, leading investment and development company based in Abu Dhabi

Hatem Ali, Global Services and Intelligence Lead, MEA, FireEye

Bassel Assah, Head of InfoSec and Business Continuity, Bankmed

Lonnie Benavides, Head of Infrastructure and Application Security, OneLogin

Simon Brady, Managing Editor, AKJ Associates Ltd

Migchiel de Jong, Systems Engineer, Illumio

Luna de Lange, Partner and Data Protection Officer, KARM Legal Consultants

Trevor Dearing, Technology Director, EMEA, Illumio

John Elliott, Director, Industry Standards, Mastercard

Mohammad Faheem, Cyber Security Lead, Chalhoub Group

Nour Fateen, Presales Manager, UKI & META, Recorded Future

Dan Fein, Director of Email Security Products, Darktrace

Jonathan Hallatt, Regional Sales Director, Pulse Secure

Taimur Ijlal, Head of Cloud Security & DevSecOps, Network International

Sreedevi Jayachandran, Information Security and Risk Advisory, MIG Holding

Amjad Khader, Enterprise Sales Manager, LogRhythm

Thom Langford, Security Advocate, SentinelOne

Kostas Lotsis, Senior Sales Engineer EMEA, FireMon

Roland Abi Najem, Cyber Security Consultant & Instructor, American University of Science & Technology

Ron Peeters, Vice President Middle East and Emerging Markets, Synack

Hamid Qureshi, Territory Sales Manager, Middle East & Africa, Entrust

Miles Tappin, VP of EMEA, ThreatConnect

Frederik Weidemann, Chief Technical Evangelist, Onapsis Inc

Agenda

08:00 Registration and networking

08:50 Chairman's welcome

09:00 **Back to basics: Security in an increasingly connected world**

Bassel Assah, Head of InfoSec and Business Continuity, Bankmed

- The implications of breaches such as SolarWinds and warning signs for security professionals
- Regulators, compliance, and governance vs. actual security: the need to balance
- Future of cybersecurity: are machine learning and AI enough?
- IoT and embedded systems: history repeating itself
- In an increasingly connected world, returning to security basics is crucial to enable growth

09:20 **Q4 2020 Malware trends: Year punctuated by ransomware and data breaches**

Nour Fateen, Presales Manager, UKI & META, Recorded Future

- Analysing trends in malware use, distribution, and development throughout 2020 and the TTPs that had a major impact on technology
- Covering how ransomware operators continue to have an opportunistic mindset when conducting campaigns, putting more emphasis on data theft extortion to increase their chances of profitability
- Explaining how threat hunters and SOC teams can strengthen their security posture by prioritising hunting techniques and detection methods based on this research and data

09:40 **CISOs, Complexity, Containment (and other C-words)**

Thom Langford, Security Advocate, SentinelOne

- Why traditional protective approaches are no longer effective enough
- How complexity has made the CISO's ability to respond more difficult
- The importance of automation in the response process to address this paradigm shift CISOs now face

10:00 **Coping with complexity: Building security into your e-Commerce journey**

Mohammad Faheem, Cyber Security Lead, Chalhoub Group

- Customer facing businesses have adapted to hybrid or online service models. This environment has proved challenging for security teams tasked with securing more applications, devices and platforms than ever before
- The initial steps for embedding security into your digital projects: addressing the challenges of time-sensitive integrations
- Third-party providers: assessing their security capabilities to reduce complexity
- Adopting a continuous approach to API security and implementing sufficient security controls and tools at every stage

10:20 **Education Seminars | Session 1**

Entrust	LogRhythm	OneLogin	ThreatConnect
Ponemon Middle East Encryption Trends Study	**How to build an advanced SOC with limited resources**	**Extortionware: Your privacy problems made public**	**Risk, threat, response: Drive complexity, time, and cost out of your security programme**
Hamid Qureshi, Territory Sales Manager, Middle East & Africa, Entrust	**Amjad Khader,** Enterprise Sales Manager, LogRhythm	**Lonnie Benavides,** Head of Infrastructure and Application Security, OneLogin	**Miles Tappin,** VP of EMEA, ThreatConnect

10:50 Networking break

11:20 **From technologist to risk manager: Changing the cybersecurity mindset**

Roland Abi Najem, Cyber Security Consultant & Instructor, American University of Science & Technology

- The prevalence of sophisticated nation-state attacks on even the most secure organisations highlights that an attack could happen to any organisation, at any time
- Despite this, cybersecurity is still often treated as a purely technical issue, with organisations investing in solutions without considering how tools will help protect their organisation in practice
- Technology is key to identifying a cyber-attack, but when your people are critical in preventing and effectively mitigating the impact of an attack, organisations must ensure that their investments are allocated accordingly
- So, how can cybersecurity professionals shake up their approach, transitioning from technologist to risk manager, to ensure cyber-risks are managed holistically?

11:40 **Lock the doors before profiling the burglar**

Trevor Dearing, Technology Director, EMEA, Illumio

- It's true that rumours of the death of the perimeter have been vastly exaggerated
- A simple approach, partnering with IT can be far more effective and helps to make threat management work better
- By employing good hygiene, it is possible to stop the spread of viruses and ransomware

12:00 **PAM: Foundational security for business transformation**

Michael Byrnes, Director of Solutions Engineering Middle East, India & Africa, BeyondTrust

- Digital transformation: what it is, why we should care and how PAM can support the security team
- Why automation isn't just for the business
- How to mitigate identity risk with PAM

12:20 **Securing the new normal: Cyber AI for the inbox**

Dan Fein, Director of Email Security Products, Darktrace

- Today, 94% of cyber-threats still originate in the inbox and 'impersonation attacks' are on the rise, as artificial intelligence is increasingly being used to automatically generate spear-phishing emails, or 'digital fakes', that expertly mimic the writing style of trusted contacts and colleagues
- Humans can no longer distinguish real from fake on their own – businesses are increasingly turning to AI to distinguish friend from foe and fight back with autonomous response
- In an era when thousands of documents can be encrypted in minutes, 'immune system' technology takes action in seconds – stopping cyber-threats before damage is done

Agenda

12:40 Education Seminars | Session 2

FireMon	FireEye	Illumio	Onapsis
Cloud usage is dramatically increasing – are your security policy controls keeping up?	**Eliminate uncertainty with security validation**	**Micro-segmentation and your security strategy**	**SAP security threat landscape 2021**
Kostas Lotsis, Senior Sales Engineer EMEA, FireMon	**Hatem Ali,** Global Services and Intelligence Lead, MEA, FireEye	**Migchiel de Jong,** Systems Engineer, Illumio	**Frederik Weidemann,** Chief Technical Evangelist, Onapsis Inc

13:10 Lunch and networking

14:10 Security through control maturity and assurance in times of rapid change

John Elliott, Director, Industry Standards, Mastercard

- Controls (and therefore compliance) deteriorate over time because of change and a lack of attention to regular tasks. This has been exacerbated by the rapid transformation many companies have gone through in the past 12 months
- Criminals are not slow to take advantage of vulnerabilities – 'do security later' is a dangerous risk decision to take. In the current landscape, criminals are likely to ransomware your computer after they have stolen cardholder data. So, the threat goes beyond just data loss to suspension of business operations
- One of the key advantages of assessments is that organisations 'discover' when a control is failing and can correct it, putting off assessments removes this independent view of your controls
- What can be done? Shift the focus to the maturity of key controls: patching & vulnerability management, log reviews

14:30 Zero trust: More than just a buzzword?

Jonathan Hallatt, Regional Sales Director, Pulse Secure

- Working from home is here to stay: the explosion of devices, data & remote workers has expanded the cyber-attack surface for organisations
- Those looking to improve secure access to mitigate cyber-risk are faced with key challenges such as over-privileged employees and shadow IT
- How can hyper-converged access address these challenges? Key considerations for actioning a zero trust model and consolidating your VPN solutions
- Looking forward: improving user experience, protecting your infrastructure when returning to the office and continuously monitoring access

14:50 Why traditional penetration testing fails: Rely instead on the wisdom of crowds

Ron Peeters, Vice President Middle East and Emerging Markets, Synack

- Learn why your current testing practices are insufficient against malicious hacking groups and state-sponsored cyber-attacks
- Discover a sophisticated offensive intelligence and attack model from the US NSA / DoD now available to organisations in the Middle East
- Hear how combining crowdsourced teams of top-class security researchers with machine learning and AI can be virtually deployed to begin finding exploits within a matter of hours
- Use case studies from the region to reduce vulnerability and harden your attack surface

15:10 EXECUTIVE PANEL DISCUSSION The cloud conundrum: Managing security and risks in the cloud

For many organisations, the adoption of cloud-based apps and storage is happening at scale. Now more than ever, information security teams need visibility and controls, they need to limit unauthorised access and they need to ensure cloud security priorities are aligned across the organisation. In this discussion, we will examine the key considerations for defining a cloud security strategy, discuss managing privacy and data protection regulations in a cloud environment and lift the lid on the big picture implications of cloud on your security staff.

Taimur Ijlal, Head of Cloud Security & DevSecOps, Network International
Shakeel Ahmed, Head of Infrastructure & IT Security, leading investment and development company based in Abu Dhabi
Sreedevi Jayachandran, Information Security and Risk Advisory, MIG Holding

15:30 Networking break

16:00 The broader context of cyber-resilience and data: Essential considerations for your organisation's ecosystem

Luna de Lange, Partner and Data Protection Officer, KARM Legal Consultants

- Effective data and cybersecurity strategies, frameworks and policies: management and implementation, for your digitisation journey
- Continuous commitment to personal data protection and privacy
- Effective, proactive management and risk-based approaches to data and security management
- Ancillary components to risk management: situational awareness, threat intelligence, testing and auditing, evolution
- Assigning accountability within your organisation: individual responsibilities, crossovers, legal and compliance considerations
- Navigating the legal and regulatory landscape in the Middle East: essentials you need to know

16:20 Combatting financial cybercrime: Insights from Western Union

Wissam Abed, Leader – Financial Intelligence Unit – Middle East & South Asia, Western Union

- Law enforcement and government authorities – collaboration, partnership & investigative assistance
- e-Crime, consumer scams, internet fraud and other financial crime types: trends in the Middle East
- Building a typology cycle – acting on intelligence & analytical process flow

16:40 The state of the CISO

Simon Brady, Managing Editor, AKJ Associates Ltd

Do Boards really value cybersecurity? Why are so many companies still focusing on the 'basics' of five years ago? And why do CISOs leave their jobs so quickly? In this session, AKJ's Managing Editor, Simon Brady, reveals our research on CISO thinking in 2021.

- Is your Board all talk and no walk?
- Do business heads care about cybersecurity?
- Has cybersecurity evolved sufficiently over the past five years?
- Is more government provision of security the answer to key problems?

17:00 Networking break **17:30** Conference close

Education Seminars

Entrust

Ponemon Middle East Encryption Trends Study

Hamid Qureshi, Territory Sales Manager, Middle East & Africa, Entrust

The 2020 Middle East Encryption Trends Study, conducted by analyst firm the Ponemon Institute, is generated from a survey of 342 IT professionals based in the Middle East and highlights how leading organisations are applying their encryption strategies, with detailed insights into the use cases that are growing the fastest.

Join this session to find out more about the:

- Growing use of encryption for emerging use cases like Docker containers and the Internet of Things
- Increasing adoption of the cloud and cloud data encryption
- Continued pain associated with managing encryption keys and how this is driving the adoption of hardware security modules

FireEye

Eliminate uncertainty with security validation

Hatem Ali, Global Services and Intelligence Lead, MEA, FireEye

If you can measure it, you can improve it. One major challenge for cybersecurity teams is establishing a measurable process of validating their security operations to be able to identify gaps in detection coverage and areas of redundancy to provide specific areas of improvement including potential saving across your security controls.

This webinar will discuss how to:

- Operationalise threat intelligence: Ensure your security controls stand up to the latest tactics, techniques and procedures used by threat actors in your region and industry
- Plan security improvements: From both a technology and process perspective
- Establish evidence-based KPIs to improve security controls
- Report the organisation's ability to mitigate pertinent cyber-risks to senior stakeholders

Join this session to uncover how security validation proves the value of your efforts and ultimately reinforces your organization's

FireMon

Cloud usage is dramatically increasing – are your security policy controls keeping up?

Kostas Lotsis, Senior Sales Engineer EMEA, FireMon

According to Gartner, 'Through 2022, at least 95% of cloud security failures will be the customer's fault.' The most significant step an organisation can take to ensure appropriate levels of cloud security is for the corporate leadership to agree that cloud computing has become indispensable and that it should be governed through planning and policy.
We will be discussing Gartner's findings.

- Why delaying cloud migrations due to an exaggerated fear of the security of cloud providers, is resulting in lost opportunity and inappropriate spending
- Why a strategic cloud strategy that is lagging behind cloud usage, is leaving a hole in governance, leading to unnecessary compliance incidents and data leakage
- The impact of a lack of skills and resources for cloud use cases
- How to secure your cloud migrations with strategy and planning

Illumio

Micro-segmentation and your security strategy

Migchiel de Jong, Systems Engineer, Illumio

Segmentation is a well-known technical concept applicable to many domains. We will discuss the current state of affairs; why segmentation is relevant and what problems it helps address. Review the problems organisations have with implementing and maintaining segmentation and how you can address those problems.

Takeaways:

- Have a good understanding of the concept of segmentation
- Understand and recognise the problems with segmentation
- How to build a segmentation strategy

Education Seminars

LogRhythm

How to build an advanced SOC with limited resources

Amjad Khader, Enterprise Sales Manager, LogRhythm

While some organisations have a 24x7 security operations centre (SOC) with teams of dedicated analysts carefully monitoring for threats around the clock, every day of the year, unfortunately, most organisations cannot afford a 24x7 SOC. The cost of having well-trained analysts onsite at all times outweighs the benefit.

In this session we will outline:

- Various security operations models – from an informal SOC to a 24x7 staffed team
- Common challenges faced by organisations with limited resources, including the dangers of an informal SOC approach
- How to balance the real cost of an informal SOC, against the potential damage caused by a data breach or uncontrolled malware
- Steps to building a SOC with limited resources

Onapsis

SAP security threat landscape 2021

Frederik Weidemann, Chief Technical Evangelist, Onapsis Inc

In the past few years, 64% of organisations' ERP systems have been breached, according to a research study by IDC. Are you aware how attackers have breached, and can break into unprotected customer SAP landscapes?

Attend this session to gain insights into:

- What attacks on your SAP systems look like
- What security challenges exist in SAP environments (e.g. S/4HANA)
- Moving to the cloud with confidence – how to address security in hybrid landscapes
- Ways to protect your organisation

OneLogin

Extortionware: Your privacy problems made public

Lonnie Benavides, Head of Infrastructure and Application Security, OneLogin

Over the last decade, ransomware has increasingly become the most popular option for hackers to monetise the access they've obtained to corporate computer systems around the world. Over the last few years, we've observed the ransomware software and techniques adapt and evolve to include the theft and exposure of private information, creating extortionware as a new breed of malicious software. This talk will provide an overview of these techniques and discuss the potential privacy and security impacts you may face as a result.

Key takeaways from this session:

- Greater understanding of the breadth of ransomware and extortionware
- The evolution of ransomware
- Prevention tools you can deploy to protect your data

ThreatConnect

Risk, threat, response: Drive complexity, time, and cost out of your security programme

Miles Tappin, VP of EMEA, ThreatConnect

Businesses of all sizes are under constant threat of cyber-attack. Making matters worse, the IoT revolution is enlarging and complicating the cyber-attack surface. Traditional security approaches will no longer work in this new environment, where security teams are drowning in vulnerabilities and alerts. Join this presentation to learn the game-changing benefits of the new Risk – Threat – Response approach to cybersecurity and risk management.

What attendees will learn:

We will explore each element of the Risk – Threat – Response paradigm in detail.

- *Risk:* Why it is necessary and possible to scope the risk scenarios that matter most to your business from a financial perspective
- *Threat:* Manage the threat landscape with a priority view into the risk scenarios that matter most to your business
- *Response:* Automate & Orchestrate response across the entire security technology stack