e-crime & cybersecurity CONGRESS

7th June 2022
Doha, Qatar

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Securing the digital nation – and the World Cup

Forthcoming events

SECURING THE LAW FIRM

5th July 2022
London

SECURING FINANCIAL SERVICES

5th July 2022
London

e-crime & cybersecurity CONGRESS

21st September 2022
Abu Dhabi

e-crime & cybersecurity SWITZERLAND

28th September 2022
Zurich

e-crime & cybersecurity MID-YEAR

19th October 2022
London

e-crime & cybersecurity NORDICS

1st November 2022
Copenhagen

e-crime & cybersecurity SPAIN

16th November 2022
Madrid

e-crime & cybersecurity BENELUX

8th December 2022
Amsterdam

For more information, please visit
akjassociates.com/contact-us

Keeping society safe

7th June 2022

The Westin Doha Hotel, Doha

All over the world, governments are trying to understand how to harness the power of technology and innovation to drive sustainable economic diversification while improving quality of life for citizens and enhancing the delivery of public services.

However, there is a price to pay for benefits of intelligent infrastructure. Increasing digitalisation and the expansion of the IoT have opened up the region's companies and public sector entities to a much broader range of potential attackers. And all of this new technology, data and connectivity must be made cybersecure at a time when attackers are becoming sophisticated.

To ensure that the benefits of digitalisation are enjoyed by societies, citizens and business, it is critical for business and government to work together, both within countries and across borders. That is why we have brought the e-Crime Congress back to Qatar, with a mix of local and foreign speakers, technical topics and useful case studies.

On behalf of AKJ Associates, welcome to this edition of the e-Crime & Cybersecurity Congress in Qatar, and please don't hesitate to reach out to a member of our team if there are any questions at all.

Simon Brady
Editor

@eCrime_Congress **#ecrimecongress**

Editor:
Simon Brady
e: simon.brady@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
t: +44 (0) 20 7242 7820
e: simon.brady@akjassociates.com

Booklet printed by:
Method UK Ltd
Baird House
15–17 St Cross Street
London EC1N 8UN
e: hello@thisismethod.co.uk

Can VPN, RDP, and Zero Trust coexist?

The shortcomings of VPNs and RDPs have long been recognised and their increased use during the COVID-19 pandemic exposed and magnified the significant security faults. Zero Trust has been developed in response to these shortcomings.

BeyondTrust reports

While Virtual Private Networking (VPN) and Remote Desktop Protocol (RDP) have been two of the go-to remote access solutions for enterprises for decades, their shortcomings have long been recognised. With the massive shift to remote work since the early days of the COVID-19 pandemic, their increased use exposed and magnified the significant security faults and other issues that were there all along.

The problem is that, while tools like VPN and RDP have their valid use cases, they are often treated by IT teams as the default ways to provide access, rather than understanding the specific use cases and then matching those use cases with the appropriate technology.

There is a common misconception that VPNs are a security tool. More accurately, VPN is a business enablement tool, which was developed to extend access and protect data in transit to outside the traditional company network.

In recent years, we've seen dozens of VPN vulnerabilities exploited in major business and government breaches. Hackers recognise that, if they can breach a VPN, they can often smoothly bypass a thick stack of traditional, perimeter-based security controls (firewalls, etc.) for complete access to a company's network. In 2020, ransomware exploded, and 52% of the time it leveraged publicly accessible RDP servers to gain an initial foothold. With threat actors increasingly focusing their efforts on remote workers and weak remote access pathways, there is urgency for organisations to better grasp their remote access risk and course correct.

The rise of Zero Trust

Inability to enforce granular access controls or the principle of least privilege, lack of remote access session monitoring and management capabilities, complex to securely implement etc.: these are only a few of the VPN shortcomings that enterprises should take into account.

Hackers recognise that, if they can breach a VPN, they can often smoothly bypass a thick stack of traditional, perimeter-based security controls (firewalls, etc.) for complete access to a company's network.

Zero Trust has been developed in response to these shortcomings and to industry trends that include remote users, dissolving network perimeters, and dynamic, cloud-based assets. It focuses on protecting resources, not logical network segments, as network segmentation is no longer seen as the prime component to the security posture of the resource.

By definition, a Zero Trust security model advocates for the creation of zones and segmentation to control sensitive IT resources. This also entails the deployment of technology to monitor and manage data between zones, and, more importantly, authentication within a zone(s). This encompasses users, applications, context, attribution, and other resources and parameters.

In addition, the Zero Trust model redefines the architecture of a trusted network inside a logical and software-defined perimeter. This can be on-premises or in the cloud. Only trusted resources should interact based on an authentication model within that construct.

Zero Trust is increasingly relevant today as technologies and processes like the cloud, virtualisation, DevOps, edge computing, edge security, personification, and IoT have either blurred or dissolved the idea of a traditional firewall and network-zoned perimeter. The seismic shift to remote working has only accelerated the demise of the traditional perimeter.

What is the role of privilege access management in this Zero Trust principle?

While Zero Trust has become a trendy catchword in IT, it's important though to call out that, in practice, this model is very specific about how things should be designed and operate. Zero Trust may not work for every environment. In practice, it is best suited for new or refreshed deployments, or to strictly control user access to sensitive resources, especially when they are connecting remotely, which is the core functionality of privilege access management.

Indeed, when applying the granularity of privileged access management, which includes secure remote

Zero Trust and privilege access management can solve remote sessions and workers' challenges and even strengthen your security posture for on-site and travelling workers.

access and endpoint privilege management, Zero Trust can ensure all access is appropriate, managed, and documented – regardless of how the perimeter has been redefined.

Together, Zero Trust and privilege access management can solve remote sessions and workers' challenges and even strengthen your security posture for on-site and travelling workers. Indeed, we are now challenged with securing significantly more remote workers than in years past – many of them working from home. A secure remote access solution using a zero-trust architecture can ensure these resources are managed from potential inappropriate connection abuse and that all applications are executed within a Zero Trust model. This means no end users are ever trusted for a remote session unless the confidence for execution can be measured. This is true for any location an asset may reside, irrespective of the perimeter.

So how to ensure that organisations have it right?

Well, here are 7 tips for maturing your Zero Trust security controls as far as remote access is concerned:

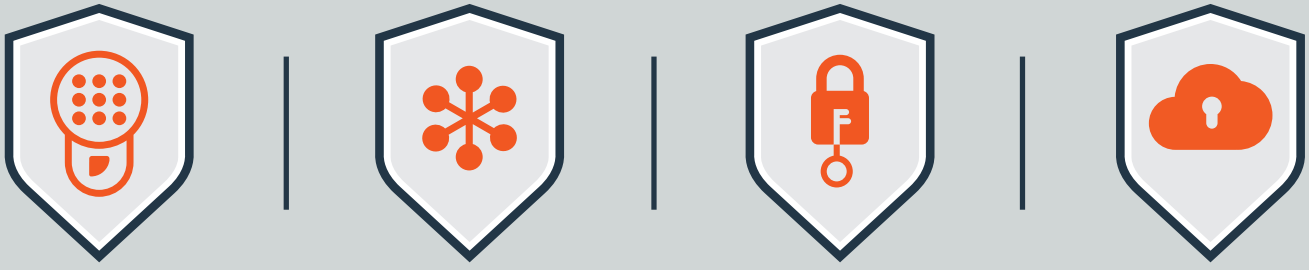
1. Disable remote access protocols (RDP, SSH, VNC, etc.) as a default on computing devices.
2. Implement a remote access solution that doesn't require inbound Internet connections.
3. Inject managed credentials to initiate the remote access session, always obfuscating the credentials from the end user.
4. Enforce least privilege across all remote access sessions with privilege elevation strictly controlled.
5. Apply just-in-time access policies.
6. Implement application-level micro-segmentation that prevents users from discovering apps they are not authorised to access.
7. Fully monitor, manage, and audit every privileged remote access session. Alerts should be issued around inappropriate commands typed, for instance.

From this perspective, privileged access management (PAM) is a key piece of the Zero Trust approach. PAM solutions can help organisations accomplish the above list, and everything from securing remote access for privileged users and vendors, to enforcing least privilege across all users, sessions, and assets, to managing all privileged credentials and secrets. This also means replacing inappropriate use of VPNs, RDP, and other remote access tools and protocols. □

BeyondTrust

UNIVERSAL PRIVILEGE MANAGEMENT

Secure and protect privileges across passwords, access, and endpoints to stop data breaches and achieve compliance



Privileged Password Management

Endpoint Privilege Management

Secure Remote Access

Cloud Privilege Protection

beyondtrust.com

Thinking differently to track down ransomware

We're no longer dealing with WannaCry and NotPetya, in fact today's attacks don't rely on malware at all – at least not until it's too late. So, what has changed? And more importantly, how do we stop it?

Vectra AI reports

Solving ransomware requires a new way of thinking. That might sound obvious to some, but when you consider that 65,000 ransomware attacks are expected by the end of the year – many of the current security systems and strategies just aren't up to the task. We're no longer dealing with WannaCry and NotPetya, in fact today's attacks don't rely on malware at all – at least not until it's too late.

So, what has changed? And more importantly, how do we stop it?

Ransomware, but not like the old days

At its core, ransom has always been about an item of value being held until price demands were met. And while that remains the same, the approach these days is much different. We're no longer seeing malware doing all the work to spread throughout a network, encrypting files along the way – that's the good news. The challenge, however, is that the effort and innovation put forth by ransomware groups like REvil and Darkside make it more accessible for criminals to launch attacks.

Not only are ransomware attacks becoming more commonplace, but they're also more difficult to detect. This is because there's no sign of ransomware until the very end of an attack. Up until that point, you're just trying to uncover unusual activity inside your systems that may or may not be recon conducted by attackers. This is where traditional security measures and prevention tools fail.

Detecting in-progress attacks

While these attacks can't be prevented by traditional security measures, it is possible to detect attacker activity that exists in your environment. This can also be done in a way that will allow security teams to contain malicious events in a timely manner. Time being the key here as Dark Reading recently reported that the global dwell time attackers remain inside an environment continues to drop.

Organisations are up against the clock when it comes to detecting attackers, and the tactics many criminals use today appear just like that of authorised users. This is where AI-driven threat detection and response can lend a hand. A good example of this can be seen in the recent Vectra Spotlight Report – Vision and Visibility: Top 10 Cybersecurity Threat Detections for Microsoft Azure AD and Office 365. The data shows specific examples of how security teams are using AI to detect and stop abnormal or unsafe activity that could lead to costly attacks.

AI-driven threat detection and response sees the telltale signs of ransomware at its earliest stages so organisations can stop it before encryption occurs.

The report discusses the top detections that customers use to mitigate malicious activity such as suspicious download and sharing activity and even mail forwarding techniques that could be used as an exfiltration channel. It's important to recognise that attacker behaviour typically comes in multiple stages and way beyond the initial compromise or entry. This could mean privilege escalation, persistence, lateral movement, internal recon and discovery, credential access, command and control and a multitude of other tactics. All of this activity is representative of human attacker behaviour inside an environment while attacks are being set up.

The bottom line is that organisations need to account for the complexity of today's expanded attack surface. This means having coverage that accounts not just for the extended enterprise, but the sophistication of ransomware operators along with the limitations of traditional security tools and the overall shortage of cybersecurity professionals.

AI-driven threat detection and response sees the telltale signs of ransomware at its earliest stages so organisations can stop it before encryption occurs. Security teams can also leverage AI to augment workloads, optimise analyst-based investigation and automate labour intensive threat hunting activities. Get to see first-hand how Vectra can track down ransomware in your environment, take a self-guided tour today. □

For more information, please visit
vectra.ai

VECTRA®

FIND and STOP RANSOMWARE

Ransomware is evolving, your threat detection and response approach better keep up.

Vectra's AI-driven threat detection and response platform allows you to:

- **Detect and respond** to intent-based behavior across everything, everywhere.
- **Agentless solution** for always-on security and no business disruptions.
- **Zero rule-writing.** AI-driven detection spots all stages of ransomware attacks.

Learn how to recognize the signs.
Schedule a demo by visiting
https://www.vectra.ai/demo

VECTRA®
SECURITY THAT THINKS.®

Just-in-Time

By 2025, 75% of cyber-insurance companies will require the use of the JIT principle when implementing Privileged Access Management (PAM)… so get ready as soon as possible with WALLIX PAM4ALL!

WALLIX reports

The digital transformation of companies and the need for remote access to information systems means that the type and number of privileged users is constantly increasing. It is therefore essential to reduce and control the footprint of privileged access in the environment by controlling their scope and duration**.** Reducing the risks associated with the abuse of privileged access, or even eliminating privileges altogether (Zero Standing Privilege – ZSP), is the very principle of Just-In-Time (JIT).

As Gartner points out, by 2025, 75% of cyber-insurance companies will require the use of the JIT principle when implementing Privileged Access Management (PAM)… so get ready as soon as possible with WALLIX PAM4ALL!

Why Just-in-Time?

Just-in-Time access security is a fundamental practice that helps reduce excessive access privileges and is a key tool in implementing the Principle of Least Privilege and the Zero Trust security model. JIT grants users, processes, applications, and systems specific rights and access to perform certain tasks for a predefined period of time.

As a policy, Just-in-Time security aims to minimise the risk of standing privileges to limit risk and exposure to potential cyber-attacks. When too many users have too many privileges at all times, the chances of credential theft, exploitation, and escalation to steal secrets, encrypt data, or bring systems to a halt increase exponentially. Granting elevated privileges only when needed – no more and no less – restricts exposure to a minimum while still allowing users to get on with their work.

Thanks to Just-In-Time, an always-on privileged account can very easily be reduced from a permanently active state to just a few minutes. If this approach is applied to all accounts, risks will be reduced extremely quickly. However, JIT will not only protect your accounts thanks to the time factor but also mitigate attack vectors that use techniques such as lateral movement, preventing malicious actors from advancing and elevating their privileges on the network.

How does JIT work?

The purpose of Just-In-Time security is to automatically assign the privileges a user needs on the fly and address the 3 main access factors: location, time, and actions.

There are many contextual JIT rules and triggers depending on the uses and characteristics of privileged accounts based on rights, approval workflows, and multi-factor authentication. In each case, it is important to ask what rules govern the use of a JIT access and what conditions must be met for revocation.

How to implement JIT?

The first step would be to audit all user access privileges, company-wide, to determine the scope and scale of the problem. How many users are there? What are their profiles and what applications and systems do they typically request access to?

Based on the answers, the next step will be to establish an internal policy to define the requirements users must meet if they wish to gain access to the target systems: For how long should access be granted? To which functions and equipment? And under what conditions?

You'll also need to regain control over all passwords and credentials to target systems. Centralising management and rotation of passwords to applications and IT assets is critical to ensuring comprehensive risk and vulnerability management.

We can now say that you are fully prepared to adopt the 'Just-in-Time' security policy, all that remains is to implement the WALLIX PAM4ALL solution!

WALLIX PAM4ALL **offers a concrete answer to the problems posed by always-on accounts**. PAM4ALL is the unified privilege and access management solution that allows you to secure, control and manage all user access (whether human or machine, from IT administrators to employees or subcontractors), laying the foundations of a Zero Trust architecture. □

For more information, please visit
www.wallix.com

WALLIX
CYBERSECURITY SIMPLIFIED

Protect your digital future

WALLIX PAM4ALL*

Regain control of your access!

Remote working and new digital uses have led to an exponential growth in the number of access to corporate infrastructures. With WALLIX PAM4ALL, the unified privilege management solution, you can manage access in a granular way by tightly defining targets, uses and durations, thus minimizing the risks associated with connections and privileges. PAM4ALL reduces your attack surface without affecting productivity and in compliance with regulations.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED

*PAM4ALL: Privileged Access Management for all

Taegis™ XDR for the Win

Discover how Taegis XDR maps to specific MITRE ATT&CK tactics, techniques, and procedures. Then test how the platform will respond to specific threats in your IT environment.

Test drive yourself today!

secureworks.com/taegis

Secureworks® | Taegis™

Why and how to build a proactive incident response plan

A thorough and well-tested incident response plan can enable organisations to quickly mitigate and recover from a compromise.

Organisations have historically relied on a piecemeal, ad-hoc approach to managing cybersecurity incidents. This approach does not scale as threat actors become more sophisticated, attacks are more complex, and advanced malware tools and services become widespread and easy to use. A reactive approach can increase the time and costs associated with an incident. According to a 2021 report, the average cost of a data breach is more than $4.24 million. Developing and testing an incident response (IR) plan to limit the impact of a compromise is paramount for all organisations, regardless of size or business model.

Why develop an incident response plan?

Organisations should implement preventive cybersecurity measures to limit risk. Endpoint detection tools, antivirus software, and security controls can block many threats. Training employees to recognise and report social engineering attacks and other suspicious activity is crucial. However, a threat actor may circumvent these protections. An established IR strategy can help mitigate the impact of a compromise, reduce downtime, and limit data loss and costs.

An IR plan outlines the roles and responsibilities of each team member during an incident. A good plan includes information technology and information security staff, and other important roles (e.g., legal, compliance, audit, human resources, finance, operations, physical security, communications) and applicable third-party providers. It defines the strategies, objectives, tools, and steps to declare, investigate, analyse, contain, and eradicate the incident. Developing and testing a comprehensive IR plan has multiple benefits:

- *Protect confidential data:* Data protection is vital. Organisations must understand what data is used and stored in their environment and how it is classified and protected. Costs associated with failure to properly secure confidential data include penalties, fines, and legal fees. Threat actors often sell stolen data on underground forums or leverage it in ransomware or social engineering attacks for financial gain. Stolen personally identifiable information (PII) can also lead to identity theft.
- *Limit the financial impact:* A compromise can have substantial financial implications. If business operations are affected, the organisation loses revenue during downtime. There may be fines, legal fees, compliance penalties, and costs associated with investigating the incident, replacing software or hardware, adding security measures, and increasing marketing and public relations efforts. The faster an organisation responds to and recovers from a compromise, the lesser the financial burden.
- *Preserve reputational integrity and customers' trust:* A compromise can negatively impact an organisation's reputation and even stock prices, especially if it is mismanaged or resulted in extended downtime. Customers want to be confident an organisation is doing everything in its power to protect their data. If an organisation fails to respond quickly and effectively to a cybersecurity incident, customers can feel betrayed and search for alternate providers.

How to build a proactive incident response plan

There are many layers to a good cybersecurity defence, and these layers may differ across organisations. An IR plan must contain the necessary steps to address a worst-case scenario and return to business as usual as quickly as possible, minimising interruption to the business and customers. A proactive IR plan should incorporate:

- *Planning and preparation:* Everyone involved in responding to an incident must understand the overall IR strategy and their specific role. They must have the necessary training and tools to fulfil their duties. The plan should identify a backup for each person if the primary contact is unavailable. Defining communication channels and escalation procedures may be the most important aspects of an IR strategy, as efficient communication facilitates a prompt response. As applicable, incident responders should comply with annual continuing education requirements. For example, standards such as Payment Card Industry Data Security Standard (PCI DSS) require at least 24 hours of continuing education each year.
- *Identification and investigation:* Many organisations use a combination of internal monitoring and third-party managed security service provider (MSSP) solutions to detect and

Secureworks reports

By proactively developing and testing an IR plan, an organisation ensures it can effectively and thoroughly respond to cybersecurity incidents and minimise damages, downtimes, and losses.

alert on suspicious activity. They must establish a process for investigating alerts, reporting malicious activity, and escalating security incidents. The IR plan should document this workflow.

- *Analysis:* Organisations should have procedures for capturing a forensic copy of memory and disk images on compromised assets so they can conduct a thorough analysis. Many organisations do not have the capabilities to perform rapid forensic analysis of a malware payload themselves, but their MSSP or another third-party provider may be able to conduct this type of analysis within hours or days.
  - Search systems and networks for evidence left by the threat actor.
  - Analyse tools, malware payloads, or binaries the threat actor leveraged in the attack.
  - Document the compromised systems, networks, devices, and accounts to determine the scope of the incident.

  This forensic analysis can reveal valuable data such filenames, IP addresses, port information, hashes, heuristic information, URLs, compromised account information, and applications used in the attack. The information enables the organisation to determine the best actions to repair damages and prevent further attacks.
- *Containment:* Incident responders contain the incident by rendering malware payloads benign or by locating all malware artifacts and isolating impacted endpoints from the network. To contain damages, the incident responders coordinate shutdowns of all compromised systems until the threat is mitigated. They should wipe and rebuild affected systems and methodically change login credentials of all accounts.
- *Eradication:* After collecting the forensic information and containing the incident, it is critical to remove the threat actor from the environment and block access vectors to prevent re-entry. Actions may include patching exploited vulnerabilities or increasing employee training about phishing attacks.
- *Recovery:* As the organisation resumes normal business operations, incident responders should monitor for indications the threat actor is attempting to re-enter the network. They should closely monitor network traffic, help-desk calls, advanced security tools (e.g., firewalls, endpoint detection tools), and logs. Other team members may focus on developing a risk mitigation strategy and a remediation strategy to protect the organisation from future incidents.
- *Post-incident review:* This is often the most overlooked part of an IR plan, but it is extremely important. It enables the organisation to learn from the incident and identify opportunities to enhance their IR plan, playbooks, security tools, and strategies. The IR team will likely need to produce a detailed written report describing the incident for stakeholders such as executive leadership, board of directors, audit and compliance staff, internal counsel, and their cyber-insurance firm.

Testing the plan

Developing an IR plan is not enough. It should be tested and reviewed at least once a year to ensure it addresses all necessary steps and all team members understand the process. Mock tabletop exercises are effective for testing. Everyone with a role or responsibility in the plan should participate to identify areas of concern and hone the plan. Ideally, a neutral third-party coordinates, analyses, and critiques the exercise. Following the critique, the organisation should implement any necessary changes and retest the plan as soon as possible.

Conclusion

The cyber-threat landscape continues to evolve, and organisations cannot afford to rely on a reactive approach. By proactively developing and testing an IR plan, an organisation ensures it can effectively and thoroughly respond to cybersecurity incidents and minimise damages, downtimes, and losses. □

Sponsors and exhibitors

BeyondTrust | Strategic Sponsor

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organisations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organisations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organisations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including more than 70% of the Fortune 500, and a global partner network.

Learn more at www.beyondtrust.com

Redington Gulf | Strategic Sponsor

Redington Gulf is amongst the leading supply chain solution providers in the Middle East, Africa, Turkey and CIS region for leading manufacturers of information technology, telecom and lifestyle products.

For more information, please visit redingtongroup.com/mea/overview

Secureworks | Strategic Sponsor

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security operations and analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information please visit www.secureworks.com

Anomali | Education Seminar Sponsor

Anomali® detects adversaries and tells you who they are. Organisations rely on the Anomali Threat Platform to detect threats, understand adversaries, and respond effectively. Anomali arms security teams with machine learning optimised threat intelligence and identifies hidden threats targeting their environments. The platform enables organisations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide.

For more information, visit us at www.anomali.com and follow us on Twitter @Anomali

Cofense | Education Seminar Sponsor

Millions of ransomware, business email compromise and credential harvesting attacks bypass expensive email security solutions every year. They are in your users' inboxes right now.

Cofense is the only company that combines a global network of 30 million people reporting phish with advanced AI-based automation to stop phishing attacks fast. That's why over half of the Fortune 500 trust us.

We're Cofense. We Stop Phish.

Our Phishing Detection and Response platform catches the phishing emails that your secure email gateway inevitably misses. We deliver the technology and insight needed to detect, analyse, and stop phishing attacks.

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organisations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of nearly 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organisations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defence, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise.

For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn

emt Distribution | Education Seminar Sponsor

emt Distribution offers one of the best platforms that brings together vendors from varied disciplines within information security, cloud, virtualisation and service management disciplines. With market intelligence and regular feedback from the Middle East region, emt Distribution knows what technology is best in demand and how to market your products in the region.

emt Distribution believes in providing the best products and services to its end users. Whether this means developing strategy for the best products in the region or training partners in all parts of the Middle East, we ensure the best experience for our customers when they choose our portfolio.

emt Distribution's Award winning 'Magnitude Partner Program' has developed partners in various parts of the Middle East, Turkey, North, West Africa and parts of Asia develop significantly.

Partners in the region can benefit from:

- Market development
- Partner program development
- Rebranding and localisation
- Training
- Sales and marketing platforms
- Business development and technical teams on the ground

For more information, please visit www.emtdist.com

Malwarebytes | Education Seminar Sponsor

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus solutions to remove the personal obstacles and business interruptions caused by modern cybersecurity threats. More than 10,000 businesses and millions of people trust Malwarebytes innovative machine-learning solutions and global team of researchers to identify emerging threats and to prevent and eradicate malware that antiquated security solutions miss and leave behind.

Malwarebytes founder and CEO Marcin Kleczynski started the company to create the best disinfection and protection solutions to combat the world's most harmful Internet threats. Marcin was recently named 'CEO of the Year' in the Global Excellence awards and has been named to the Forbes 30 Under 30 Rising Stars of Enterprise Technology list and the Silicon Valley Business Journal's 40 Under 40 award, adding those to an Ernst & Young Entrepreneur of the Year Award.

For more information, please visit www.malwarebytes.com/business

ManageEngine | Education Seminar Sponsor

As the IT management division of Zoho Corporation, ManageEngine prioritises flexible solutions that work for all businesses, regardless of size or budget. ManageEngine crafts comprehensive IT management software with a focus on making your job easier. With our 90+ products and free tools covering everything your IT needs, you can take complete control of your IT infrastructure and services – both on-premises and in the cloud.

For more information, please visit www.manageengine.com

Paramount | Education Seminar Sponsor

Paramount is the leading cybersecurity provider for companies across the Middle East enabling customers to protect their critical information assets and infrastructure through a prudent combination of people, process and technology.

Find us at: https://www.paramountassure.com/

OPSWAT | Education Seminar Sponsor

OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organisations from malware and zero-day attacks. To minimise the risk of compromise, OPSWAT Critical Infrastructure Protection solutions enable both public and private organisations to implement processes that ensure the secure transfer of files and devices to and from critical networks. More than 1,000 organisations worldwide spanning financial services, defence, manufacturing, energy, aerospace, and transportation systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations, and protect their reputation, finances, employees and relationships from cyber-driven disruption.

For more information on OPSWAT, visit www.opswat.com

Synack | Education Seminar Sponsor

Synack, the most trusted crowdsourced security testing platform, delivers on-demand security testing, intelligence, and operations through a continuous, offensive SaaS platform with crowdsourced talent. The company combines the world's most skilled and trusted ethical hackers with AI-enabled technology to create a scalable, effective security solution. Headquartered in Silicon Valley with regional offices around the world, Synack protects leading global banks, the top 10 global consulting firms and security companies, DoD classified assets, and over $2 trillion in Fortune 500 revenue. Synack was founded in 2013 by former NSA security experts Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.

For more information, please visit us at www.synack.com

Vectra AI | Education Seminar Sponsor

Vectra® is a leader in threat detection and response for hybrid and multi-cloud enterprises. The Vectra platform uses AI to detect threats at speed across public cloud, identity, SaaS applications, and data centres. Only Vectra optimises AI to detect attacker methods – the TTPs at the heart of all attacks – rather than simplistically alerting on 'different'. The resulting high-fidelity threat signal and clear context enables security teams to respond to threats sooner and to stop attacks in progress faster. Organisations worldwide rely on Vectra for resilience in the face of dangerous cyber-threats and to prevent ransomware, supply chain compromise, identity takeovers, and other cyber-attacks from impacting their businesses.

For more information, visit vectra.ai

WALLIX | Education Seminar Sponsor

A software company providing cybersecurity solutions, WALLIX is the European specialist in digital identity and access security solutions. WALLIX PAM4ALL, the unified privilege management solution, enables companies to respond to today's data protection challenges. It guarantees detection of and resilience to cyber-attacks, which enables business continuity. The solution also ensures compliance with regulatory requirements regarding access to IT infrastructures and critical data. WALLIX PAM4ALL is distributed through a network of more than 300 resellers and integrators worldwide. Listed on the Euronext (ALLIX), WALLIX supports more than 1,900 organisations in securing their digital transformation. WALLIX is a founding member of the HEXATRUST group and has been included in the Futur40, the first ranking of growth companies on the stock exchange published by Forbes France and is part of the Tech 40 index.

For more information, please visit www.wallix.com

Orchestra Group | Networking Sponsor

Orchestra Group's mission is to address the major roadblocks that make it difficult for CISO, CIO, and their teams to manage cybersecurity, such as:

1. Fragmented technologies using different paradigms for each slice of the cybersecurity puzzle leading to a cyber stack of between 25 to120 different technologies in every large organisation.
2. Lack of standard metrics to measure, manage, and benchmark cyber-defence. This is crucial to drive efficiency, effectiveness, and continuous improvement of organisations' security.
3. Constant change is now the norm for business and IT. Cybersecurity requires constant tuning of the trade-offs between shifting IT\Business needs and cyber-risk.

Orchestra Group is promoting the following solutions:

Harmony IoT – a unique solution that provides an airspace dome around the organisation to monitor, detect threats and mitigate cyber-attacks through the attack surface of WiFi and Bluetooth protocols, and smart-connected devices & IoTs using them.

It delivers visibility, continuous monitoring and real time attack mitigation.

What makes it different from traditional network access control (NAC) and mobile device management (MDM) is it monitors the airspace rather than the devices.

Its policy engine makes it easy to establish effective airspace security hygiene to ensure the devices operating in your airspace are configured to meet your wireless security standards.

Harmony Purple – a next-generation Automated Purple team tool that continuously showcases validated, global, multi-vector, Attack Path Scenarios™ (APS) and creates risk modelling-based prioritisation, so red and blue teams can focus their time and resources on those vulnerabilities that threaten critical assets and business processes.

It unifies scanning, penetration testing, network analysis, risk prioritisation and remediation. It's easy to use and automated – and because it is low impact, scans can be run anytime on production systems.

For more information, please visit orchestragroup.com

SOCRadar | Branding Sponsor

We're one of the fastest-growing cybersecurity companies in the world. Enterprises around the world are increasingly selecting SOCRadar to get proactive by understanding their attack surface and gaining automation-enabled visibility into surface, deep, and dark web. Our customers worldwide leverage our expertise and investment in scalable, innovative solutions to protect their most valuable assets: brand reputation, employees, customers and overall business operations.

Visit us at socradar.io

AGENDA

08:00	Registration and networking break
08:50	Chairman's welcome
09:00	**Closing the cybersecurity skills gap** **Shaik Abdulkhader,** CISO for Leading Energy Company in Qatar In the new digital world, our livelihoods are more 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. • Introduction – cybersecurity skills • Widening cybersecurity skills gap • Challenges in cultivating the cybersecurity talent • Global response & solutions
09:40	**Education Seminars | Session 1** **See pages 20 and 21 for more details** **OPSWAT** **Critical infrastructure protection by OPSWAT** **Sertan Selcuk,** Regional Sales Director, META, OPSWAT **Vectra AI** **How AI-based 'threat detection & response' finds and stops ransomware** **Abdullrazaq Zahran,** Security Engineering Manager | META, Vectra AI
10:20	Networking break and refreshments
10:50	**FIFA World Cup 2022 and privacy** **Imran Chowdhury,** Global Data Protection Officer, Al Jazeera Media Network • Millions of fans are expected to visit Qatar during the FIFA World Cup. With global privacy regulations on the rise, how do organisations in Qatar stay compliant? • What are the main accountabilities organisations should focus on? • Is complying with FIFA Cybersecurity Framework enough to stay compliant?
11:10	**Is XDR your must-have cybersecurity solution?** **Paul John,** Cloud Architect, Secureworks Extended detection and response (XDR) delivers visibility into data across networks, clouds, endpoints, and applications while applying intelligence, analytics and automation to detect, analyse, hunt, and remediate today's and tomorrow's threats. In this session learn: • What to consider in an XDR framework? • The best XDR strategic approach • How to improve security operations productivity • Precision threat detection and immediate response
11:30	**Education Seminars | Session 2** **See pages 20 and 21 for more details** **Synack** **Offensive and continuous security testing – the emerging standard beyond traditional penetration testing** **Ron Peeters,** Vice President Middle East/Emerging Markets, Synack **WALLIX** **Regain control of your access with WALLIX PAM4ALL** **Afi Hashim,** Regional Manager, Middle East, Turkey & India, and **Danish Khan,** Presales Manager, WALLIX
12:10	Networking break and refreshments
12:30	**Building a human firewall** **Sirajhusen Modi,** System Sec Head, Al Meera Consumer Goods • How to strengthen our human firewall: User awareness and what tools to use • Give training to weakest group of people • Hiring process – what is important

12:50 **Education Seminars | Session 3** See pages 20 and 21 for more details

Anomali
Infinity war: Continuous use of infinite insights to detect attacks and stop breaches
Parthi Sankar, CISSP, Technical Director N.Europe, Anomali

Malwarebytes
Incident response in the age of ransomware and data protection
Kapil Matta, Regional Manager, Enterprise – MEA, Malwarebytes

13:30 Networking and lunch break

14:20 **EXECUTIVE PANEL DISCUSSION** **Does the blockchain create more security headaches than it solves?**

Prof. Dr. Roberto Di Pietro (Moderator), Professor of Cybersecurity, HBKU College of Science and Engineering; **Radhakrishnan M,** Innovation Lead/Chief Technology Advisor, Chapter Lead – Government Blockchain Association, Qatar; **Giorgio Torre,** Project Manager, Leading Consulting Firm; **Hani Al Khatib,** Card Payments Expert, Leading Bank in Qatar

- Are cryptocurrencies just a distraction?
- Are blockchains really more secure?
- Security in public versus private ledgers
- Cybersecurity in a blockchain-dominated world

14:40 **Zero Trust: Getting least privilege right, finally**

Michael Byrnes, Director of Solutions Engineering iMEA, BeyondTrust

- 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

15:00 **Education Seminars | Session 4** See pages 20 and 21 for more details

Cofense
Adaptive email security architecture: Moving from incident response to continuous response
Alaa Abu Gharbieh, Regional Sales Manager – META, Cofense

ManageEngine
Cybersecurity automation in SecOps
Karthik Ananda Rao, Chief Technical Evangelist, ManageEngine

15:40 Networking break and refreshments

16:00 **Security enhancements for 5G wireless networks**

Dr. Maode Ma, Research Professor, Qatar University

- Introduction to 5G wireless network architecture
- Vulnerability and threats in the space
- Motivation to secure
- Examples of enhancement
- Open research issues
- Conclusion

16:20 **Role of Security Operation Centre (SOC) during cyber-attacks**

Davar Dattawala, Cybersecurity CD Manager, Ooredoo

- SOC is the backbone of your cybersecurity programme
- Importance of onboarding of assets in SIEM
- Role of 'use case' and 'fine-tuning' leading to true positive incidents
- Incident responder and forensics during and after the cyber-attack

16:40 **European approach to data protection, lessons learned after 4 years of GDPR**

Maarten Stassen, Partner – Lawyer, Crowell & Moring LLP

On 25 May 2022, we celebrated the fourth birthday of the General Data Protection Regulation (GDPR). During this session, we will discuss the following topics:

- What has happened since 25 May 2018?
- How to manage GDPR in an international environment
- European enforcement: should international companies be worried?
- How did our digital lives change?
- Is European data now truly better protected than before?

17:00 Conference close

Education seminars

Throughout the day a series of education seminars will take place as part of the main agenda. Delegates will be able to choose to attend any of the seminars, all of which will provide vendor-neutral, hands-on advice. Seminars within each session run concurrently.

Session 1: 09:40–10:20

OPSWAT

SESSION 1
09:40–10:20

Critical infrastructure protection by OPSWAT

Sertan Selcuk, Regional Sales Director, META, OPSWAT

How can file transfers be secured across the entire enterprise, especially between uncontrolled devices? Sertan Selcuk, META Regional Sales Director at OPSWAT will explain how to secure files transfer into, across, and out of secure environments to avoid malware and/or data breach.

- Breach prevention with multiscanning
- Cybersecurity compliance
- Digital perimeter control with automated device blocking
- Secure file transfer with automated media blocking

Vectra AI

SESSION 1
09:40–10:20

How AI-based 'threat detection & response' finds and stops ransomware

Abdullrazaq Zahran, Security Engineering Manager | META, Vectra AI

Cybercriminals are always looking for easy targets and opportunities to steal personal information. With no application, network, or data centre being invulnerable, decision-makers often harbour a false sense of security about their ability to fend off hackers – especially when they're not armed with the necessary tools to succeed.

During our presentation, we will cover:

- How prepared your organisation is to detect and respond to a ransomware attack
- What approaches other organisations are taking to stop ransomware gangs
- How to detect and respond to ransomware before it impacts you

Session 2: 11:30–12:10

Synack

SESSION 2
11:30–12:10

Offensive and continuous security testing – the emerging standard beyond traditional penetration testing

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

Increasingly sophisticated cyber-attacks can easily exploit serious Vulnerabilities in live systems that you are not aware of TODAY, are not found with the common vulnerability scanning tools and neither by traditional penetration testing. Hence the need for a new, next generation approach of offensive security testing that better mimics and preempts malicious attack behaviour.

In this session, you'll learn:

- Why the current model of compliance-based penetration testing is increasingly ineffective and obsolete
- Which exploitable vulnerabilities are missed the most and cause the greatest concern
- How a model combining highly skilled security researchers (with a hacker mindset) deployed in large cohorts provides the necessary critical mass
- Several customer examples in the Middle East benchmarking the advantage of offensive security testing

WALLIX

SESSION 2
11:30–12:10

Regain control of your access with WALLIX PAM4ALL

Afi Hashim, Regional Manager, Middle East, Turkey & India, and **Danish Khan,** Presales Manager, WALLIX

Remote workforce, migration to the cloud, equipment multiplication, and new digital uses are leading to an explosion in the number and type of access to companies' critical assets. Face this challenge with PAM4ALL, the Unified Privilege Management solution that enables you to easily secure, control, and manage all your access. During this session, discover how

WALLIX can help you reduce your threatscape by treating every user as a privileged user while keeping simplicity at the administration level.

During this session, you will discover:
- How to prevent credentials theft from external attacks
- How to stop lateral & vertical movement
- How to prevent privilege escalation and insider threat
- How to control third-party access
- How to meet audit and compliance requirements

Session 3: 12:50–13:30

Anomali

SESSION 3
12:50–13:30

Infinity war: Continuous use of infinite insights to detect attacks and stop breaches

Parthi Sankar, CISSP, Technical Director N.Europe, Anomali

Learn how The Anomali Platform uses big data management, machine learning, and the world's largest intelligence repository in order to:
- Automatically and continuously correlate ALL security telemetry against active threat intelligence
- Enable organisations to understand what's happening inside and outside their network to stop breaches
- See how Anomali ties attack infrastructure to threat actors, campaigns and MITRE ATT&CK® to predict and stem the next attack

Malwarebytes

SESSION 3
12:50–13:30

Incident response in the age of ransomware and data protection

Kapil Matta, Regional Manager, Enterprise – MEA, Malwarebytes

Recent trends – current industry situation and ransomware NIST Framework and ransomware incident response automation lever for next gen SOC Malwarebytes value proposition.

Key take aways:
- 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

Session 4: 15:00–15:40

Cofense

SESSION 4
15:00–15:40

Adaptive email security architecture: Moving from incident response to continuous response

Alaa Abu Gharbieh, Regional Sales Manager – META, Cofense

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.

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.

This session will cover:
- 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

ManageEngine

SESSION 4
15:00–15:40

Cybersecurity automation in SecOps

Karthik Ananda Rao, Chief Technical Evangelist, ManageEngine

In this presentation, we will demonstrate on how SecOps can help regulate an organisation's cybersecurity risk exposure by incorporating SOAR and SOC technologies. This automation of cybersecurity processes helps to prioritise, detect and respond to threats effectively by regulating business operations from password management to endpoint and data security.

- Seamlessly collaborate between IT security and IT operations
- Automate crucial security tasks, reduce cybersecurity risk and improve agility
- Create a centralised function by continuously monitoring and improving security infrastructure
- Detect anomalies and report on any unusual activity by UEBA □

Speakers and panellists

The e-Crime & Cybersecurity Congress in Qatar is delighted to welcome delegates, speakers and panellists. The event has attracted a large number of key names and decision-makers across industry.

Shaik Abdulkhader

CISO,
Leading Energy Company in Qatar

Shaik Abdulkhader is a proven visionary cybersecurity leader with 28+ years of experience with strong business acumen and excellent working knowledge of cybersecurity, IT, IOT, IIOT & OT technologies. He has highly diversified industry exposure and multi geography experience, having excellent knowledge of business & IT systems, products, solutions, platforms & services in banking, oil & gas, manufacturing, telecom & government sectors and has been associated with the biggest global brands like TCS, Vodafone, QNB, IBM, QAPCO etc at various technical & leadership roles.

Alaa Abu Gharbieh

Regional Sales Manager – META,
Cofense

Hani Al Khatib

Card Payments Expert,
Leading Bank in Qatar

Hani holds a bachelor's in Computer Science, and a master's degree in Blockchain Technology, with a total experience of 10 years in the card payments space. He participated in several digitisation and automation projects to enhance traditional banking services. Being in the blockchain space, Hani carries a comprehensive view of blockchain applications and use cases from the public and private sectors.

Karthik Ananda Rao

Chief Technical Evangelist,
ManageEngine

Karthik Ananda Rao has over 20 years of IT experience, having started his career as a Network Administrator at Zoho. Today, he is the Chief Technical Evangelist for ManageEngine and heads the Technical Research and Marketing Team for MENA region. He has hands-on experience in all IT domains – vis-à-vis – IT/Enterprise Service Management, IT Operations Management, Active Directory and Identity Management, Security and Information Event Management, Unified Endpoint Management, Privileged Access Management, and Data Analytics. He represents ManageEngine at all trade shows and events, be it physical or virtual, across MENA primarily (and the rest of the world, depending on his activity schedule) and leads the team during webinars and seminars. He is an enthusiastic speaker and is often spotted at industry events across the region. He has had the privilege of delivering guest lectures at quite a few educational institutions across Oman, Malaysia, India, France, Morocco, Belgium, UK and the US.

Michael Byrnes

Director, Solutions Engineer iMEA,
BeyondTrust

Michael Byrnes is the Director, Solutions Engineer iMEA for BeyondTrust. He has acquired a wealth of cybersecurity experience in a number of engagements over the last 10 years with a diverse set of IT companies across the Middle East. Thanks to his various roles as a Security Consultant, a Systems Engineer or within pre-sales, he gained extensive expertise in network and information security, architecture design and virtualisation. Within his current position at BeyondTrust, Michael manages the solution engineers' team in the Middle East, India and Africa. With his group, he engages and advises partners, customers and prospects in their Privileged Access Management (PAM) strategy to secure and manage their entire universe of privileges.

Imran Chowdhury

Global Data Protection Officer,
Al Jazeera Media Network

Imran Chowdhury is a data trust professional with extensive experience in privacy, cybersecurity, and data governance. Imran brings together a diverse professional experience of over 25 years in technology in establishing data trust. When asked, he says he likes to connect dots. His expertise in business architecture, portfolio management, service management, project management, governance, risk, and compliance comes together in his work with an entrepreneurship spirit. His own experience in establishing a digital-first organisation gives him a unique insight to establish the right level of governance as an organisation moves

from inception to maturity. Imran feels passionate about user trust in the digital world and believes that the organisation needs to establish that trust with its users. Imran is the Global Data Protection Officer at Al Jazeera Media Network, where he launched the Privacy function.

Davar Dattawala

Cybersecurity CD Manager, Ooredoo

An established and certified professional, bringing to the table 17+ years of cybersecurity and information risk management experience, Davar possesses proficiency in offensive and defensive cybersecurity measures based on anticipated risks across assigned programmes. He can establish effective BCP & DR plans according to project risk parameters, reengineering processes and implement changes to minimise risks. Furthermore, Davar has demonstrated skill in managing and delivering multiple projects through objective tracking including metric reporting. Davar is deft in collaborating with internal teams, customers and other business partners to generate accurate programme goals.

Prof. Dr. Roberto Di Pietro

Professor of Cybersecurity, HBKU College of Science and Engineering

Prof. Dr. Roberto Di Pietro, ACM Distinguished Scientist, is Full Professor in Cybersecurity at HBKU-CSE (College of Science and Engineering at Hamad Bin Khalifa University). Previously, he was in the capacity of Global Head Security Research at Nokia Bell Labs, and Associate Professor (with tenure) of Computer Science at University of Padova, Italy. He started his Computer Scientist career back in 1995, serving for a few years as a Senior Military Technical Officer with the Italian MoD (Ministry of Defence). He has been working in the security field for 25 years, leading both technology-oriented and research-focused teams in the private sector, government, and academia (MoD, United Nations HQ, EUROJUST, IAEA – International Atomic Energy Agency, WIPO – World Intellectual Property Organisation). His main research interests include AI-driven cybersecurity, security and privacy for wired and wireless distributed systems (e.g. Blockchain technology, Cloud, IoT, OSNs), virtualisation security, applied cryptography, intrusion detection, and data science. Other than being involved in M&A of start-up – and having founded one (exited) – he has been managing several multimillion-dollar security projects, producing 240+ scientific papers and 15 patents over the cited topics, has co-authored three books, edited one, and contributed to a few others. In 2011–2012, he was awarded a Chair of Excellence from University Carlos III, Madrid. In 2020, he received the Jean-Claude Laprie Award for having significantly influenced the theory and practice of dependable computing. He is consistently ranked among the 2% top world scientists since this ranking existed.

Afi Hashim

Regional Manager, Middle East, Turkey & India, WALLIX

Afi Hashim spearheads the Middle East & India business at WALLIX. With a customer-centric approach, the company has grown its revenue and install base for the last five years and beyond. Having a comprehensive identity and access security stack, the company helps enterprise organisations to implement a true Zero Trust security model. Under Hashim's leadership, the region has got a strong and committed channel base consisting of value-added distributors and channel partners.

Paul John

Cloud Architect, Secureworks

Danish Khan

Presales Manager, WALLIX

Danish Khan helps organisations overcome and resolve their Privileged Access Management challenges. He is an experienced Presales Manager with a demonstrated history of working in the information security and services industries. Skilled in delivering POCs, demos and presentations with strong convincing skills to convert opportunities into business value, he joined WALLIX in 2019 as Presales Manager for MEA, India and APAC regions.

Dr. Maode Ma

Research Professor, Qatar University

Prof. Maode Ma, a Fellow of IET, received his PhD degree from Department of Computer Science in Hong Kong University of Science and Technology in 1999. Now, Dr. Ma is a Research Professor in the College of Engineering at Qatar University. He has extensive research interests including network security and wireless networking. Dr. Ma has more than 460 international academic publications including more than 220 journal papers and over 230 conference papers. His publication has received more than 7,400 citations by Google Scholar. He has delivered over 80 keynote speeches and 10 tutorials at various international conferences. He currently serves as the

Editor-in-Chief of International Journal of Computer and Communication Engineering and Journal of Communications. He also serves as a Senior Editor for IEEE Communications Surveys and Tutorials, and an Associate Editor for International Journal of Wireless Communications and Mobile Computing and International Journal of Communication Systems. Dr. Ma is a senior member of IEEE Communication Society and a member of ACM. He is now the Chair of the ACM, Singapore Chapter.

Kapil Matta

Regional Manager, Enterprise – MEA, Malwarebytes

A postgraduate in Business (Finance & Economics) from Auckland University of Technology, New Zealand, with a bright academic profile and an illustrious career in banking, risk management & technology consulting, Kapil is a self-starter with strong mentoring, teamwork and inter-personal skills and high adaptability to new challenges, as demonstrated by successful transitions across functions.

He possess over 15 years of spread across business management, sales & distribution, project management, risk, operations and service delivery.

Kapil has assisted several clients in risk assessments and cybersecurity technology solutions recommending implementable solutions for future scalability. He is an active speaker, director with ISACA UAE Chapter and member of several industry bodies.

His areas of interest include addressing cybersecurity consulting, leadership challenges, risk management modelling, building business through social & digital media marketing and branding.

Sirajhusen Modi

System Sec Head, Al Meera Consumer Goods

Sirajhusen is a certified Network & System Engineer with 15+ years of experience in the areas of cybersecurity management, infrastructure management, IT operations & NOC management. Currently, he is working at Al Meera as a cybersecurity professional, managing security and IT infrastructure including system and database.

Ron Peeters

Vice President Middle East and Emerging Markets, Synack

Ron Peeters is a seasoned IT industry executive with more than 30 years' experience working for an array of advanced technology companies around the world. He is Vice President of Middle East and Emerging Markets for Silicon Valley based Synack, Inc., a rapidly emerging market leader in offensive and crowdsourced security testing. Normally every month Ron is in the Middle East with focus on UAE and Saudi Arabia.

Radhakrishnan M

Innovation Lead/Chief Technology Advisor, Chapter Lead – Government Blockchain Association, Qatar

An ICDL, WHO, Bullet Proof® certifiedIT Global Advisory Head [enterprise & large scale blockchain, artificial intelligence solutions, cloud, industrial automation applications] with 21+ years of successful technology strategy, product ideation & strategy, business solution management, CxO consulting, data & analytics engineering, reporting engineering services, corporate technology strategy consulting & technology operations, technology planning, national technology roadmap definition, key parameters assessment & planning, cloud transformations, technology innovations management, automotive solutions & delivery management, global digital vision management track record on various domains.

Parthi Sankar

CISSP, Technical Director N.Europe, Anomali

Parthi is the Technical Director for Anomali ensuring Anomali clients realise the value of cybersecurity within their organisation. This involves exploring an organisation's place on the cybersecurity maturity curve in order to splice the right set of solutions and processes with the organisation's SOC and CTI teams to detect and prevent attacks from capable adversaries. The right solutions may come in the form of actionable threat intelligence from a threat intelligence platform, taking security from intelligence to detection in seconds using Cloud XDR or workflow efficiency brought through a natural language processing (NLP) tool. Parthi is passionate about ensuring solutions contribute to greater ROI to existing investments and bringing silos of teams, processes and tools together to markedly improve an organisation's security posture and reduce the attack surface. Parthi has extensive experience in the SOC and CTI industry working for global companies. His experience includes consulting, services, support, sales and solutions engineering leading him to be a trusted advisor that knows how to acquire, implement and use solutions and processes to derive maximum value and align that to business goals and outcomes. His formal qualifications include a BSc degree in Virology, MSc degree in Information Security, CISSP, CEH, CISM.

Sertan Selçuk

Electronics and Communications Engineer, EMT

Proud to be the father of Ateş and Alev, Sertan Selçuk has been in the cybersecurity industry for over 20 years, taking on both commercial and technical responsibilities to protect critical infrastructures and air-gapped networks at global vendors, system integrators and customers. Sertan Selçuk, an Electronics and Communications Engineer, has a master's degree in Cybersecurity from Middle East Technical University and an MBA degree from Manchester University.

Maarten Stassen

Partner – Lawyer, Crowell & Moring LLP

Maarten Stassen is a Partner in the Brussels office of Crowell & Moring, where he is a member of the firm's Privacy & Cybersecurity Group. His practice focuses on privacy and data protection, including the General Data Protection Regulation (GDPR) and cross-border data transfers solutions, as well as on the legal and operational aspects of the digital ecosystem, including Internet of Things (IoT), MedTech, and upcoming technologies such as distributed ledger technology (e.g. blockchain). Maarten has been named a 'Next Generation Partner' by Legal 500 in EU Regulatory: Privacy and Data Protection. A Legal 500 source described him as follows: 'Maarten Stassen is one of the brightest and most talented lawyers I have ever met. He is a team player and an excellent lawyer'. He was furthermore described as 'very experienced in privacy' and a 'name to note' in the Belgian IT & Telecoms industry. Before joining Crowell & Moring, Maarten was a Director in Deloitte's Cyber practice, as well as the Faculty Leader of the European Privacy Academy. He has been focusing on privacy and data protection law for many years, first as a lawyer in both Spain and Belgium, and later as European Privacy Officer of an international health insurance company. Characterised by his entrepreneurial spirit and drive to provide client-specific, business-focused, practical and pragmatic advice, Maarten has extensive experience advising a wide range of private organisations and public sector entities on national and international privacy and data-protection-related matters. Clients include household names in the automotive, MedTech, transportation, financial services, life sciences, and retail sectors. Maarten has both a Belgian and a Spanish law degree. His international experience helps to provide a different point of view for his clients. Maarten is fluent in Dutch, English, French, Spanish, and Catalan. Maarten is Vice-Chair of the American Bar Association (ABA) Privacy and Computer Crime Committee (Science & Technology Law Section) and Co-Chair of the Brussels KnowledgeNet of the International Association of Privacy Professionals (IAPP), as well as a former member of its European Advisory Board. He teaches at the Data Protection Institute and is a frequently asked speaker at privacy and data protection events. Being a practitioner in matters of blockchain, Maarten is part of the Beltug Blockchain Task Force which meets, discusses, and makes suggestions and recommendations to Beltug regarding issues, activities, and lobbying efforts that can be undertaken in the area of blockchain. Topics can extend beyond the national borders of Belgium.

Giorgio Torre

Project Manager, Leading Consulting Firm

Project Manager with international experience in technological and disruptive markets. He has managed multi-million dollars projects in Europe and in the Middle East, while offering through social media reports, dossiers and market insights regarding blockchain, Web 3.0, metaverse, digital humans and AI.

Abdullrazaq Zahran

Security Engineering Manager | METNA, Vectra

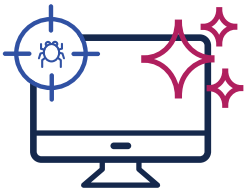
Abdullrazaq Zahran is working as Security Engineering Manager for Vectra.ai and covering METNA region. Zahran has a total of 12 years+' experience in the Middle East region went through different cybersecurity and advanced networking solutions. Previously, he was working as Security Engineering Team Leader across ME for multiple solutions, and across his career path he gained a wide experience from the different verticals helping the customers to overcome their pains and achieving a positive business outcome. Zahran hold a BSc degree in Electrical Engineering/Telecommunication and Electronics from Jordan University of Science and Technology, and now he is part of the professional certificate programme in the major of advanced computer security at Stanford university. □

Malwarebytes

DATA SHEET

Malwarebytes business product line

From infection to recovery in seconds – without sacrificing endpoint performance



Advanced security, simplified

From blocking threats to removing attacks, the cloud-hosted Malwarebytes Nebula cloud platform makes it easy to defeat ransomware and other malware. Bringing all Malwarebytes products together under a single pane of glass, the platform reduces complexity through a guided user interface, next-generation threat intelligence, and seamless integration capabilities. For organizations large or small, the result is unmatched protection and return on your security investment.

Respond, deliberately

Responding to a threat requires speed and know-how. Malwarebytes allows security professionals to actively and quickly respond by isolating an attack in progress and automating the remediation and recovery of the impacted endpoint. Our endpoint detection and response technology saves precious time typically spent hunting for the threat, and returns endpoints to operation without costly re-imaging.

Adapt to the threat

Your organization's success depends on endpoints being operational. Malwarebytes delivers cyber protection that creates a resilient security posture tailored to your endpoint environment. And because advanced, polymorphic threats are targeting the endpoint with adaptive techniques, we use multiple layers of technology applied at various points along the attack chain—including machine learning–enhanced and heuristic detection capabilities—to crush their attacks.

Cloud-native Endpoint Security Products

Malwarebytes business product line's cloud-native architecture was designed to defeat even the most sophisticated and fast sprawling malware.

Malwarebytes Nebula cloud platform

Malwarebytes Incident Response (IR)

Cloud-native remediation

Malwarebytes Endpoint Protection (EP)

Endpoint and server protection and remediation

Malwarebytes Endpoint Detection and Response (EDR)

Threat hunting, protection, and remediation for endpoints and servers

Malwarebytes Incident Response (IR)

Malwarebytes Incident Response is a threat detection and remediation tool built on a highly scalable, cloud-based management platform. It scans networked endpoints for advanced threats including malware, PUPs, and adware and thoroughly removes them. Malwarebytes Incident Response improves your threat detection and the time it takes to respond to an attack with the added benefits of scalability, flexibility, and automation.

Malwarebytes Endpoint Protection (EP)

Malwarebytes Endpoint Protection (EP) and Malwarebytes Endpoint Protection for Servers is a complete malware protection and remediation solution with predictive threat detection, proactive threat blocking, and integrated end-to-end protection. Driven from the cloud through a single pane of glass, Malwarebytes Endpoint Protection provides flexible management and speed for organizations of all sizes. And, both endpoints and servers are protected against advanced malware threats including ransomware.

Malwarebytes Endpoint Detection and Response (EDR)

Malwarebytes Endpoint Detection and Response (EDR) and Malwarebytes Endpoint Detection and Response (EDR) for Servers makes it easy to quickly investigate, isolate, remediate, and recover from threats—all in a matter of minutes. The solution's "one-and-done" remediation thoroughly and permanently removes infections in a single operation from both endpoints and servers. And, Ransomware Rollback returns the device to a known, healthy state even after ransomware has triggered.

LEARN MORE

For more information about Malwarebytes business products, contact your account team or your authorized channel partner. Or, to communicate with a local sales expert, visit: www.malwarebytes.com/business/contact-us/.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.

Why your Secure Email Gateway isn't as secure as you think

Every hour of every day, phishing emails evade perimeter controls – in most cases, secure email gateways (SEGs).

Cofense reports

Once delivered to the inbox, phish tempt users to click and give up network or personal credentials, activate malware, or fall for scams. Over 50% of enterprises report that phishing emails reach the inbox roughly once a week. Since SEGs are missing so many phish, there's a good chance other technologies – firewalls, anti-virus, and EDR – also aren't spotting these threats. Such gaps can leave you vulnerable for hours or even days.

What is a SEG?

Secure email gateways – AKA email gateways or email security solutions – are the most common type of perimeter technology used to stop phish from reaching the inbox.

Unlike firewalls and other security technologies, SEGs receive no regulatory or compliance oversight. That's right, SEGs get zero validation testing against the problem they're meant to solve – phishing, the #1 global cyber-threat.

Why SEGs fail

As we've seen, SEGs can handle the basics of perimeter phishing defence. But today's attacks are anything but basic. Here are three reasons why technology fails to stop determined attackers.

1. Attackers constantly innovate

Every time you configure your SEG to thwart the latest Tactics, Techniques and Procedures (TTPs), attackers adjust. They innovate relentlessly to stay a step ahead. Some of the TTPs attackers use to sidestep defences are as follows:

- Leverage trusted cloud infrastructure
- Obfuscate or encrypt malicious content
- Inject malicious content into legitimate email conversations

2. SEG vendors are reactive

You're not the only one having trouble keeping up. As phishers refine their tactics, SEG vendors scramble too.

3. Business can't wait

Tuning your SEG to the latest TTPs takes time. But email must flow freely for your business to operate. Too often, you're forced to choose between speed and organisational security. Sooner or later, speed wins out and phish land in the inbox.

Your best defence against phishing attacks

Because SEGs are so porous you need something to back them up, a consistent way to find and remove threats that reach the inbox. We're talking defence-in-depth, combining human intuition and purpose-built automation.

Security awareness

When human attackers deliver threats to the inbox, humans need to respond. Besides educating users on phishing, your security awareness programme needs to let them practice in a real-world setting: their inboxes. Phishing simulations are your best bet. Make sure the training is positive, not punitive, and that scenarios mirror threats your organisation faces.

Email reporting

Your security teams can't stop a threat in the inbox unless it's reported. A 'Report Phishing' button on the email toolbar makes it easy. With a single click, end users get involved. As employees get more practice, both in training and real situations, they'll sharpen their intuition – something tech controls like email gateways lack.

Email analysis

When security teams try to respond manually to email reports, they usually fall behind. There are simply too many emails, most of them harmless. Automation can cut through noise and identify real threats, plus prioritise them so analysts can budget their limited time.

Search & quarantine

Thanks to well trained users and advanced automation, your SOC has identified a phishing email in a handful of inboxes. But who else received the phish? Again, you'll rely on automation to search all inboxes ASAP and quarantine the threat before lasting damage is done.

At the end of the day, attackers will continue to evolve their tactics faster than most technologies can keep up with. Your best defence against phishing attacks is a combination of technology and humans working together. □

For more information, please visit **www.cofense.com**


We
Stop
Phish.
Phishing campaigns continue to evolve and innovate.
MILLIONS of attacks bypass expensive email security solutions EVERY YEAR.
Download the Annual State of Phishing Report to learn how you can avoid a breach from the phishing threats that are targeting businesses around the globe.
DOWNLOAD THE REPORT
COFENSE

Why seasonality factors are important to anomaly detection in cybersecurity

It's important for organisations to detect anomalies to ward off potential cyber-attacks.

ManageEngine reports

Seasonality factors need to be considered while attempting to detect behaviour anomalies of users and hosts in a network. But before we make a case for that, let's first try and understand what seasonality is by looking at a few examples from daily life:

1. *Seasonality in product sales:* Numerous products such as chocolates, summer clothes, workout gear, and Halloween costumes belong to seasonal markets. The demand for these products typically peaks for a few days or months and then tapers off. Depending upon the market, the sales that can be attributed to seasonality can vary. For instance, the sales of winter clothes during the winter months may actually eclipse the sales during the rest of the year.
2. *Seasonality in water consumption:* This is an easy example to understand: People usually consume a lot more water during the summer months.
3. *Seasonality in the stock market:* Historically, stocks have underperformed between the months of May and October but have done well from November to April. There is a popular saying that goes, "Sell in May and go away."

Is there an example of seasonality when it comes to an organisation's computer network? Yes, there is....

In an organisation's network, users and hosts may exhibit seasonal behaviour such as:

1. A database server that's heavily queried on Monday every week.
2. A user who works on alternate Saturdays.
3. A user who accesses a particular file server only once a month, particularly on the last working day of the month.

The three examples above involve relatively rare occurrences that are seasonal in nature, but they're not anomalies.

An anomaly, by definition, is something that deviates from what's expected. These three activities (and others like it), though rare, aren't anomalies because they start to become accepted as normal after they occur a few times. They're normal activities that follow a seasonal trend.

Anomaly detection in cybersecurity

It's important for organisations to detect anomalies that happen in the network to ward off potential cyber-attacks. To do this, organisations typically use a security analytics solution or a SIEM solution that has anomaly detection capabilities fuelled by machine learning algorithms. This solution creates a baseline of expected behaviour for every user and host in the network. If a user's or host's observed behaviour deviates beyond a learned threshold, it's flagged as an anomaly and the risk score is raised accordingly.

Anomaly detection with the ability to identify seasonality

The machine learning algorithms used to detect anomalies must be able to account for seasonality. They should understand seasonal effects on the behaviour of users and hosts and be able to identify a particular activity as non-anomalous even if it's rare. After accounting for seasonality, no red flags should be identified and risk scores should not be raised. So, what if the activity occurs outside of this seasonal window? That would be an anomaly, as the use case below illustrates.

A seasonality use case

Your bank operates on the first and third Saturday of every month. On the second Saturday of the month, your security analytics platform notices an employee logging in to the network. A lesser-trained system would accept this; after all, the employee was online the previous Saturday, so why not today? But yours is well-trained to spot seasonal anomalies just like this. It knows the difference between the various Saturdays of a month. An alarm goes off, and the risk score of the employee increases.

Seasonality factors are critical for calculating the real risk posed by users and hosts in your network. Without considering seasonality, there are chances of both blind spots and false negatives. The anomaly detection engine within your SIEM solution should make use of this capability to show you a more accurate picture of what's taking place. □

ManageEngine

Bringing IT together

Comprehensive IT management
software for all your business needs.

Our Solution

Identity and access management | Enterprise service management
Unified endpoint management and security | IT operations management
Security information and event management | Advanced IT analytics
IT management for MSPs | Cloud solution for enterprise IT
Remote work management

www.manageengine.com

ManageEngine is a division of ZOHO Corp.

We are the product of our own thinking processes and whatever we are thinking of today is **PARAMOUNT** for our tomorrow.

INFORMATION SECURITY SERVICES

CONSULTING SERVICES SERVICES

MANAGED SECURITY SERVICES

IDENTITY & ACCESS MANAGEMENT

CyberSecurity is

Paramount

paramount
@ssuring Value

marketing@paramountassure.com

www.paramountassure.com

About Us

Founded in 2004, reconfigured in 2007 through a Management Buy Out and being reinvented in 2015 to morph into a trusted cybersecurity solutions provider, Paramount always remains a work in progress. Building quality into the very fabric of the business has made excellence a way of life at Paramount. The company started as early as 2007 at the ISO level and graduated through the EFQM framework by introducing and sustaining a culture of continuous learning, quality and focus on individual value-add inside and outside the organization. Today, Paramount is the only IT services company in the entire Middle East to have secured an amazing gamut of certifications and unbiased recognition: ISO 9001:2015; ISO 27001:2013; ISO 22301:2012; Business Excellence and Great Place to Work Award.

A strong workforce of over 50 professionals with 35 Security Consultants and Engineers makes Paramount one of the largest reservoirs of security talent in Qatar. The essence of Corporate Governance at Paramount is not only to allow the Management to propel the company forward with freedom, but to exercise that freedom within a governance framework that assures transparency, accountability, effective operational control and management of risk. It is the consistent focus on Quality and Excellence that has enabled Paramount to acquire a huge base of customers across Qatar in all verticals – Oil & Gas, Banking & Finance, Government, Airlines & Transportation and other large corporations.

What we do

NETWORK SECURITY SOLUTIONS

- APT Prevention Solutions
- Next Generation Firewall Platforms
- Intrusion Prevention Systems
- Network Behaviour Analysis
- Network Access Control
- Web Application Firewall

DATA SECURITY SOLUTIONS

- Email and Web Security Solutions
- CASB Platforms
- Data Classification and Data Leakage
- Prevention
- Information Rights
- Management Solutions
- Endpoint Application Control

CONSULTING & SOLUTIONS

- Standards: ISO(27001, 20000, 22301)
- Digital Fraud/Forensics
- Critical Infrastructure (SCADA Security) - Framework, Risk Assessment, Roadmap, Trainings
- SAP/ERP Security
- Compliance Services (ISO, NIAP, GDPR)
- Vulnerability & Penetration Testing

MOBILE APP SECURITY - PARAMOUNT APPSECURE paramount AppSecure

RED TEAMING

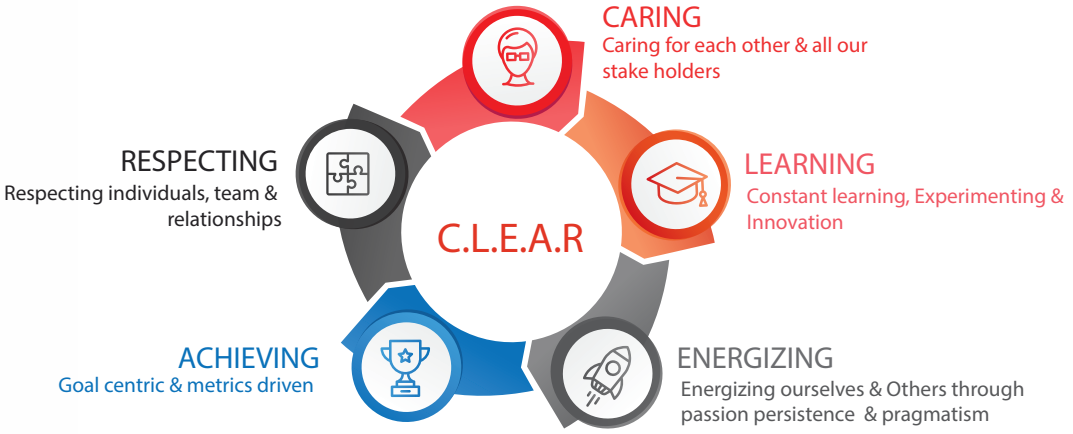
MALWARE RESEARCH

CEO Speak

"Our risk-based approach to cybersecurity is all encompassing – people; process; technology. This enables our customers to focus on their business while we manage their dynamic risks in the cyber world.

If you are one of our valued customers, I Sincerely thank you for having respond your confidence in Paramount. If you are evaluating for a reliable cybersecurity partner, I request you to give us an opportunity to compete for your business."

Paramount Values



What we do

SECURITY & RISK MANAGEMENT

- Governance Risk & Compliance
- SOC Solutions
- Vulnerability & Compliance Management
- Change & Configuration Management
- Digital Forensic Solutions

IDENTITY & ACCESS MANAGEMENT

- User Provisioning/ De-provisioning
- Privileged Access Management
- Strong Authentication
- Web Single Sign-On
- Enterprise Single Sign-On
- Data Access Governance
- Application Access Governance

MANAGED SERVICES & STAFFING SOLUTIONS

- Staffing Solutions
- Training & Skill Development
- Security Incident Response Platform
- Managed Security Services

DEVSECOPS

BREACH INVESTIGATION AND COMPRIMISE ASSESMENT

SECURITY AWARENESS & EDUCATION

Our Products

VinRansomware

VinRansomware is your one stop guide for everything related to ransomware. From detailed threat analysis of popular ransomware to detection tools that can quickly identify if you are under attack, VinRansomware has a huge database of information that can help you in your fight against ransomware.

VPhish

VPhish is a multilingual phishing simulation SaaS platform that enables security officers to assess the employee behaviour to phishing attacks through simulated phishing emails.

paramount AppSecure

AppSecure is a mobile application security testing solution to detect and fix vulnerabilities in mobile apps using a combination of automated and manual tests.

e-Crime & Cybersecurity Congress in Abu Dhabi 2022

"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

"It is a pleasure to attend every year to network and to learn more about the cybersecurity world. It was so beneficial to be honest and I will be glad to provide a testimonial from my side."

Manager Security Compliance
DU

"Once again It was my pleasure to be part of e-crime conference. I am looking forward the next one in Dubai in March 2020."

Head of Fraud Investigations, Risk Management
RakBank

2019 sponsors included:

Strategic Sponsors

Attivo Networks
DARKTRACE
LexisNexis Risk Solutions
ThreatMetrix
mimecast
PALADION High Speed Cyber Defense
proofpoint.
Recorded Future
Synack

Education Seminar Sponsors

Accellion
Akamai — Intelligent Security Starts at the Edge
Centrify — Zero Trust Privilege
Cyxtera
FORTINET
HELP AG — Protecting Information
okta
OPSWAT.
PGI

Networking Sponsors

Arcon
BULWARK Technologies
Check Point Software Technologies Ltd.
CLOUDFLARE
CYBERBIT — Protecting a New Dimension
CYWARE
eliteVAD
PhishRod
Pulse Secure
SECURRENT IT Security Solution Provider
SANS EMEA
VECTRA — Security that thinks

Branding Sponsor

FIREEYE

For more information, please visit
akjassociates.com/contact-us

Thank you to all our sponsors

Strategic Sponsors

BeyondTrust

Redington
SEAMLESS PARTNERSHIPS

Secureworks®

Education Seminar Sponsors

ANOMALI®

COFENSE

emt
TECHNOLOGY DISTRIBUTION

Malwarebytes

ManageEngine

paramount
@ssuring Value

OPSWAT.

Synack

VECTRA®

WALLIX
CYBERSECURITY SIMPLIFIED

Networking Sponsors

ORCHESTRA

Branding Sponsors

SOCRadar®