



**19<sup>th</sup> March 2019**  
**Dubai**



@eCrime\_Congress  
#ecrimecongress



#ecrimecongress

**Real-life solutions  
for the virtual enterprise**

It would take



8,774 data analysts,



working 8-hour shifts, 5 days a week,



for 52 weeks per year

to process the same amount of security event data machine analytics can process each year.

Harness the Power of Machine Learning for  
Threat Intelligence With Recorded Future



LEARN MORE AT [RECORDEDFUTURE.COM](https://RECORDEDFUTURE.COM)

# Real-life solutions for the virtual enterprise

19<sup>th</sup> March 2019  
Conrad Dubai, Dubai



Cybersecurity is now borderless: in a world where hyper-connectivity has moved the perimeters of your attack surface – and your remit – issues of cyber-risk transcend functions, organisations, and sectors. Hyper-connectivity also means perimeters now extend outside the business. The security of third parties is now as important as the security of your own organisation. And for cybercriminals national borders have no meaning.

So, for our 11<sup>th</sup> anniversary e-Crime & Cybersecurity Congress in Dubai, we are bringing industry leaders from both the region and our international network to share real-life insights and case studies on the hard hitting truths that affect global CISOs everywhere.

Cybersecurity is now universal. And at our Congress we provide the ideal platform for high-level information sharing, networking, and debate, to find real, actionable solutions.

It is also a chance for you to mingle, enjoy, rekindle old relationships and form new ones. One of the main aims of our events is to facilitate conversation and dialogue. So please, enjoy your event, and take the opportunity to mingle with peers, colleagues and solution providers. If you have any questions, please do not hesitate to ask any member of the team.

**Amanda Oon**  
Editor

@eCrime\_Congress



#ecrimecongress

- 3 Harness the power of global shared intelligence with the ThreatMetrix Digital Identity Network**  
Distinguish fraudsters from genuine customers in real time, throughout the customer journey.  
**ThreatMetrix**
- 5 How organisations can start using threat intelligence to boost their security**  
Taking the initiative back from the attackers.  
**Recorded Future**
- 7 Addressing the endpoint – the first step to secure cloud enablement**  
Endpoints are operated by users and attackers can trick them into all sorts of deceptive things.  
**Help AG**
- 10 21st Century Fox: Leveraging OneTrust for privacy compliance**  
Many companies are evolving from a traditional business-to-business operation into a more direct-to-consumer business model.  
**OneTrust**
- 12 The evolution and future of SIEM**  
To combat advanced threats and meet the growing demands of the security market, SIEM solutions have also been evolving over the years to leverage new-age technology including big data analytics and machine learning.  
**ManageEngine**
- 14 More offensive security testing at one of Europe's largest banks, Banco Santander**  
Trust in the cybersphere is more critical than ever.  
**Synack**

**Editor and Publisher:**  
Amanda Oon  
e: amanda.oon@akjassociates.com

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

**Forum organiser:**  
AKJ Associates Ltd  
27 John Street  
London WC1N 2BX  
t: +44 (0) 20 7242 7498  
e: amanda.oon@akjassociates.com

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

© AKJ Associates Ltd 2019. All rights reserved. Reproduction in whole or part without written permission is strictly prohibited. Articles published in this magazine are not necessarily the views of AKJ Associates Ltd. The publishers and authors of this magazine do not bear any responsibility for errors contained within this publication, or for any omissions. This magazine does not purport to offer investment, legal or any other type of advice, and should not be read as if it does. Those organisations sponsoring or supporting the e-Crime & Cybersecurity Congress in Dubai bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those organisations sponsoring or supporting the e-Crime & Cybersecurity Congress in Dubai, either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.



- 17 Synchronised security: cybersecurity as a system**  
Cybersecurity is not getting any easier.  
**Sophos**
- 19 Sponsors and exhibitors**  
Who they are and what they do.
- 28 Agenda**  
What is happening and when.
- 30 Education seminars**  
Throughout the day a series of education seminars will take place as part of the main agenda.
- 35 Speakers and panellists**  
Names and biographies
- 42 Digital transformation escalates compliance challenges**  
Digital transformation is changing the face of the modern data-driven enterprise.  
**Thales eSecurity**
- 44 Threat actor – a love story**  
A closer look at the strange love-hate relationship we have with cyber-threat actors  
**Anomali**
- 46 The business of information**  
The massive increase in cybercrime and fraud over the years has highlighted the challenges businesses face across all industries.  
**Kaspersky Lab**
- 48 Architecting a multi-tiered control strategy**  
We need to have a more profound/clear/strong view on the security solutions we need to avoid business disruption.  
**SABSA**
- 51 Network and security solutions**  
Enabling your IT Infrastructure.  
**TNCT**
- 53 How much does credential stuffing cost your business?**  
Credential stuffing is a relatively new problem, and it's serious.  
**Shape Security**

# Harness the power of global shared intelligence with the ThreatMetrix Digital Identity Network

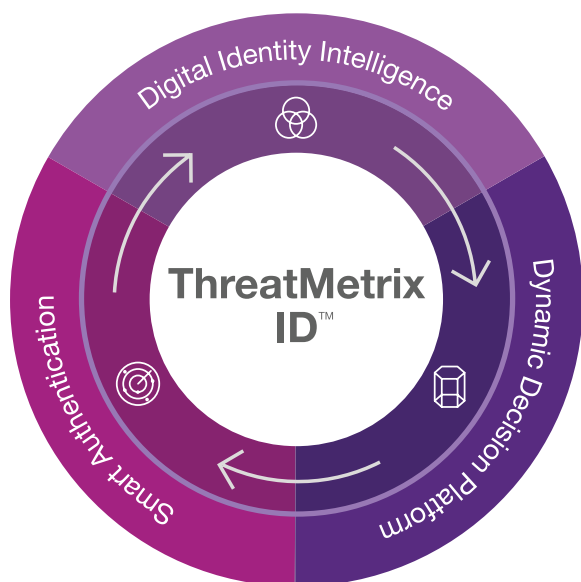
Distinguish fraudsters from genuine customers in real time, throughout the customer journey.

**A network that grows more powerful each day**  
Global digital businesses are increasingly having to balance the pendulum swing of a slick, frictionless online experience, with the ability to accurately detect and block fraud. This has become more complex with the persistence of global data breaches that flood the dark web with stolen identity data and make it easier for fraudsters to perpetrate sophisticated and convincing attacks. Fraudsters masquerade as customers while good customers expect businesses to recognise them in real time with no associated friction.

ThreatMetrix gives businesses the ability to genuinely recognise good, returning customers by collating Digital Identity Intelligence from the complex digital DNA of online transactions; whether logins, payment transactions or new account applications.

ThreatMetrix ID is the technology that brings this Digital Identity Intelligence to life; helping businesses elevate fraud and authentication decisions from a device to a user level as well as unite offline behaviour with online intelligence.

ThreatMetrix ID helps businesses go beyond just device identification by connecting the dots between the myriad pieces of information a user creates as they transact online and looking at the relationships between these pieces of information at a global level and across channels/touchpoints. ThreatMetrix ID comprises a



unique digital identifier, a confidence score and a visualisation graph for each connecting user, which together act as a benchmark for the trustworthiness of current and future transactions.

## The three components of the Digital Identity Network

### Digital Identity Intelligence

The best crowdsourced intelligence from the world's largest digital identity network.

- *Web and mobile device intelligence:* Device identification, detection of device compromises across web and mobile, device health and application integrity
- *True location and behaviour analysis:* Detection of location cloaking or IP spoofing, proxies, VPNs and the TOR browser detection of changes in behaviour patterns, such as unusual transaction volumes

### Dynamic Decision Platform

Using Digital Identity Intelligence to make the most accurate and timely decisions.

- *Behavioural analytics (ThreatMetrix Smart Rules):* Advanced behavioural analytics rules that enable better understanding of legitimate user behaviour and more accurately detect genuine fraud
- *Machine learning (ThreatMetrix Smart Learning):* A clear-box approach to machine learning that integrates Digital Identity Intelligence with Smart Rules to produce optimised models with fewer false positives
- *Workflow and orchestration:* Ability to integrate external data sources into the ThreatMetrix decision engine as well as access pre-integrated third-party services for transactions that require additional assurance/exception handling
- *Case management:* Enabling continuous optimisation of authentication and fraud decisions by monitoring, updating and isolating transactions that require additional review, providing a smarter, more integrated way to handle increasingly complex caseloads with shrinking resources

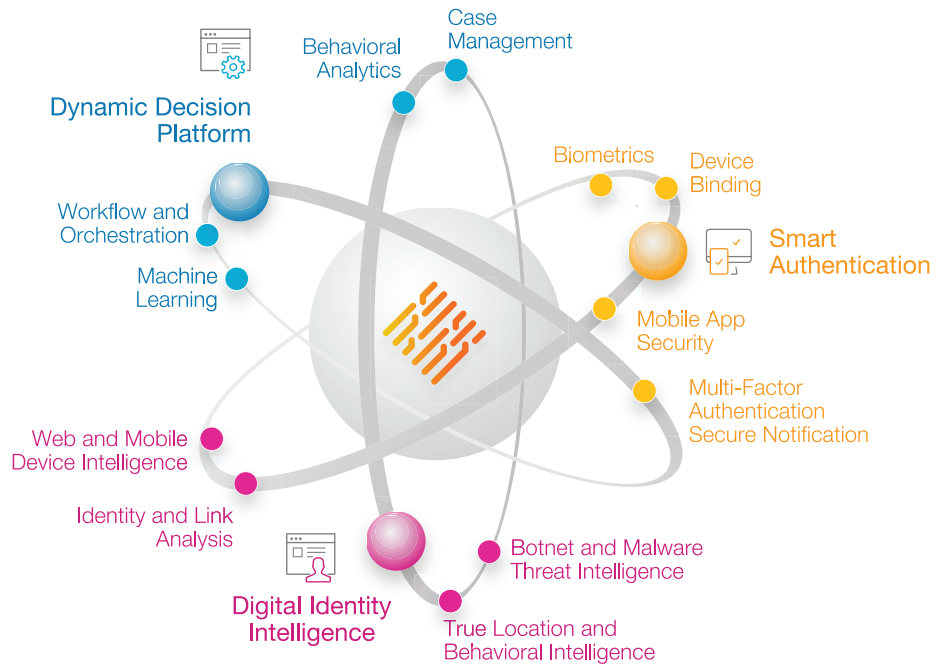
### Smart Authentication

Combining frictionless RBA with low-friction SCA for an enhanced customer experience.

- *Mobile app security:* Detect breaches to the application itself and verify the trustworthiness of the mobile device
- *Device binding:* Leverage the trust of existing devices, using strong device ID and carrier ID, to avoid repetitive authentication

## ThreatMetrix reports

**The ThreatMetrix Digital Identity Network: Distinguish fraudsters from genuine customers in real time, throughout the customer journey**



- **Multi-factor authentication (MFA) secure notification:** Push notifications to the user’s mobile device for low friction authentication
- **Biometrics:** A comprehensive range of FIDO-compliant, low friction, password-free authentication strategies

**Personalising the ThreatMetrix solution to your business**

ThreatMetrix offers a powerful policy engine allowing customisation that helps business incorporate their own processes and tolerance for risk. This allows organisations to fine tune and automate responses to online transactions for agility, simplicity and efficiency.

**The ThreatMetrix advantage**

- **An unparalleled network:** The ThreatMetrix Digital Identity Network protects 1.4 billion unique online accounts using intelligence harnessed from 2 billion monthly transactions
- **A comprehensive end-to-end solution:** Universal fraud and authentication decisioning across all use cases and throughout the customer journey
- **Bringing digital identities to life:** ThreatMetrix ID combines a unique identifier, a confidence score and a visualisation graph to genuinely understand a user’s unique digital identity across all channels and touchpoints
- **An integrated approach to authentication:** Flexibly incorporate real-time event and session data, third-party signals and global intelligence into a single Smart Authentication framework, to deliver a consistent and low-friction experience with reduced challenge rates

- **Advanced behavioural analytics and a clear-box approach to machine learning:** ThreatMetrix Smart Analytics analyses dynamic user behaviour to build more accurate, yet simpler, risk models. The result is a competitive edge in customer experience with reduced false positives, while maintaining the lowest possible fraud levels
- **Privacy by design:** ThreatMetrix is unique in its ability to solve the challenge of providing dynamic risk assessment of identities while maintaining data privacy through the use of anonymisation and encryption
- **Rapid, lightweight deployment:** The ThreatMetrix solution is cloud based, providing simple and straightforward integration with existing systems □

ThreatMetrix®, a LexisNexis Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion anonymised user identities, ThreatMetrix ID™ delivers the intelligence behind 75 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time.

ThreatMetrix is recognised as the sole Leader in the 2017 Forrester Wave™ for risk-based authentication.

For more information, please visit

[www.threatmetrix.com](http://www.threatmetrix.com)



# How organisations can start using threat intelligence to boost their security

Taking the initiative back from the attackers.

Cybercriminals have become increasingly bold, organised, and equipped with more sophisticated tools in recent years. New attack techniques and malware are developed and refined so quickly that organisations often have little choice but to take a reactive, defensive stance.

One of the most effective ways of taking the initiative back from the attackers is for organisations to arm themselves with high-level threat intelligence that will help them to identify potential malicious activity in advance. Gathering information from a mixture of open sources and hidden channels such as the dark web, threat intelligence reports can help companies to prepare against incoming attacks and take action to block them or mitigate their impact.

However, hearing the phrase 'high-level threat intelligence', the immediate reaction for many people would be to think of elite security analysts employed only by secretive government organisations and the world's largest mega corporations. For many years, accessing intelligence was seen as both too expensive and too complicated for ordinary businesses.

While it is true that threat intelligence was once available only to those that could afford to hire the highest level of advanced analysts in the industry, it has become rapidly more accessible in recent years. Advancing technology has enabled the market to expand rapidly, and any organisation can now access high-quality intelligence without breaking the bank on paying for the security elite.

Armed with access to threat intelligence that is clear, relevant and available in real time, organisations will be better informed and equipped for all of their security activity. Everything from the ability to deal with daily threats through to high-level strategic decisions made by executive leadership.

## Supercharging SOCs

One destination for threat intelligence will be the Security Operations Centre (SOC). Whether run in-house or via a third-party supplier, the SOC is the nerve centre of an organisation's security activity. Security alerts from tools such as SIEM, IDS and EDR all feed through to the SOC, enabling the security team to identify and respond to potential threats. Threat intelligence will provide powerful visibility of

the wider world to provide context alongside these various sources of internal security information.

One of the most common challenges for SOC teams is dealing with the vast volume of threat data heading their way. Alongside the sheer number of reports, teams also need to deal with the fact that security alerts will contain a mixture of false positives and false negatives that they will need to disentangle. With so much going on, it can be easy to overlook data that could point towards a serious threat.

With this in mind, if a SOC is already struggling with its own internal data streams, simply piling on even more information from external sources will make it even more difficult to keep up. Security alerts need to be filtered so that only relevant data is passed through to the SOC analysts, presented with context and enriched with additional information that can help the team to understand and act on their data streams more easily.

## Combating emerging threats

Most security experts accept that it is impossible to guarantee complete protection from cyber-attacks, especially because threat actors can exploit previous unknown zero-day vulnerabilities. This means that incident response is one of the most important aspects of any security strategy, with a well-planned response strategy often making the difference between a minor incident and an expensive disaster.

That said, even the most thorough incident response playbook will be rendered ineffective if the security team is not accessing essential data that will help them understand the situation. Many teams are stymied by the use of disjointed technologies that provide fragmented data streams, as well as the ongoing industry shortage of skilled and experienced professionals. The more time that must be spent trying to untangle disorganised threads of data, the more time the attack can progress unimpeded and the more damage it will cause.

If the response team has access to a threat intelligence tool that is able to break sources down into relevant and usable items, the team will be able to get to grips with the situation much faster. This will help them to utilise their resources far more efficiently and make swifter decisions in the midst of an active threat when every second counts.

**Recorded  
Future  
reports**

## Access to clear and accurate threat intelligence can help CISOs and other security leaders ensure that their companies are investing in a security strategy that is optimised for their specific needs.

### Addressing vulnerabilities

The ability to discover and respond to threats in real time will make a huge difference in a company's ability to mitigate the damage cybercriminals can inflict. Just as important however is the capability to proactively identify and manage vulnerabilities in advance, before they can be discovered and exploited by attackers.

The complexity of the average IT system and the rate at which new vulnerabilities are discovered means that very few companies have the resources to keep up with everything. Instead, remediation efforts need to be prioritised based on the level of risk involved. Incorporating threat intelligence into the risk assessment process will enable the company to factor in context from the wider security landscape as well as its own internal operations.

Intelligence reports might reveal that certain software has been the focus of a major attack campaign in recent months, for example, which would make updating and patching this software a much greater priority than it might have been otherwise.

Equipping themselves with their own threat intelligence streams will also give organisations a better chance of staying ahead of attackers. While new vulnerabilities that have been discovered by the security community are listed on the National Vulnerability Database (NVD), it takes an average of seven days for new threats to be published. This is ample time for more advanced and organised cybercriminals to exploit the vulnerability before companies are aware of it. By using their own intelligence rather than relying on the NVD and other sources, organisations can proactively take control of their own security.

### Empowering leadership with genuine intelligence

While organisations are unquestionably better protected from cyber-threats if they are able to take a proactive stance rather than reacting to incoming attacks, there are many challenges standing in the way of a successful proactive strategy. One of the biggest issues is the amount of capital and resources required.

Acquiring the required personnel and technology will generally involve a heavy financial investment.

Companies are often reluctant to devote so much capital to security, with many still seeing it as an IT issue rather than the essential business priority it has become.

Even when organisations do decide to invest in security appropriately, the expansive and fast-moving nature of the cyber-landscape means it is often difficult to prioritise effectively. As a result, we often find companies have opted to invest in advanced new security tools because of market hype or the actions of their peers and competitors, rather than through a real understanding of their own priorities.

Access to clear and accurate threat intelligence can help CISOs and other security leaders ensure that their companies are investing in a security strategy that is optimised for their specific needs. Intelligence will also lend extra weight when it comes to presenting the threats to the board and convincing them to authorise the required investment in technology and personnel.

From informing top level strategic business decisions to helping to deal with daily security demands, organisations are now able to incorporate threat intelligence into all essential security activity. However, while it is true that threat intelligence has advanced beyond the limits of the security elite to become accessible to the wider business world, the information must be presented in a succinct, relevant and targeted way if it is to make a difference. □

To find out more about how organisations can start using threat intelligence to boost their security, contact Recorded Future today for a Live Product Demo, tailored for your top use cases.

[www.recordedfuture.com](http://www.recordedfuture.com)

 Recorded Future



# Addressing the endpoint – the first step to secure cloud enablement

Endpoints are operated by users and attackers can trick them into all sorts of deceptive things.

After years of being little more than an industry buzz word, cloud computing in the Middle East has rapidly gained momentum and is expected to be a \$290 million market in the UAE alone by 2020<sup>1</sup>. We are already seeing evidence of this as 2019 is looking to be the tipping point at which the number of organisations that have some portion of their infrastructure or services in the cloud outweighs those that don't. Major technology vendors including AWS, Microsoft, Alibaba, and SAP have also been quick to recognise the region's cloud-readiness and have begun investing in Middle East based cloud data centres.

It should come as no surprise either – digital transformation has placed IT at the epicentre of business change and enablement while budget constraints have challenged organisations to do more with less. Cloud computing, with its flexible 'pay as you grow' and 'pay for only what you consume' consumption model solves this challenge while delivering so much more. Unlike their on-premise equivalents, cloud applications are constantly upgraded with new features. Office 365 is a good example of this as its enhancement cycles are ongoing unlike Microsoft Exchange, which only gets new features at major releases.

Added to this, most prominent providers are capable of delivering uninterrupted services – typically only allowing for downtime of 0.001%, or just 5 minutes per year. And for those concerned about security, the truth is that cloud services are often more secure than standard on-premise deployments as cloud providers tend to invest heavily in security technologies that all subscribers then benefit from.

## Cloud concerns

For all these benefits, the cloud does raise some pressing and pertinent questions. First, by their very nature, cloud services move control away from the organisation so what action can be taken when things

**The successful breach of a single cloud provider's systems could expose sensitive information for thousands of users and companies making this very appealing to cybercriminals.**

go wrong? And since security is in the hands of the cloud provider, how do you apply the same level of control as you would for an on-premise deployment?

With cloud, while the attack surface area might be smaller, the target is actually significantly larger. The successful breach of a single cloud provider's systems could expose sensitive information for thousands of users and companies making this very appealing to cybercriminals. And even if the cloud provider has taken the necessary steps to address these concerns, vulnerabilities might still arise due to misconfiguration by the customer, opening the doors to management interface attacks and the like.

The fact is, in the era of the cloud, information security teams will be presented with a new set of security challenges that will require fundamental shifts in their approach to security as traditional standards and methodologies will often not be easily adaptable to the cloud consumption model.

## The target has changed

Most importantly, we must acknowledge that the focus of cloud-related attacks has shifted. As with any endeavour, cybercriminals are keen to maximise the outcomes of their efforts. It has become apparent to them that with cloud providers investing heavily in the security of their platforms, these are now challenging targets. So, while we will no doubt continue to see the occasional data breach of large service providers that expose login credentials and the information of multiple users, the volume of cloud related attacks will shift away from the service itself to the endpoint and the end user.

## Exploiting the endpoint

Cyber-defences tend to tail away at the endpoint as user behaviour can be exploited and unpatched vulnerabilities become attack vectors. This is because endpoints are operated by users and attackers can trick them into all sorts of deceptive things – something we typically call social engineering. The endpoint also has a lot of interfaces to attack: e-mail, web-browsers and other applications are just some of these. When we combine this with the fact that many users have far too many system rights, you have a recipe for disaster.

Another reason why the endpoint is of so much interest when aiming to attack cloud applications

**By Nicolai Solling**

In the era of the cloud, the endpoint is set to be at the forefront of cyber-attacks and with the right strategy that incorporates identification, authentication, policies, and education, organisations can place themselves on the path for cloud success.

and data is that more and more, traffic and even data stored on the cloud is being encrypted. It is therefore only on the client that you can be certain to see the traffic in the clear as well as get full understanding of what happens on the client when a piece of code is executed.

User credentials are another target for attackers. Gaining these through methods such as social engineering and other 'non-technical' means enables cybercriminals to gain 'legitimate' access to the cloud services and data. Since the service perceives these users to be correctly identified via their authentication, all the security technologies built into cloud are circumvented and attackers can carry out their objectives without raising any suspicion.

#### Critical first steps to cloud security

At Help AG, we understand that usage of the cloud is inevitable and work closely with our customers to enable them to securely leverage cloud services. To secure the new frontier of enterprise attacks, you need to first understand the robustness of your endpoint security and configuration. This involves ensuring and operating a solid endpoint security solution and evaluating the state of the endpoints in your network before connecting them to any cloud service. To understand the need for this, consider that many users will be accessing services from their personal devices, and even if they use an enterprise issued device, the responsibility for updating and ensuring the operating systems and applications on these are up to date will lie with the users themselves.

Authentication is the next piece of the endpoint security puzzle. You must have the ability to identify the device and authenticate users (with due consideration to aspects including Who/What/Where) before connecting them to the cloud. Such strong authentication for any service must apply to all devices and since users can't always be trusted to observe best password practices, technologies such as single sign-on and multi-factor authentication must be incorporated. Location of access should also be taken into consideration as policies can and will often change according to this.

Finally, even with the best technologies, policies and practices in place, the cybersecurity chain is only as strong as its weakest link. So, to truly secure the

endpoint and ready it for cloud utilisation, organisations must dedicate resources to educating users. After all, these are the individuals who will be at the frontlines of attacks and training will help them understand why the technical controls you have in place must be adhered to.

While cloud services can shift the responsibility for security away from the IT team over to the cloud provider, it does not absolve anyone of need to conduct due diligence. In the era of the cloud, the endpoint is set to be at the forefront of cyber-attacks and with the right strategy that incorporates identification, authentication, policies, and education, organisations can place themselves on the path for cloud success. □

<sup>1</sup> <https://www.khaleejtimes.com/uae-cloud-service-market-set-to-cross-dh1b>

**Nicolai Solling** is CTO at Help AG.

Help AG provides leading enterprise businesses and government organisations across the Middle East with tailored cybersecurity assurance services and solutions that addresses the most diverse and complex requirements. Founded in Germany in 1995, we have been present in the Middle East since 2004 and have firmly established ourselves as the region's leading cybersecurity advisor.

Our Cyber Security Analysis Division offers essential security services that are imperative to uncovering security vulnerabilities that would otherwise go unnoticed. We offer extensive technical expertise in delivering penetration test, detailed web assessment, mobile application hacking, social engineering, and source code review services, to guide our customers' security investments so that they can best secure their information, data and assets.

For more information, please visit [www.helpag.com](http://www.helpag.com)





**HELP AG**  
PROTECTING INFORMATION

**\$5.31**  
million

Average total cost of a data breach  
for organizations in the Middle East

(Source: Ponemon Institute)



Not encrypting data would be analogous to not locking the bank vault!

# DATA ENCRYPTION IS A KEY COMPONENT OF A LAYERED SECURITY APPROACH

HELP AG HELPS CLIENT STAY SECURE- FROM END  
POINTS AND NETWORK TO DATA ITSELF

## SOLUTION SELECTION CRITERIA



Proven, tested  
and certified  
solution



Ease of  
deployment and  
management



Minimal impact on  
performance and  
business processes



Broad  
range of  
use cases



Skilled and  
resourceful  
implementation  
partner

To help our clients stay secure HELP AG offers best-of-breed solutions for comprehensive security, from advanced end-point protection and network security to data encryption.

Visit [www.helpag.com](http://www.helpag.com), Phone us at +971 4 440-5666 or Email at [info@helpag.com](mailto:info@helpag.com).

# 21st Century Fox: Leveraging OneTrust for privacy compliance

Many companies are evolving from a traditional business-to-business operation into a more direct-to-consumer business model.

## OneTrust reports

21st Century Fox (21CF) is one of the world's leading media companies. With a global portfolio of cable, broadcast, film, payTV and satellite assets spanning six continents across the globe, 21CF properties reaches nearly two billion subscribers each day. Fox, National Geographic, Fox News, Twentieth Century Fox, FX and Star India are all brands under the 21CF portfolio.

Like many companies in the ever-changing media landscape, 21CF is too evolving from a traditionally business-to-business operation into a more direct-to-consumer business model. Data-driven insights are incredibly valuable to delivering 21CF content to the right people at the right time, but can cause data protection concerns.

21CF took a proactive approach to its privacy programme to assure its consumers that they have the policies and procedures in place to protect their data. Two years before the 2018 deadline, 21CF hired Fabrizia Giacomini as its VP Associate General Counsel of EU Data Protection to get the company GDPR ready.

### A simple tool to solve a complex business challenge

21CF is a complex, multinational organisation, according to Giacomini, and ensuring data protection across various regions and global privacy regulations was an initial challenge to compliance. 21CF took a risk-adverse approach to its privacy programme. Even in cases where GDPR may not be a requirement (based on region or number of employees), 21CF chose to implement the most privacy-focused approach.

"We chose OneTrust to help with the complexity of our business," explained Giacomini. "We wanted to ensure we were doing all we could to meet GDPR requirements, and OneTrust helped. I found OneTrust to be so intuitive and easy to use, even for a lawyer like me!" she said.

### Building a privacy management programme to scale

To get started, Giacomini created a network of internal privacy champions in specific 21CF's operating countries. Together with DLA Piper, the law firm assisting 21CF with GDPR implementation, they customised the OneTrust environment to meet the needs of the organisation and structure.

With the OneTrust environment set, 21CF inputted data into the system and began sending out assessment automation queries and data mapping questionnaires to various business units across the company. The network of privacy champions helped evangelise the process across the organisation and increase response times. With this information, Giacomini was and continues to be able to identify risks and mitigate data protection gaps within the company.

### Looking forward to ePrivacy and marketing compliance

As 21CF looks beyond GDPR into other global privacy laws like the ePrivacy Regulation, Giacomini and her team plan to leverage other OneTrust modules for marketing compliance.

"Consent tracking is the next mission for our websites and any product or service where there is a web form," she said. Marketing compliance is a major priority for the business, and Giacomini can leverage OneTrust Universal Consent to track marketing consent for compliance.

Also on the list is OneTrust Cookie Compliance and Website Scanning. "We already love the cookie tool and are just waiting for development and progress with the ePrivacy pieces of regulation for our final decision on cookies," said Giacomini.

From assessment automation, to data mapping, to DSARs, to universal consent and cookie compliance, Giacomini is able to bring all the aspects of a GDPR-compliance programme together into one tool with OneTrust.

"My goal has been to have everything in one place," she said. "OneTrust is a real one stop shop for privacy. I can't understate the importance of using a tool instead of doing it by yourself. You may need to invest more on the front end, but the work more than pays itself back in the end." □

For more information, please visit  
[www.onetrust.com](http://www.onetrust.com)

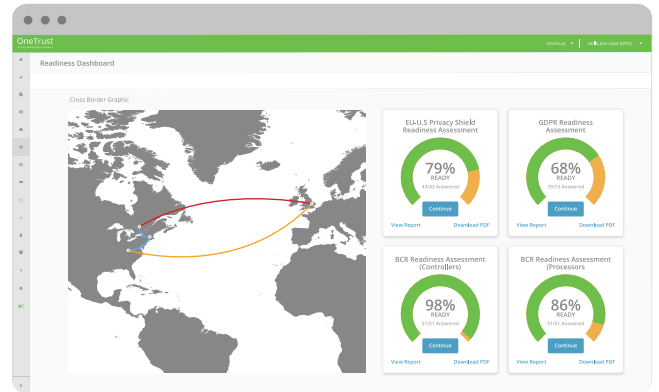


# OneTrust

Privacy Management Software

## A SINGLE PLATFORM TO MANAGE PRIVACY RISKS AND COMPLIANCE

OneTrust is the global leader for GDPR and Privacy Management Software used by over 1,500 organisations to manage privacy risks and compliance with comprehensive platform for Privacy Programme Management and Marketing Compliance.



### PRIVACY PROGRAMME MANAGEMENT TOOLS



#### Assessment Automation

Streamline privacy assessments (PIA/DPIA) and generate regulator-ready reporting

GDPR Articles 5, 24, 25, 35 & 36



#### Data Inventory & Mapping

Create a comprehensive data inventory and map for processing activities and assets

GDPR Articles 6, 30 & 32



#### Vendor Risk Management

Review and remediate vendor risks with detailed privacy and security templates

GDPR Articles 28, 24, 29, 46



#### Incident & Breach Management

Assess incidents to inform breach notification decisions and provide reporting

GDPR Articles 33 & 34

### MARKETING & WEB COMPLIANCE TOOLS



#### Data Subject Rights Management

Facilitate, document, and resolve data subject requests via a secure messaging portal

GDPR Articles 12-22



#### Website Compliance Scanning

Conduct a privacy scan of websites to identify and categorise tracking technologies

ePrivacy



#### Cookie Consent Management

Manage user consent and preferences with adaptable settings for various consent standards

GDPR Articles 4(11), 7, 21, & ePrivacy



#### Universal Consent & Preference Management

Generate, store and sync consent records to demonstrate accountability

GDPR Articles 4(11), 6-9

### WHY OVER 1,500 ORGANISATIONS CHOOSE ONETRUST



#### Most Comprehensive TECHNOLOGY

200 Member R&D Team Driving Product Innovation with 20 Patents Awarded



#### World-Class Privacy RESEARCH

Over 100 Certified Privacy Professionals In-house with Continuous Privacy Research



#### Expert Global SERVICES

Multi-lingual, 50 Person Consulting Team and Large Global Partner Network



#### Large Active User COMMUNITY

Thousands of Members Sharing Best Practices in 55 Global PrivacyConnect Workshops.

1500  
CUSTOMERS

500  
EMPLOYEES

6  
GLOBAL LOCATIONS

50  
LANGUAGES

# The evolution and future of SIEM

To combat advanced threats and meet the growing demands of the security market, SIEM solutions have also been evolving over the years to leverage new-age technology including big data analytics and machine learning.

## ManageEngine reports

Security information and event management (SIEM) has been a crucial component of security operations for several years now. Scheduling daily reports to review activity and investigate events of interest has always been, and perhaps always will be, an important aspect of IT compliance. But with the evolution of cyber-attacks, basic log management techniques no longer suffice. To combat these advanced threats and meet the growing demands of the security market, SIEM solutions have also been evolving over the years to leverage new-age technology including big data analytics and machine learning.

### Expanding your security boundary to include the cloud

One of the biggest concerns in today's IT security landscape is that businesses are moving to the cloud. Although the cloud helps increase productivity, it also creates new security challenges. Users and computers are no longer confined to the boundaries of the corporate network, making it harder to monitor them.

For example, you may have a user in your sales team who's always travelling and connecting to the corporate network via VPN, or you may have users working on cloud platforms such as Azure, AWS, and Office 365. Keep in mind, all of these platforms see interactions between users and data, too, and must be continuously monitored.

What if one of these remote users connect to a network that's not secure? What if they unknowingly download a malicious file? What if a disgruntled employee copies customer data stored in one of your cloud platforms? To truly gain visibility into your network, you need to audit logs from your public cloud infrastructure.

### Combating insider threats with UBA

Insider threats are on the rise, which means you need to track all user activity in your network, including that of administrators. This is where user behaviour analytics (UBA) is redefining the way security teams track insider threats. Instead of only monitoring known indicators of compromise (IOCs) such as repeat failed access attempts, UBA uses machine learning techniques to detect deviations from normal user behaviour so you can more quickly spot threats.

## Receiving alerts and responding to security incidents swiftly can help you avoid data breaches that could otherwise cost you millions.

For example, if a user normally works from 9am to 5pm but tries to remotely access a file server at 11pm, UBA can alert you about this suspicious activity. In fact, UBA has become so popular that many vendors provide dedicated solutions just for monitoring user behaviour.

### Using correlation to discover security incidents

To keep up with the advances in analytics, event correlation engines have become more dynamic. These powerful correlation engines can associate several disjointed pieces of event information to unravel security incidents that would've otherwise gone unnoticed. Many SIEM vendors have also added correlation rules to detect modern-day cybersecurity threats like cryptomining.

Additionally, many SIEM solutions provide integrations to speed up the process of incident detection and response. Threat feeds can be integrated with SIEM solutions to detect and block known malicious sources. Some SIEM solutions come with built-in integrations with threat feed providers while others allow you to integrate custom threat feeds that you've purchased.

Going one step further, integrating with ticketing tools allows you to raise alerts as tickets for the designated security administrator to streamline the process of incident management. Receiving alerts and responding to security incidents swiftly can help you avoid data breaches that could otherwise cost you millions.

Now's as good a time as ever to evaluate your SIEM solution, because when it comes to mitigating data breaches, effective SIEM is a game changer. □

For more information, please visit  
[www.manageengine.com](http://www.manageengine.com)

**ManageEngine** 

# Bringing IT together

for over **180,000** customers  
with more than **90** products  
across **6** continents.



## ManageEngine®

Comprehensive IT management software  
for all your business needs.

[www.manageengine.com/middle-east](http://www.manageengine.com/middle-east)

# More offensive security testing at one of Europe's largest banks, Banco Santander

Trust in the cybersphere is more critical than ever.

**Ron Peeters,**  
**Synack**

**Reghu Mohandas,**  
**SecureLink**

**Mayank Verman,**  
**SecureLink**

**B**anco Santander is one of the largest banks in Europe and in the top-15 worldwide. Trust in the cybersphere is more critical than ever, which is why companies like Banco Santander are committed to building and maintaining their customers' trust. To do that, they realised they have to transform to a more scalable and dynamic cybersecurity model.

Santander knows their customers are trusting them to keep personal information and digital transactions safe, which is why they opt for a cyber-defence that matches the innovation and agility of their own business model. The bank has adopted crowdsourced security, because they know that the model provides effectiveness, efficiency and control that traditional models have failed to deliver on.

How did Santander get here? To protect its constantly changing attack surface, Santander thought of a simple security strategy: test anything new and anything that had been updated. In theory, this strategy was good, but practically, it was difficult to implement. Traditionally each pen test done took an average of 5 days to complete, and the testing period was followed by an additional two weeks for the final written. Given their vendor's limited access to skilled researchers, it was hard to test more than one asset at a time. The traditional model wasn't scaling at the speed of Santander UK's software development and deployment. Dave Sheridan, Banco Santander UK CISO, looked to Synack to help them push out new software securely, without slowing down the business.

Within 36 hours of their first program launch with Synack, Banco Santander was notified that the Synack Red Team had found a critical vulnerability, which could have taken down banks across the globe. Santander had full control of the Synack platform at all times and could drive the cadence that was comfortable for their team. Throughout the testing with Synack, Santander got valuable real-time data about the Synack Red Team testing activity and details on each vulnerability that proved invaluable to the security and DevOps teams to efficiently remediate the issues. Synack provided Santander with detailed and actionable reports including potential business impact and replicable steps for prompt and effective remediation of vulnerabilities found.

"My number one goal is to protect our customers. Even a series of small risks can be aggregated into a massive one, with the potential to do a lot of damage. We rely on third-party insights from Synack's crowd to understand our risk from an attacker's perspective, which is extremely valuable to us," Sheridan said.

As businesses become increasingly digital and agile to deliver products and services easily and conveniently to their consumers, these benefits come with a caveat. A recent study by IDG revealed that 78% of consumers would stop engaging with a brand if the brand experienced a data breach. Protecting the brand and business in a digital world threatened by damaging cyber-attacks is just as important as running the business in the first place. Cybersecurity has become an endeavour of building consumer trust.

Synack's main goal is to help its customers lower their vulnerability against cyber-attacks and attack surface, thereby building trust with their own customers. Trust is a mantra that transcends all stages of the relationships that Synack plays a part in, from Synack to Synack customer, Synack customer to end consumers, security teams to development teams and hackers to companies. □

**"To put it simply, my goal as CISO has always been to make Santander a safer place for our customers to bank."**

**Dave Sheridan, Santander UK CISO**

**Ron Peeters** is  
Managing Director  
EMEA at Synack.



**Reghu Mohandas** is  
Director Risk Advisory  
& Analytics at SecureLink.



**Mayank Verman** is Manager Consulting Service  
at SecureLink.

To learn more about Synack, visit us at  
**[www.synack.com](http://www.synack.com)**

To learn more about SecureLink, visit them at  
**[www.securelinkme.net](http://www.securelinkme.net)**





# THE LEADING CROWDSOURCED SECURITY TESTING PLATFORM



## **MORE EFFECTIVE**

Find serious, exploitable vulnerabilities  
your last pen test missed

## **DISRUPTIVE APPROACH**

Combine the world's best researchers with military  
grade reconnaissance technology

## **TRANSPARENT PLATFORM**

Cloud solution with no footprint  
and a real-time customer portal

## **FAST DEPLOYMENT AND RESULTS**

Deploy in days; comes with actionable  
remediation advice and free re-testing

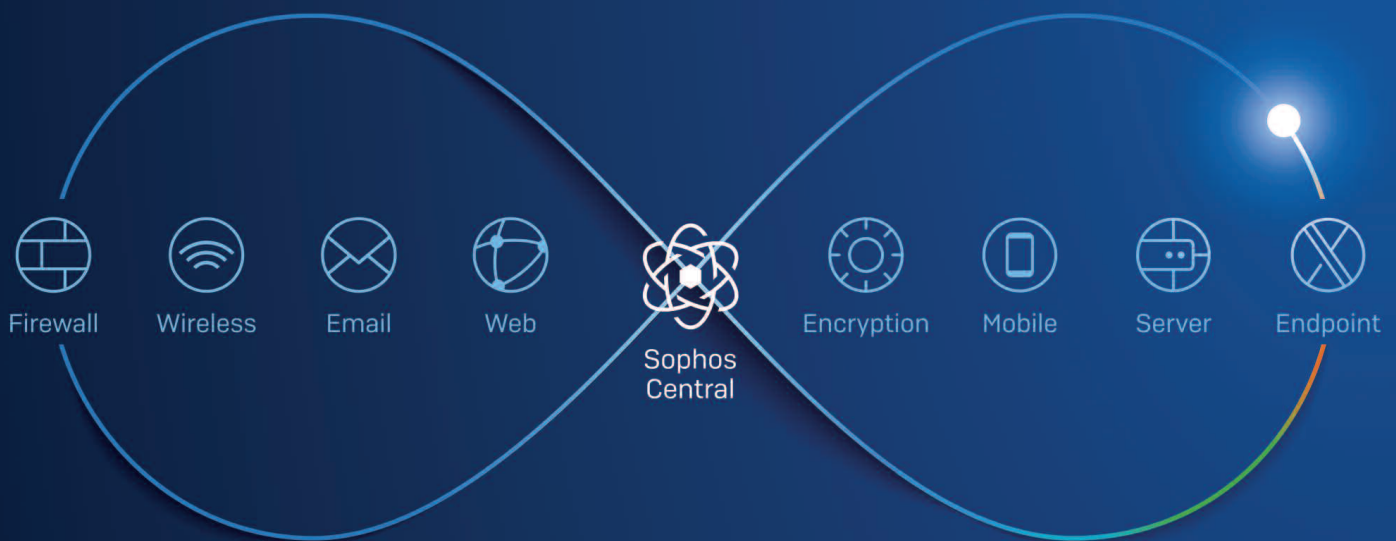
Visit us at [www.synack.com](http://www.synack.com)

**SECURELINK**

Visit SecureLink at [www.securelinkme.com](http://www.securelinkme.com)

# Synchronized Security

It's time your security solutions started talking.



Sophos Central allows you to manage our award-winning Synchronized Security platform. Advanced attacks are more coordinated than ever before.

For more details contact [salesmea@sophos.com](mailto:salesmea@sophos.com)

# SOPHOS

[www.sophos.com/en-us/lp/synchronized-security.aspx](http://www.sophos.com/en-us/lp/synchronized-security.aspx)



# Synchronised security: cybersecurity as a system

Cybersecurity is not getting any easier.

Connectivity is one of the defining characteristics of the 21st century, permeating every aspect of our lives. We depend on it for both our business and personal lives. As countries in the Middle East region continue to adopt digital technologies and implement e-services, so are the opportunities for cybercrime increasing. Unsurprisingly, today's enterprising cybercriminals have enthusiastically embraced connectivity. They use a range of connected techniques in their malware attacks: a phishing email leads to an initial foot in the door, followed by a malware infection through exploitation of a known or unknown defect, then an escalation of privileges or a lateral movement across the network to spread the infection across different devices. A single compromised device can mean your network and connectivity are held hostage or used for malicious intent. Essentially, they exploit our IT connectivity to achieve their malicious ends.

Cybersecurity is not getting any easier – we continue to face the same core challenges we did 10 or even 20 years ago. Indeed, rather than making progress in the fight against cyber-attacks, 83% of IT managers agree that threats have actually got harder to stop over the last year. In addition to exacerbating security risks, our disconnected approach to cybersecurity also puts a heavy burden on IT teams. Manually correlating data between systems and identifying appropriate actions burns valuable hours. A busy administrator may not mentally assemble the disparate events across the various products in order to realise that there is an attack or compromise underway.

While standalone cybersecurity solutions can address specific vectors of attack, cybercriminals will continue to be able to exploit the gaps between point solutions and take advantage of the lack of connectivity. Organisations need a layered approach to security, one where products connect and share information. It's time to embrace this new approach. It's time for Synchronised Security.

Synchronised Security is cybersecurity as a system. Security solutions connect with each other in real time via a Security Heartbeat™, working together to combat advanced threats. This automation enhances your defences, responding automatically to events, so you can mitigate risk and slash the time and effort spent managing IT security. Synchronised Security is

built on three pillars: Discover, Analyse, and Respond. These pillars enable security components to become more than the sum of their parts by working together to stay ahead of the attackers.

The more security services that share real-time information in a Synchronised Security system, the more you can benefit from their inter-connectivity. Here are three of the ways Synchronised Security elevates your protection while simplifying IT security management.

- ***Slash incident response time: 3.3 hours to 8 seconds***

Identifying and remediating infected computers is a laborious task, taking on average 3.3 hours per machine. Synchronised Security's automated threat response slashes that down to just 8 seconds. It automatically responds to threats and provides detailed analysis of exactly what happened across your entire infrastructure so you can prevent future recurrences.

- ***Take back control of your network***

A recent survey revealed that IT managers can't identify almost half (45%) of the traffic running through their network. As a result, they cannot block risky or malicious traffic – instead, it flows through the organisation unchecked and unhindered. Synchronised Security is the simple, elegant solution to this problem. The endpoint always knows the true identity of an application – even if it tries to disguise itself from the firewall to avoid being blocked. By enabling the endpoint and firewall to share application identity information in real time, the firewall can identify all the network traffic and the IT team can take back control of their network. With the information to hand, they can enhance security by blocking malicious apps while speeding up business applications by de-prioritising non-work traffic

- ***Reduce risk from mobile devices***

Mobile devices are just as much a door to your organisation's data and systems as your desktops and laptops. Mobile devices travel with us everywhere, connecting to a wide variety of protected and unprotected networks, making their security state questionable. Allowing compromised devices to access the network increases your risk of attack. Yet on its own the wireless network cannot make any judgement as to the health of the devices connecting to it.

**Malay Upadhyay reports**

By working together, security solutions can detect, analyse, and respond automatically to incidents and infections. This slashes response time and enables IT security to switch from being a business cost to a business enabler.

Again, Synchronised Security, this time between the mobile and wireless solutions, provides the answer to the problem.

Cybersecurity is traditionally associated with cost and inconvenience. For finance teams it's an often significant line in the IT budget. And for the wider organisation it's a dull necessity that takes IT teams away from delivering business-enabling projects. The enhanced protection with Synchronised Security reduces downtime while freeing up valuable IT staff to work on growing the business. The implementation of Synchronised Security will help IT to enable the business organisations in:

#### Operational cost savings

- Save day-to-day IT security resources by controlling all your IT security through a single console
- Reduce resources spent making disparate products play well together by using solutions engineered to work together
- Be up and running with new products quickly – no new interface to learn

#### Vendor consolidation

- Streamline purchasing by working with a single supplier for all IT security solutions
- Simplify ongoing vendor management with a single point of contact for all support needs (technical, sales, finance)

#### Cyber risk mitigation

- Stop hackers moving across your network to find a more valuable person (e.g. escalated privileges) or asset (e.g. server)
- See how the threat entered and spread with full root cause analysis, enabling you to act to prevent future security risks
- Identify risky apps and users through visibility of all network traffic

#### Improve productivity

- Reduce user downtime from infections and incidents with adaptive policies that automatically respond to threats. Slash average response time from 3.3 hours to 8 seconds
- Improve response speed by managing all your IT security through a web-based platform that can be accessed from any location
- Avoid downtime from product compatibility by choosing solutions engineered to work together

#### Complete estate visibility

- See and control all your IT security services in one place – anytime, anywhere – through the web-based platform
- See all network traffic, enabling identification of risky apps and malicious traffic
- Identify risky users by correlating behaviour across multiple activities

#### Enhance the profile of IT

- Reduce downtime from infections and incidents from hours to seconds
- Free up IT to better support the business by working with a single vendor, and single support team
- Avoid downtime from product compatibility with solutions engineered to work together

We live in an interconnected world and with half of the world using the internet, IDC estimates that there will be 30 billion connected devices in the market by 2020. Focusing on individual point security products is not the answer – not only does it leave us vulnerable to threats, it also increases the cost of IT security to the business. Rather than resisting connectivity, it's time to actively take advantage of an integrated approach by moving to cybersecurity as a system. By working together, security solutions can detect, analyse, and respond automatically to incidents and infections. This slashes response time and enables IT security to switch from being a business cost to a business enabler. □

**Malay Upadhyay** is Technical Head Middle East at Sophos.

For more information, please visit [www.sophos.com](http://www.sophos.com)

**SOPHOS**  
Cybersecurity made simple.

# Sponsors and exhibitors

## Arrow | Principal Sponsor



*For more information, please visit [www.arrowecs.co.uk](http://www.arrowecs.co.uk)*

## RSA | Principal Sponsor



*For more information, please visit [www.rsa.com](http://www.rsa.com)*

## Help AG | Strategic Sponsor

Help AG provides leading enterprise businesses and government organisations across the Middle East with tailored cybersecurity assurance services and solutions that addresses the most diverse and complex requirements. Founded in Germany in 1995, we have been present in the Middle East since 2004 and have firmly established ourselves as the region's leading cybersecurity advisor.



Our Cyber Security Analysis Division offers essential security services that are imperative to uncovering security vulnerabilities that would otherwise go unnoticed. We offer extensive technical expertise in delivering penetration test, detailed web assessment, mobile application hacking, social engineering, and source code review services, to guide our customers' security investments so that they can best secure their information, data, and assets.

Help AG's offering for information security governance and compliance is based on our unique Governance & Assurance Framework, which ensures that information security follows a risk-based and information-centric approach, to meet an organisation's specific needs and compliance requirements.

Our Cyber Security Operations Centre (CSOC), which is staffed by top-level security analysts, offers monitoring, analysis and interpretation of security events occurring within your infrastructure 24 hours a day and 7 days a week. Help AG Managed Security Services (MSS) is designed to detect, analyse and respond about security threats, malicious, abnormal and unauthorised behaviour, as well as anomalies and deviations in trends and baselines specific to your organisation.

Help AG's Incident Response service allows you to recognise an incident, evaluate the associated risks, and determine the most effective approach to remediate the incident. Our approach to incident response enables you to position your organisation a step ahead of any incident.

We value our customers' privacy and although local data collection is a must, we handle this in the most secure way possible by our unique service offering that ensures that data does not leave the customer's environment.

*For more information, please visit [www.helpag.com](http://www.helpag.com)*

**OPSWAT | Strategic Sponsor**

Founded in 2002, OPSWAT has since grown to become a global company. Headquartered in San Francisco, they also have offices in Romania, Hungary, Vietnam, Taiwan, Japan, Israel, and the UK.



Today, they have nearly 200 employees, over 1,000 customers, hundreds of technical partners, and dozens of resellers, but their mission is the same: to provide the most effective threat prevention technology possible.

To solve the challenges faced by modern enterprises and to shut off major attack vectors, they offer two product platforms: MetaDefender for threat prevention and MetaAccess for cloud access control and endpoint compliance. Their guiding principles: Trust No File. Trust No Device.

*For more information, please visit [www.opswat.com](http://www.opswat.com)*

**Recorded Future | Strategic Sponsor**

Recorded Future delivers the only complete threat intelligence solution powered by patented machine learning to lower risk. We empower organisations to reveal unknown threats before they impact business, and enable teams to respond to alerts 10 times faster. To supercharge the efforts of security teams, our technology automatically collects and analyses intelligence from technical, open, and dark web sources and aggregates customer-proprietary data. Recorded Future delivers more context than threat feeds, updates in real time so intelligence stays relevant, and centralises information ready for human analysis, collaboration, and integration with security technologies. 91% of the Fortune 100 use Recorded Future.



*For more information, please visit [www.recordedfuture.com](http://www.recordedfuture.com)*

**Sophos | Strategic Sponsor**

Sophos is a leader in next-generation endpoint and network security. As the pioneer of synchronised security, Sophos develops its innovative portfolio of endpoint, network, encryption, web, email and mobile security solutions to work better together. More than 100 million users in 150 countries rely on Sophos solutions as the best protection against sophisticated threats and data loss. Sophos products are exclusively available through a global channel of more than 34,000 registered partners. Sophos is headquartered in Oxford, UK and is publicly traded on the London Stock Exchange under the symbol 'SOPH'.



*For more information, please visit [www.sophos.com](http://www.sophos.com)*

**Shape Security | Strategic Sponsor**

Shape Security is defining a new future in which excellent cybersecurity not only stops attackers, but also welcomes good users. Shape disrupts the economics of cybercrime, making it too expensive for attackers to commit online fraud, while enabling enterprises to more easily identify and transact with genuine customers on their websites and mobile apps. The world's leading organisations rely on Shape as their primary line of defence against attacks on their web and mobile applications, including three of the Top 5 US banks, five of the Top 10 global airlines, two of the Top 5 global hotels and two of the Top 5 US government agencies. The Shape platform, covered by 55 patents, was designed to stop the most dangerous application attacks enabled by cybercriminal fraud tools, including credential stuffing (account takeover), fake account creation, and unauthorised aggregation. Today, the Shape Network defends 1.7 billion user accounts from account takeover and protects 30% of all US savings. The company is headquartered in Mountain View, California, and also has offices in London and Sydney.



*For more information, please visit [www.shapesecurity.com](http://www.shapesecurity.com)*

## ThreatMetrix | Strategic Sponsor

ThreatMetrix®, a LexisNexis Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion anonymised user identities, ThreatMetrix ID™ delivers the intelligence behind 100 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters.



*For more information, please visit [www.threatmetrix.com](http://www.threatmetrix.com)*

## Virsec | Strategic Sponsor

Virsec is an innovative cybersecurity leader protecting industrial controls from today's most dangerous threats. Through its unique technology, Virsec prevents attacks that bypass conventional security tools, such as fileless attacks, memory exploits and attacks that weaponise at runtime (WRT). Virsec's patented Trusted Execution™ deterministically stops advanced attacks in real-time, delivering unprecedented accuracy, while eliminating false positives. The solution provides virtual patching for any application, whether new, legacy, or un-patchable.



*For more information, please visit [virsec.com](http://virsec.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, please visit [www.anomali.com](http://www.anomali.com)*

## Kaspersky Lab | Education Seminar Sponsor

Kaspersky Lab is a global cybersecurity company and celebrated its 20-year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.



*For more information, please visit [me-en.kaspersky.com](http://me-en.kaspersky.com)*

## ManageEngine | Education Seminar Sponsor

ManageEngine simplifies IT management with affordable software that offers the ease of use SMBs need and the powerful features the largest enterprises demand. More than 90,000 companies around the world – including three of every five Fortune 500 companies – trust our products to manage their networks and data centres, business applications, and IT services and security.



At the show, ManageEngine will showcase: Log Analysis, IT Security & Compliance, Network Performance Management & Monitoring, Integrated IT Management, Help Desk & Desktop Management – ITSM, Active Directory Management & Auditing, Server & Application Performance Management.

*For more information, please visit [www.manageengine.com](http://www.manageengine.com)*

## OneTrust | Education Seminar Sponsor

OneTrust is the largest and most widely used dedicated privacy management technology platform for compliance with global privacy laws. More than 2,000 customers, including 200 of the Global 2,000, use OneTrust to comply with global data privacy regulations across sectors and jurisdictions, including the EU GDPR, ePrivacy (Cookie Law), the California Consumer Privacy Act and more. An additional 10,000 organisations use OneTrust's technology through a partnership with the International Association of Privacy Professionals (IAPP), the world's largest global information privacy community.



The comprehensive platform is based on a combination of intelligent scanning, regulator guidance-based questionnaires, automated workflows and developer plugins used together to automatically generate the record keeping required for an organisation to demonstrate compliance to regulators and auditors. The platform is enriched with content from hundreds of templates based on the world-class privacy research conducted by our 300+ in-house certified privacy professionals.

The software, available in 50+ languages, is backed by 43 awarded patents and can be deployed in an EU cloud or on-premise.

OneTrust is co-headquartered in Atlanta, GA and in London, UK, with additional offices in Bangalore, Melbourne, Munich and Hong Kong. The fast-growing team of privacy and technology experts surpasses 650 employees worldwide.

*For more information, please visit [OneTrust.com](https://www.onetrust.com)*

## SABSA | Education Seminar Sponsor

SABSA, the world's leading free-use and open-source security architecture development, management method and framework is changing the enterprise architecture landscape. With SABSA Chartered Security Architects in over 50 countries around the world, SABSA is transforming information security, risk management, and even compliance & audit, into 'Centres of Business Enablement'.



SABSA does not start with technical matters but focuses on the creation of models and frameworks to enable business opportunities while remaining within the risk appetite of real stakeholders, establishing real traceability from business requirements to solutions.

SABSAcourses are the foremost global provider of Accredited SABSA Training, with training locations spanning Europe, The Middle East, Africa, North America and India. Our diverse range of training and consulting options allow for an enterprise security architecture solution for organisations of all sizes and levels of maturity.

*For more information, please visit [www.sabsacourses.com](https://www.sabsacourses.com)*

## Synack | Education Seminar Sponsor

Synack offers a new and more disruptive security testing platform for finding and helping resolve serious vulnerabilities in mission critical applications and infrastructure that otherwise go undetected. It arms clients with large teams of international top class security researchers who can provide a more diverse, adversarial perspective to clients' IT assets; often without taking hours or days.



Combined with the deployment of self-learning, intelligence-based reconnaissance technology and a transparent AI-enabled platform with a real-time customer portal, it provides a more advanced and effective way for security testing. This next-generation testing platform overcomes the shortcomings of traditional pen testing and vulnerability scanning and better simulates increasingly sophisticated cyber-attacks and TTPs.

The Synack solution comes in a continuous security testing subscription to assure protection of mission critical assets. For assets that demand point-in-time testing there is a 14-days security test.

*For more information, please visit [www.synack.com](https://www.synack.com)*



## Thales eSecurity | Education Seminar Sponsor

Thales eSecurity is a leader in advanced data security solutions and services, delivering trust wherever information is created, shared or stored. We ensure that company and government data is secure and trusted in any environment – on premise, in the cloud, in data centres and in big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices.



Thales eSecurity provides everything an organisation needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenisation, privileged user control and meeting the highest standards of certification for high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organisation's digital transformation. Thales eSecurity is part of Thales Group.

*For more information, please visit [www.thalesecurity.com](http://www.thalesecurity.com)*

## TNCT | Education Seminar Sponsor

As an IT service-provider organisation, TNCT was established with the focus on offering professional IT services in order to address the market requirements in the Middle East and Africa regions for true value-added IT services including educational services, technical implementation and project management services, consultancy services, as well as pre-sales and post sales technical support services. Being a high-tech service-oriented organisation and given our skills and expertise in the network security domain we aim to deliver such value-added services with the best quality yet in the most efficient way. Our present focus is to provide these value-added services for technologies and solutions from Check Point Software Technologies within GCC and Africa regions.



*For more information, please visit [www.tnctrade.com](http://www.tnctrade.com)*

## Airlock Digital | Networking Sponsor

At Airlock Digital, we want to turn the security paradigm on its head, because we believe a fundamentally different approach is needed to combat the risk posed by adversaries, such as cybercriminals and nation state attackers.



About 10 years ago the industry moved from a prevention to a detect and response mindset. Having decided that it's too difficult to prevent attacks, there was a push to detect, respond and remediate.

Most organisations find it extremely difficult to reduce the risk of intruders and we believe at Airlock we can reduce the risk of sophisticated threats towards zero.

Application whitelisting is considered one of, if not the most effective control in reducing the risk posed by targeted attacks and malware/ransomware. Even though most security experts agreed on the effectiveness of application whitelisting as a security control we continued to see that organisations were reluctant to embark on implementing application whitelisting. This was primarily due to the reputation the application whitelisting had as being resource intensive to manage and maintain.

Airlock Digital was started with a single goal. To develop a solution to allow organisations to implement application whitelisting at scale in dynamic computing environments utilising a simple, well defined, repeatable process.

Our platform provides a framework and workflow that greatly reduces the burden typically associated with application whitelisting whilst ensuring the integrity of the control is maintained.

*For more information, please visit [www.airlockdigital.com](http://www.airlockdigital.com)*

## ARCON | Networking Sponsor

ARCON is a leading enterprise information risk control solution provider, specialising in privileged access management and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help them control by robust solutions that predict, protect and prevent.



ARCON is a privately held technology company, which was established in London in 2006 with a research and development centre in Mumbai.

The Mumbai-based company has now been in the domain for more than 10 years.

Having started as an upcoming tech start-up, the Company is now recognised as one of the world's most trusted brands by information security professionals.

Our product portfolio includes three robust risk control solutions:

- ARCON | Privileged Access Management
- ARCON | Secure Compliance Management
- ARCON | User Behavior Analytics

We are a team of futurists. Our product development strategy is based on constant interactions with the industry thought leaders. Close collaboration allows us to understand emerging technology-related threats for organisations. Subsequently, we brainstorm and develop best-in-class solutions that enable enterprises to overcome humongous challenges related to information security.

Our enterprise-class solutions provide seamless access and have scalable architecture. More than 250 global enterprises, spanning wide-ranging industries such as banking, finance, insurance, government organisations, oil & gas, pharmaceutical, logistics, Fintech trust ARCON solutions to safeguard critical business information.

ARCON is widely recognised by the analyst community such as Gartner and KuppingerCole. The Company has a global presence, enabled by its well-distributed partner network.

While we continue to be a leader in India and the Middle East, we are fast gaining traction in the APAC region, Africa and Europe.

*For more information, please visit [www.arconnet.com](http://www.arconnet.com)*

## Cloudflare | Networking Sponsor

Cloudflare, Inc. is on a mission to help build a better internet. Today the company runs one of the world's largest networks that powers more than 10 trillion requests per month, which is nearly 10% of all internet requests worldwide. Cloudflare protects and accelerates any internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all traffic routed through its intelligent global network, which gets smarter with each new site added. As a result, they see significant improvement in performance and a decrease in spam and other attacks.



Cloudflare was recognised by the World Economic Forum as a Technology Pioneer, named the Most Innovative Network & Internet Technology Company for two years running by the Wall Street Journal, and ranked among the world's 50 most innovative companies by Fast Company. Headquartered in San Francisco, CA, Cloudflare has offices in Austin, TX, Champaign, IL, New York, NY, Washington, DC, London, and Singapore.

*For more information, please visit [www.cloudflare.com](http://www.cloudflare.com) or follow us on Twitter @cloudflare*

## DriveLock | Networking Sponsor

DriveLock SE, is headquartered in Munich, Germany with offices and distributors in the USA, Australia and Middle East. The expert for cybersecurity has become one of the leading Endpoint Protection Platform software vendors over the past 15 years.



The Endpoint Protection Platform from DriveLock is particularly strong when used in the extremely granular environment of device control for USB protection, as well as for the encryption of hard disks, SSDs or USB memory devices. Applications and their associated devices can be comprehensively protected with the Smart AppGuard based on integrated artificial intelligence with predictive whitelisting and machine learning functionality.

DriveLock supports various operating systems, devices, and is available as a hybrid solution either on-premise or from the cloud.

Facts and figures:

- Multiple awards as an endpoint protection solution
- Honoured as a TOP 100 innovator in 2017 and 2018
- More than 3,000 customers in 30 different countries across the world
- Customer environments with up to 180,000 endpoints supported
- Made in Germany, 'without a backdoor'

*For more information, please visit [www.drivelock.com](http://www.drivelock.com)*

## emt Distribution | Networking 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 programme 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](http://www.emtdist.com)*

## PGI | Networking Sponsor

PGI is a specialist British cybersecurity company. We help our clients build their in-house cybersecurity capability through consultancy, assurance and training.



PGI's Cyber Academy builds technical cybersecurity skills using UK government-certified courses and a powerful, immersive cyber range. We address skills shortages – creating new cybersecurity staff through reskilling, and helping practitioners develop advanced skills. Government agencies – including SAMA and CBK – and banks in six Middle Eastern countries have used PGI to reskill, train and certify staff for SOC, penetration testing, forensics, incident response and consultancy roles. Government and academic institutions in the Middle East, Europe and SE Asia have also chosen us as a training partner. And CISOs recently named PGI 'Most Effective Training Provider' in the AKJ Associates 'Who Secures the UAE' report (<https://www.cyberviser.com/who-secures-the-uae-report>).

PGI has worked with its corporate, critical infrastructure and government clients in the EMEA region to develop their security functions including Security Operations Centres (SOCs), Cyber Threat Intelligence Teams (CTIs), and Cyber Security Incident Response Teams (CSIRTs). We designed roles and operational processes, and advised on selecting, implementing and tuning technology solutions.

We offer a full range of cybersecurity services. We are accredited to design and implement IS management systems ranging from ISO27001 to Cyber Essentials according to business need and maturity. Our penetration testing and incident response services are approved by the UK government and registered through the CREST scheme. Our experienced consultants bring current operational experience of government and commercial cybersecurity best practice and risks.

*For more information, please visit [www.pgiti.com](http://www.pgiti.com)*

## SECURRENT | Networking Sponsor

Against today's complicated cybersecurity challenges, SECURRENT is a trusted partner of yours by delivering the best security solutions by combining best expertise and outstanding services since 2009.



Located in Istanbul and Dubai, SECURRENT provides next generation network security, identity and access management, PCI DSS consultancy and payment security, encryption management, ICS/SCADA Security services and cloud security solutions for enterprise-class organisations.

SECURRENT is the key partner of leading security vendors like Check Point, Backbox, CyberArk, Thales, Gemalto, Forcepoint, Tufin and more.

SECURRENT will reveal the details of Check Point's new Gen V Infinity platform and Backbox's Intelligent Automation solutions for all network and security devices during the event.

*For more information, please visit [www.securrent.com](http://www.securrent.com)*

## FireEye | Branding Sponsor

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cybersecurity for organisations struggling to prepare for, prevent, and respond to cyber-attacks.



FireEye has over 7,700 customers across 103 countries, including more than 50% of the Forbes Global 2000.

*For more information, please visit [www.fireeye.com](http://www.fireeye.com)*

## Green Method | Branding Sponsor

Green Method is a leading specialist information security services provider in the UAE. Green Method was established in the UAE in 2008.



Over the years, Green Method has assisted various clients in banking & financial services, government, utilities, hospitality, transportation, retail and large & medium enterprises in multiple services offerings and has built an extensive clientele in the region.

Green Method provides a wide range of consulting services, testing services, training and solutions in this domain. Green Method recently launched Managed Security Services in Dubai through its subsidiary Green Sentries.

Green Method had been pioneering the cause of evangelising the information security best practices in the country and has executed a number large and small turnkey projects for some of the leading organisations here. Green Method had been in the forefront in assisting the organisations to be aligned with the evolving security standards.

Green Method has shown exemplary efficiency in enhancing the security posture of the organisations, and that too within their stringent budgets, resulting in continuous, repeated engagements. Our prestigious list of customers includes some of the major names in the region in the financial, government and other sectors.

Green Method partners with the world majors in the domain. Our Partner Veracode provides the world's leading Application Risk Management Platform and has been ranked # 20 among the Forbes list of promising companies. Green Method has several other partnerships with leading providers like Mimecast, Wombat, Groundlabs, that has helped achieve the significant growth witnessed in the recent years.

---

*For more information, please visit [greenmethod.net](http://greenmethod.net)*



# AGENDA

08:00	Breakfast networking and registration		
08:50	Chairman's welcome		
09:00	<b>In it for the long run; building a sustainable solution to cybersecurity resourcing</b>		
	<p><b>Craig McEwen</b>, Global Head of Cyber Operations, Anglo American</p> <ul style="list-style-type: none"> <li>• Current state of affairs – attacks etc</li> <li>• Current state of affairs – recruitment figures</li> <li>• Future touch points – OT (blended or dedicated and a complete lack of existing skill in the OT area)</li> <li>• Winning the war, not the battle – apprenticeships, talent development etc</li> <li>• What should we be looking for – what is easier to train, cyber-skill and a natural talent/analytical mind etc</li> </ul>		
09:20	<b>Communicating with the Board effectively – security strategy definition 101</b>		
	<p><b>Antonio Campos Dionisio</b>, Group CIO, MIG Holding, and <b>Frank Murray</b>, CISO, Associate Vice President – IT Security, Risk &amp; Business Resilience, MIG Holding</p> <ul style="list-style-type: none"> <li>• Understanding your stakeholders. Identify different functions' business risks, and communicate your message accordingly</li> <li>• Hacking the boardroom. Gaining executive management buy-in by adopting the model of a hacker</li> <li>• Defining your priorities. It's not just about the budget or the underlying technologies. Understand the value for the business instead of 'just squeezing money' out of the board</li> </ul>		
09:40	<b>The dark secrets of the Dark Web: an insight into this unique asset and risk, and how it differs from other sources of intelligence</b>		
	<p><b>Nour Fateen</b>, Pre-sales Consultant, Recorded Future</p> <ul style="list-style-type: none"> <li>• Real-world examples of threat actor activities in dark marketplaces</li> <li>• Methods for uncovering emerging threats using Dark Web sources</li> </ul>		
10:00	<b>The emergence of credential stuffing and cybercriminal AI</b>		
	<p><b>Shuman Ghosemajumder</b>, CTO, Shape Security</p> <ul style="list-style-type: none"> <li>• Credential stuffing has been named by CSO Online as the #1 most significant security issue in 2019</li> <li>• Shuman Ghosemajumder, CTO of Shape Security, will explain how this threat has evolved, starting from when Shape first introduced the term to the marketplace over seven years ago, to how it gained international prominence in numerous sophisticated public attacks</li> <li>• He will also provide insights into the heightened challenges businesses are facing as a result of cybercriminals leveraging AI to attack websites and mobile apps in these cases</li> </ul>		
10:20	<b>Education Seminar   Session 1</b>		<b>See pages 30 to 32 for more details</b>
	<p><b>Anomali</b> <b>Threat actor – a love story?</b> <b>Andrew de Lange</b>, Solutions Consultant, Anomali</p>	<p><b>Kaspersky Lab</b> <b>The ceaseless evolution of consumer transformation</b> <b>Tim Ayling</b>, Kaspersky Fraud Prevention Lead, Kaspersky Lab</p>	<p><b>OneTrust</b> <b>Risky business: a privacy &amp; security team's guide to risk scoring</b> <b>Ian Evans</b>, Managing Director, EMEA, OneTrust</p>
	<p><b>Thales eSecurity</b> <b>Re-evaluating data security in modern, multi-faceted environments</b> <b>Slam Laqtib</b>, Sr. Product Manager, Thales eSecurity</p>		
11:00	Networking and refreshments		
11:30	<b>Running the risks and regulations. The insider truth on cyber-risk management</b>		
	<p><b>Christos Christou</b>, Chief Compliance Officer, Lulu Exchange</p> <ul style="list-style-type: none"> <li>• Introduction to AML/CFT risk management – the regulatory requirements</li> <li>• Security – what is required from a business perspective and how important is security to the decision to make or buy?</li> <li>• Cloud vs Hosted services – what is the business perception and what is the regulatory requirement?</li> <li>• How do we manage the AML/CFT risk and security in Lulu Financial Group?</li> </ul>		
11:50	<b>Harnessing the power of a digital identity network: reducing e-crime, building trust</b>		
	<p><b>Andy Renshaw</b>, Senior Director, Market Planning, Fraud and Identity, ThreatMetrix</p> <ul style="list-style-type: none"> <li>• How harnessing a global view of trust, and risk, helps detect and block advanced fraud</li> <li>• Building trust using digital identity intelligence can help better distinguish between good customers and fraudsters in near real time</li> <li>• An analysis of recent attack patterns and fraud typologies from the ThreatMetrix Digital Identity Network, which analyses 110 million transactions a day</li> </ul>		
12:10	<b>FILES: The enfant terrible of any IT environment</b>		
	<p><b>Nicolai Solling</b>, Chief Technology Officer, Help AG Middle East</p> <ul style="list-style-type: none"> <li>• There are thousands of file formats and they are ultimately the agents that deliver everything from a website to an attachment in your inbox. While files are good and deliver functionality, they can also be bad, weaponised delivery vehicles for malware</li> <li>• In this session we will talk about files, the types one should be extra careful about and how these are utilised in social engineering, malware and crypto-attacks</li> <li>• In a world where attackers have more resources and capabilities than ever, we will discuss how small changes and new technologies can significantly increase your robustness against both file-based and file-less attacks</li> </ul>		

<b>12:30</b>	<b>Industrial control, ICS-SCADA and other vital systems</b>			
	<p><b>Atiq Raza</b>, CEO, Virsec, and <b>Bobby Gupta</b>, VP of Sales for APAC and EMEA, Virsec</p> <ul style="list-style-type: none"> <li>• Critical infrastructure systems around the world are under assault from targeted cyber-attacks seeking to cause damage, disruption, theft and significant financial losses. Advanced attacks like Stuxnet, BlackEnergy, Triton, and Industroyer bypass conventional security and subvert legitimate applications and processes to infiltrate sensitive systems</li> <li>• Virsec is the first solution to provide ICS cybersecurity and protect industrial control systems (ICS), supervisory control and data acquisition (SCADA), and other mission-critical applications at the process memory level. Acting as a memory firewall, Virsec scrutinises application process memory to ensure that critical applications only behave as intended and aren't corrupted by advanced exploits</li> </ul>			
<b>12:50</b>	<b>Education Seminar   Session 2</b>			<b>See pages 30 to 32 for more details</b>
	<p><b>OneTrust</b>  <b>A privacy playbook for 'reasonable and appropriate' security measures and safeguards</b>  <b>Ian Evans</b>, Managing Director, EMEA, OneTrust</p>	<p><b>SABSA</b>  <b>Using SABSA techniques to develop a cybersecurity strategy</b>  <b>Michael Hirschfeld</b>, Cyber Security Adviser, SABSA</p>	<p><b>Synack</b>  <b>Offensive security testing with a Hacker mindset</b>  <b>Ron Peeters</b>, Managing Director EMEA, Synack</p>	<p><b>TNCT</b>  <b>Let's demystify cloud security!</b>  <b>Ilmaz (Kory) Kashkooli</b>, Managing Director, TNCT</p>
<b>13:30</b>	Lunch and networking			
<b>14:30</b>	<b>Getting smart about threat intelligence</b>			
	<p><b>Ebrahim AL-Alkeem</b>, Information Security Manager, ENEC</p> <ul style="list-style-type: none"> <li>• How AI impacts and aids threat intelligence</li> <li>• How AI impacts and aids threat intelligence: how they are using AI in the cybersecurity effort</li> <li>• How and where to invest in AI and machine learning tools</li> </ul>			
<b>14:50</b>	<b>Synchronised security: cybersecurity as a system</b>			
	<p><b>Malay Upadhyay</b>, Technical Head Middle East, Sophos</p> <ul style="list-style-type: none"> <li>• Ever changing threat landscape</li> <li>• How a tightly integrated cybersecurity system enables you to stay ahead of the adversaries and nation-state attacks</li> <li>• How to turn cybersecurity from a business cost to a business enabler</li> </ul>			
<b>15:10</b>	<b>Upping the cybersecurity benchmark. How good is good enough?</b>			
	<p><b>Suresh Nair</b>, Chief Information Security Officer, MENAT, GE</p> <ul style="list-style-type: none"> <li>• The various challenges of large multi-national corporations vs. SMEs</li> <li>• Managing third-party security. Is the security of your third parties as important as the security of your organisation itself? How do you audit and benchmark the security of your third parties?</li> <li>• 'Minimum baselines and standards' of cybersecurity. How do you decide what is the bare minimum for your business?</li> <li>• Cyber-risk management. What are the metrics? How do you model and analyse cyber-risk?</li> </ul>			
<b>15:30</b>	<b>Cyber: the senior management perspective</b>			
	<p><b>Balaji Nagabhusan</b>, Group Chief Administrative Officer, Tristar Transport</p> <ul style="list-style-type: none"> <li>• What do your senior management and stakeholders want to know about the cybersecurity of your organisation?</li> <li>• How does cybersecurity fit alongside other functions such as risk, legal and CSR?</li> <li>• Risk management perspective. How has cybersecurity become a wider part of overall operational risk? Is cyber-risk unique? And should it be measured and valued in the same way as other forms of operational risk?</li> <li>• Communicating with stakeholders. What do they need to know and how does cybersecurity now arguably affect the market share price and commercial value of an organisation?</li> </ul>			
<b>15:50</b>	Networking and refreshments			
<b>16:10</b>	<b>Journey from the 'dark side': one business leader's journey from vendor to end-user</b>			
	<p><b>Neil Haskins</b>, Head of Security &amp; Technology Operations, Careem</p> <ul style="list-style-type: none"> <li>• Double perspectives on navigating the solutions provider landscape and truths about cybersecurity budget and procurement</li> <li>• The journey from the dark side, the transition to the good side. What both sides know – and need to share – about cyber-resilience</li> <li>• Case study from Careem: what went wrong. And what we did to put it right...</li> </ul>			
<b>16:30</b>	<b>EXECUTIVE PANEL DISCUSSION</b>	<b>The new inconvenient truths on AI, machine learning and its impact on business</b>		
	<p><b>Adam Lalani</b>, Group Head of IT, Tristar Transport  <b>Ebrahim AL-Alkeem</b>, Information Security Manager, ENEC  <b>Brian Byagaba</b>, Senior Manager Information Security, Commercial Bank International  <b>Bharat Gautam</b>, Head of Information Security, DAMAC Properties</p>			
<b>16:50</b>	<b>Making Big data big business. How information security and data governance can work to your commercial advantage</b>			
	<p><b>Mike Pitman</b>, CISO, Dunhumby</p> <ul style="list-style-type: none"> <li>• Information security as a commercial competitive advantage</li> <li>• How your data governance can win or lose you clients</li> <li>• The CISO as business enabler: working with commercial functions</li> <li>• ISO 27001 certification: Does this give your clients confidence or a false sense of security?</li> </ul>			
<b>17:10</b>	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: 10:20–11:00

### Anomali

#### Threat actor – a love story?

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

SESSION 1  
10:20–11:00

Do we romanticise cyber-threat actors? When a cyber-incident strikes, we may love the idea that it is some APT (insert number here) or Fancy/Angry (insert animal here) or some other famous threat actor, perhaps with nation-state abilities. But we may also hate the idea that it might be: these are the most dangerous adversaries. In reality our enemies aren't even on our radar, because we turn a blind eye to the smaller signals our controls catch for us. But sometimes these are small pieces of a bigger puzzle we need to understand.

#### What you will learn in this seminar:

- Leveraging critical thinking and finding trends in the noise
- Actor profiling
- The importance of remaining unbiased in your research
- Collaboration to find the common enemy

### Kaspersky Lab

#### The ceaseless evolution of consumer transformation

**Tim Ayling**, Kaspersky Fraud Prevention Lead, Kaspersky Lab

SESSION 1  
10:20–11:00

In this presentation, hear about the recent history and the future of technology and consumer patterns and drivers. This session explores the continued proliferation of social media, IoT, cryptocurrency & artificial intelligence and the implications of this technology. The huge rise in cybercrime and fraud highlights the challenges businesses face across all industries.

This session takes a look at what those challenges are, how we can react to them and what we can do better.

#### It covers:

- Changes in our digital lives and how this drives the consumer
- The value of data in today's world and the implications of this
- The current state of e-fraud

### OneTrust

#### Risky business: a privacy & security team's guide to risk scoring

**Ian Evans**, Managing Director, EMEA, OneTrust

SESSION 1  
10:20–11:00

Risk scoring across vendor management, breach notifications, DPIAs and other activities is imperative for compliance with many global privacy laws and security frameworks. Organisations routinely tailor their data protection and security activities based on the results of detailed risk assessments, but this leads to a myriad of questions. How do you calculate risk? What constitutes low, medium or high risk? How do you define a risk criteria? What's the difference between inherent, current and residual risk? In this session, we'll detail the importance of conducting risk assessments under global privacy laws like the GDPR and security frameworks such as ISO 27001, provide scenario-based approaches to risk assessment and give examples on how to tailor your approaches based on risk level.

- Understand various approaches to conducting risk assessments
- Learn how to define a risk criteria and how to calculate risk level
- Learn how to tailor your privacy and security programmes using a risk-based approach

### Thales eSecurity

#### Re-evaluating data security in modern, multi-faceted environments

**Slam Laqtib**, Sr. Product Manager, Thales eSecurity

SESSION 1  
10:20–11:00

Businesses, institutions and government agencies continue to be breached. Hackers have proven that





traditional technologies and conventional approaches are not enough to prevent this epidemic. This is true even for the most sophisticated organisations with world-class security specialists and scientists. And now the challenge has become more complex, with deployments involving the rise of multi-faceted environments, including on-premises, public cloud and hybrid cloud implementations. Because breaches are inevitable, rendering data useless to hackers by applying data security best practices is critical: using key management and encryption to attach security to the data itself is the only way out.

In this talk, we will do a deep dive into:

- Securing data and rendering it useless in multi-cloud and hybrid environments
- Best practice key management, encryption, tokenisation and de-identification techniques
- Cloud management as a service with true multi-cloud support

## Session 2: 12:50–13:30

### OneTrust

**A privacy playbook for 'reasonable and appropriate' security measures and safeguards**

**Ian Evans**, Managing Director, EMEA, OneTrust

SESSION 2  
12:50–13:30

With a new era of privacy regulations upon us, requirements for implementing 'reasonable and appropriate' security measures and safeguards are becoming more common than ever. While privacy and security professionals often view security from different perspectives and may have competing priorities, there are a number of ways in which these differences can be used to the advantage of both teams. In this session, we'll share a playbook on how to build a harmonised and risk-based security framework that addresses a variety of divisions within an organisation, as well as how security and privacy teams can work together to become more effective.

- Understand the requirements and importance of

implementing 'reasonable and appropriate' security measures and safeguards for privacy professionals

- Outline several areas of common ground that should help every organisation align their security and privacy operations
- Take away a playbook for building a harmonised and risk-based security framework

### SABSA

**Using SABSA techniques to develop a cybersecurity strategy**

**Michael Hirschfeld**, Cyber Security Adviser, SABSA

SESSION 2  
12:50–13:30

The SABSA architectural methodology has a number of tools, techniques and frameworks that can help IT security professionals understand the challenges they face, present and discuss with their executive and stakeholders when building and progressing a cybersecurity programme.

Fundamentally, a strategy is a document that sets out how you plan to achieve a series of long-term objectives.

Within cybersecurity our objectives must be closely aligned with those of the ICT group and, just as importantly, with those of the business as a whole.

If our cybersecurity strategy isn't helping the business or ICT meet their objectives, then we will struggle to articulate our relevance and we will find it difficult to get budget. On the other hand, when our strategy clearly aligns and strengthens the business we are viewed more as a partner.

This presentation will cover a few of the basics of SABSA, provide you with a framework for a cybersecurity strategy and then demonstrate how understanding and applying some key techniques from the SABSA tool kit can assist you in developing and presenting a coherent and aligned cybersecurity strategy that the business will understand.

**What attendees will learn:**

- The basics of SABSA



- How to structure a cybersecurity strategy
- Key inputs into the cybersecurity strategy
- Key techniques for developing a cybersecurity strategy

## Synack

SESSION 2  
12:50–13:30

### Offensive security testing with a Hacker mindset

**Ron Peeters**, Managing Director  
EMEA, Synack

CISOs are experiencing exponential growth in cyber-attacks, and those attacks are increasingly sophisticated with greater break-in success. Traditional vulnerability scanning and compliance-based penetration testing have proven insufficient to reduce vulnerability against such malicious hackers and Nation State attacks.

#### During this session, attendees will learn:

- Why traditional solutions such as vulnerability scanners and pen testing are no longer sufficient enough to protect against cyber attacks
- Of a revolutionary security testing approach that deploys large teams of international, top-class security researchers
- How a controlled crowdsourced deployment platform can find serious vulnerabilities in any live system within a matter of hours
- And you'll hear about several case studies, including one on the Pentagon where Synack was able to break in within just four hours

## TNCT

SESSION 2  
12:50–13:30

### Let's demystify cloud security!

**Ilmaz (Kory) Kashkooli**, Managing Director, TNCT

- How much of the 'cloud' do we really use on a day-to-day basis?
  - Chances are we think we do not use any form of cloud-based services. In fact, it is otherwise and we will be reviewing some examples in our daily lives which are clear indications of how extensively we actually utilise cloud-based services in our daily lives.
  - The reality of 'shadow-IT' as an inevitable result of using cloud!
- A quick introduction of cloud-based services (Something-as-a-Service)!
  - Nowadays we come across a long list of 'something-as-a-service'! Let's take a look at some of these terms and demystify them a bit.
- A closer look at SaaS and IaaS as well as their use cases and some of the security concerns.
  - Why, where and when do we seem to use SaaS or IaaS based cloud-based services?
  - Before starting to use SaaS and IaaS we must really be aware of the fundamental security concerns around them in a corporate context.
  - How can we address the listed security concerns as of today using the available technologies?
  - Let's explore some of the challenges that are still not addressed today.
- Final take away – visibility!
  - Cloud is Complex! Security is Complex! And Securing our Cloud usage can be quite Complex! A bird's-eye-view and holistic visibility is KEY to effectively and more pro-actively securing our cloud usage.

# Forthcoming events



2<sup>nd</sup> April 2019  
Paris



18<sup>th</sup> June 2019  
Munich



3<sup>rd</sup> July 2019  
London



17<sup>th</sup> September 2019  
Abu Dhabi



18<sup>th</sup> September 2019  
London



26<sup>th</sup> September 2019  
Stockholm



17<sup>th</sup> October 2019  
London



17<sup>th</sup> October 2019  
London



6<sup>th</sup> November 2019  
Edinburgh



21<sup>st</sup> November 2019  
Madrid



3<sup>rd</sup> December 2019  
Amsterdam



January 2020  
Frankfurt

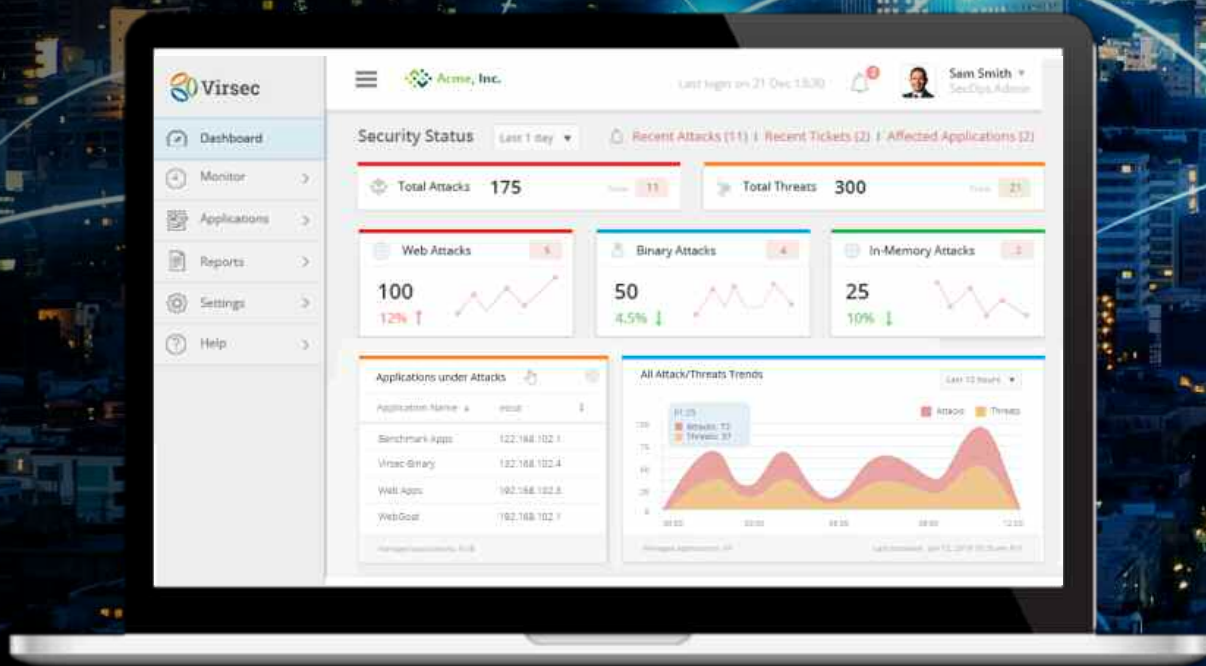


January 2020  
London

For more information, please call Robert Walker on +44 (0)20 7404 4597  
or email [robert.walker@akjassociates.com](mailto:robert.walker@akjassociates.com)

# ADVANCED CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

- Patented memory protection
- Makes applications self-defending
- Virtual patching without downtime



# Speakers and panellists

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

## Tim Ayling

**Kaspersky Fraud Prevention Lead,  
Kaspersky Lab**



Tim has over 20 years' experience in the cybersecurity and anti-fraud industry, beginning straight after university in 1997. Beginning in technical support, and working as a System Engineer, Tim began his leadership career when he established Entrust Inc. in Australia in 2003, being made Vice-President Asia Pacific in 2006.

Tim has held numerous leadership roles in large cybersecurity vendors, including Trend Micro, RSA Security, and now Kaspersky Labs, as well as spending time in the cybersecurity practise of KPMG. Tim holds an MBA from the Warwick Business School, and an MSc in Secure e-Commerce from the Royal Holloway University, University of London.

## Ebrahim AL-Alkeem

**Information Security Manager,  
ENEC**



Ebrahim AL-Alkeem is a global digital leader specialising in the effects of artificial intelligence and other exponentially developing technologies on the economy, healthcare, and society, Ebrahim explains the threats and opportunities created by these new developments. During his 13 years in the cybersecurity industry, Mr Ebrahim has worked with many technologies in different positions from technical to management. Currently, he is managing the information security department within ENEC and acting as CISO.

He holds a Master of Science in Information Security and a bachelor's degree in Communication Engineering from Khalifa University. He is currently pursuing his PhD studies at Khalifa University. Ebrahim has presented many international and domestic seminars and published many papers in the security related field. In 2015, Ebrahim won a Tamayaz Excellence Award, Appreciation award in the category of inventions of information technology & smart services. Also, he is an active member of many of engineering associations across the world.

## Brian Byagaba

**Senior Manager Information Security,  
Commercial Bank International**



In his current role, Brian leads the Information Security team of Commercial Bank International (CBI), which is a UAE-based bank. At the top of his agenda is working with CBI's senior leadership team to prioritise and align security initiatives with the bank's evolving strategy and risk appetite. This is especially important considering the fast pace of changes within cybersecurity, (new threat actors, changing methods and motives of attack) and how banks do business today.

Brian started out in risk management, consulting for clients across multiple industries; from financial services to telecom, retail and oil & gas companies. In his 15 years of security profession experience, Brian has worked in leading institutions such as PwC, Barclays Bank delivering risk projects across Africa, Middle East, Europe and Asia in numerous capacities. Roles included Head of Operational Risk and Information Security, Assistant Manager Systems and Process Assurance, Chief Operating Officer – Technology Risk, Vice President Internal Audit and Chief Internal Auditor. He holds industry certifications including CCISO, CISM, CISA, FCCA and an MBA from Durham University.

## Christos Christou

**Chief Compliance Officer,  
Lulu Exchange**



Christos Christou is a professional Compliance Officer working 28+ years in the banking and non-banking industry. He has a BSc/Associateship degree from IFS, London, and an MBA from the University of Liverpool. He is a CAMS® certified professional and he also has long experience in project management (ex-PMP® certified). He started his career from operations, but after four years he moved into training within the bank due to his excellent knowledge and training talent. Since 1996, he worked part-time as a Tutor/Adjunct Lecturer for professional academies and universities in Europe. In 2000, he was assigned as a Group Project Manager for compliance projects within the bank he worked for and he continued in management positions within compliance, designing

and implementing policies, procedures, and systems. In mid-2013, he moved to UAE and since then he is the Chief Compliance Officer for Lulu International Exchange, managing and directing the compliance and AML/CFT function for the Group having presence in 10 countries around the world.

### Andrew de Lange

**Solutions Consultant,  
Anomali**



Andrew de Lange is a Solutions Consultant for Anomali. Andrew has over 15 years' experience in cybersecurity, with the bulk of that time spent in financial services and banking. He is an evangelist for cyber-threat intelligence collaboration initiatives and community-driven defence.

### Antonio Dionisio

**Group CIO,  
MIG Holdings**



Antonio is a senior executive with more than 24 years of experience working in ICT. He spent 12 years of his career working for Arthur Andersen, Deloitte and 12 years in the insurance industry, notably as Director in Charge of the Security, Continuity, Compliance and IT Risk Centre of Excellence for AXA Mediterranean and Latin American region. He was a permanent member of the Group Security and Continuity Strategic Council and lately held positions as Senior IT Director and CIO. He is now in charge of IT Transformation for MIG Group of companies and is sponsoring the Group Information Security and Business Resilience Programme. Antonio holds a Computer Science degree, Information Systems Security post-graduation and an Advanced Management Certificate from Catolica Lisbon School of Business and Economics.

### Ian Evans

**Managing Director, EMEA,  
OneTrust**

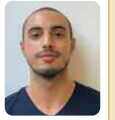


Ian Evans serves as Managing Director for EMEA at OneTrust, a global leader in privacy management and marketing compliance software, which helps organisations operationalise data privacy compliance and Privacy by Design. Evans is a diversified senior executive with over 20 years of experience in data privacy and CRM technology applications and services. In his role, Evans supports thousands of multi-national brands across the European, Middle Eastern, and African regions, leading the delivery of technology solutions to secure and privatise customer and employee personal information under

new privacy regulations. Prior to OneTrust, Evans served as Vice President and Managing Director for EMEA at AirWatch (acq. by VMware in 2014 for \$1.54bn). AirWatch now serves more than 20,000 global customers and is recognised as the undisputed market leader in enterprise mobility management.

### Nour Fateen

**Pre-sales Consultant,  
Recorded Future**



Nour Fateen is a cybersecurity specialist with more than five years in experience in the industry. Currently at Recorded Future, Nour has previously held positions in Cisco Systems and Goldman Sachs. Nour graduated with a master's in Electronic Engineering & Nanotechnology from University College London. Nour has spent the last three years helping some of the largest businesses in the world improve their security posture using threat Intelligence.

### Bharat Gautam

**Head of Information Security,  
DAMAC Properties**



Bharat Gautam is addicted to everything related to cybersecurity/information security and is always trying to contribute to the cybersecurity fraternity. Bharat Gautam brings in multi domain experience and is spearheading the information security vertical as Head of Information Security for a leading luxury real estate developer in Dubai.

Bharat has previously worked with some of the biggest IT consulting companies for many years and brings in 14 years of core cybersecurity knowledge. Bharat is aware of the ever-changing threat landscape and the need to improve our security posture to remain ahead of the internal and external threats.

### Shuman Ghosemajumder

**CTO,  
Shape Security**



Shuman is CTO at Shape Security, whose technology platform protects the web and mobile applications of the world's largest banks, airlines, and retailers, against advanced fraud and cybercrime. In 2018, it was ranked by Deloitte as the #1 fastest-growing company in Silicon Valley and named by Fortune as one of the leading AI companies. Shuman previously led global product management for click fraud protection at Google, enabling \$23bn in pay-per-click annual revenue. He joined Google in 2003 as one of the early product managers for AdSense and helped launch Gmail. He is co-author of CGI Programming

Unleashed (Macmillan Publishing), a contributing author to Crimeware (Symantec Publishing), and a regular guest lecturer at Stanford University. In 2011, the Boston Globe named him to their MIT150 list, as one of the top innovators of all-time from the Massachusetts Institute of Technology.

## **Bobby Gupta**

**VP of Sales for APAC and EMEA,  
Virsec**

Bobby Gupta is Virsec's VP of Sales for APAC and EMEA. Bobby brings more than 20 years of global leadership experience in analytics, cybersecurity, storage, and IT services markets to this role, managing Virsec sales across Asia Pacific, India and MEA. He has held numerous senior management positions, overseeing sales, operations, market development and organisational change.

Prior to joining Virsec, Bobby served as VP Asia Pacific at Guavus, VP West Coast Cognizant, Senior Vice President at Tech Mahindra and Asia Pacific Leader at IBM Global Services. Bobby has been part of Global Transformation Teams and is experienced in selling large scale, complex transformation deals and has led sales teams with revenues of \$300m.

## **Neil Haskins**

**Head of Security & Technology  
Operations, Careem**



Neil is a senior executive specialising in information and cybersecurity with nearly 30 years of architectural, operational and leadership experience. He holds memberships in the Institute for Information Security Professionals and the Royal United Services Institute for Defence and Security studies. He has operated within both internal security organisations and external consultancy practices. He is credited with designing, delivering and implementing enterprise security programmes and provided thought leadership to Fortune 500/FTSE 100 organisations. Neil is currently the Head of Security & Technology Operations for a \$2.5bn company. He has had articles published in several newspapers and magazines. Neil was a security expert referenced in the NHS 'WannaCry' incident and has been published as a cryptocurrency expert in Forbes, InfoSecurity Magazine, The Independent and most recently, Bobs Guide.

## **Michael Hirschfeld**

**Cyber Security Adviser,  
SABSA**



Michael is a Cyber Security Adviser with David Lynas Consulting providing high-level assistance on cyber-

related matters. He was formerly the Chief Information Officer and CISO at the Australian Commonwealth Department of Finance and where he had executive responsibility for ICT as well as physical security within that agency. He has previously held senior roles with a number of Australian government agencies including as Assistant Secretary for ICT Planning and Governance at the Australian Department of Foreign Affairs and Trade and Assistant Secretary, ICT Efficiency Review undertaken in 2009. Through his public sector career, Michael has worked in nine agencies responsible for delivering a range of Commonwealth services to the Australian community. He has been involved in both business and technology systems, advising on issues such as security, audit outcomes and risk management. He was Head of Technology Security for the Australian Taxation Office in the early noughties.

Michael has been involved in security for the past 18 years and has been effectively educated by a group of excellent technical staff. He was involved in a number of early working groups defining the direction of whole of government initiatives in both e-Government and e-security including the 'Secure Communications' and 'On-line Authentication' working groups and has been a member of the Protective Security Policy Committee. He takes a leadership role in the delivery of ICT and security services to organisations focussing on risk analysis, governance and assurance, policy and awareness in building effective and practical security measures. He has a diverse background and has been managing major projects since the mid 80s. He began his career as a Programmer and Project Manager on building control and IT systems and holds a Bachelor of Engineering, a Diploma in Education and a Master of Business Administration. In 2011, he participated in the Executive Leadership Programme delivered by the Lee Kuan Yew School of Public Policy at the National University of Singapore.

## **Ilmaz (Kory) Kashkooli**

**Managing Director,  
TNCT**



Ilmaz (Kory) Kashkooli is the founder of TNCT, a Cybersecurity System Integrator team that no matter what has always stayed loyal to its core values of professionalism, integrity, and innovation. Kory has more than 17 years of experience in the IT industry most of which has been focused on network security, virtualisation and cloud security. Throughout this journey, he has had various roles such as: network engineer, IT instructor, technical support engineer, pre-sales engineer, and an entrepreneur. As a technical and people person who is passionate about technology and intrigued with nature, he firmly

believes in the spirit of teamwork and sees it as a key and determinant factor that significantly contributes to the success of a complex cybersecurity project as well as sustainability of the deployed technologies. In the past 10 years, Kory and his team in TNCT have successfully completed more than 70 complex network security implementation projects for various customers ranging from government, banking, utilities, oil and gas, hospitality, health care, retail, and insurance throughout UAE, Oman, Qatar, and Canada.

### **Adam Lalani**

**Group Head of IT,  
Tristar Transport LLC**



Adam Lalani is the Group Head of IT for the Tristar Group of Companies. Tristar is a fully integrated liquid logistics company servicing the downstream oil and gas industry with one-stop fuel logistic solutions offering surface transport, ocean shipping, dangerous goods warehousing, fuel farm management, aviation, petroleum retail, chemicals, and turnkey fuel supply operations. The company has a presence in 18 countries spread across the GCC, Africa, Asia, Pacific and Central America and employs more than 1,800 people.

In his varied career, he worked for one of the UK's oldest high street chains tasked with a Y2K driven phase-out of old IBM AS/400 mainframes, before working on an automation project for 150 stores across the UK that provided real time sales data from each outlet. Later, he worked as the IT Manager for Europe and the Middle East for the steel trading subsidiary of Arcelor Mittal (Macsteel) before joining ESHIPS as Head of IT & Administration – working on projects that included the early adoption of various cloud computing technologies. He moved to Tristar as a result of their US\$90 million acquisition of ESHIPS in March 2016. At Tristar, Adam led the implementation of the region's first production Blockchain SCM solution as well as the Group's various digital transformation efforts. Adam is a certified ITILv3 Expert, a PRINCE2 Project Management Practitioner, a Member of the British Computer Society and holds an MSc in Computer Network Management.

### **Slam Laqtib**

**Sr. Product Manager,  
Thales eSecurity**



Slam Laqtib is a well-known figure in the encryption world as a speaker and technology evangelist with over 20 years' experience. As a Silicon Valley software veteran, Slam has designed innovative key management and data protection technologies and

solutions; he has also architected and deployed numerous data protection solutions for enterprise and government organisations, globally. Prior to joining Thales eSecurity, his previous experience includes stints at Ingrian, SafeNet, and Gemalto as well as other market leaders in the security space. Slam has worked and lived in Africa, Scandinavia and the US. Slam has spoken at several e-crime conferences worldwide.

### **Craig McEwen**

**Global Head of Cyber Operations,  
Anglo American**



Craig McEwen is the Global Head of Cyber Operations at Anglo American, a position he has held since 2017. Before this role, Craig held a number of senior roles in threat intelligence and cybersecurity at Vodafone and other internationally established institutions. Craig has worked primarily in the defence sector, and has experience and expertise in managing large budgets, running large scale projects and navigating spending constraints when it comes to cybersecurity investment.

### **Frank Murray**

**CISO, Associate Vice President – IT  
Security, Risk & Business Resilience**



Frank has over 12 years of experience in technical IT security and risk in defence, legal and insurance sectors. With experience in both operational and strategic security functions, Frank has the unique skillset of Red teamer turned Architect. In previous roles, Frank was instrumental in the delivery of ISO 27001 and 22301 certification for the world's largest law firm, and worked extensively on projects for the US, UAE, British and Australian military.

Prior to joining MIG, Frank was Security Architect for AXA Group in the Gulf region, implementing a comprehensive security transformation programme. He is now leading the IT Security, Risk & Business Resilience unit for MIG Group of companies. Frank holds a Computer Science degree and CISSP, CEH, CISA, CISM, GIAC GCIH and GMON certifications and is a member of the GIAC Advisory Board.

### **Balaji Nagabhusan**

**Group Chief Administrative Officer,  
Tristar Transport**



Balaji is Group Chief Administrative Officer at Tristar Group. Experienced in setting up governance, controls, compliance, AML, risk & investigation functions in banking & finance, Balaji is a natural leader managing teams efficiently and able to



connect and convince top management. He has the important certifications necessary to continue improving his skills and knowledge in the subject areas.

### Suresh Nair

**Chief Information Security Officer –  
MENAT, GE**



Suresh is currently Chief Information Security Officer – Middle East, North Africa & Turkey (MENAT) at GE Global, a position he has held since 2018. In this role, he is responsible for defining cybersecurity strategy for MENAT region and providing strategic leadership to IT security related projects and initiatives. Suresh supports all GE businesses including healthcare, aviation, power, oil & gas in the MENAT region.

Before this position, Suresh was Regional Leader for Gulf and Turkey. Here he aligned security initiatives with enterprise programmes and business objectives for the Gulf & Turkey region, ensuring that information assets and technologies are adequately protected. Suresh has been at GE since 2016. Before GE, he held a number of senior positions across the cybersecurity solutions industry.

### Ron Peeters

**Managing Director EMEA,  
Synack**



Ron Peeters is a seasoned IT industry executive with more than 30 years' experience in IT working for an array of advanced technology companies around the world. As Managing Director, he is responsible for the Europe, Middle East and Africa region for Silicon Valley based Synack, Inc., a rapidly emerging market leader in offensive security testing and controlled crowdsourced ethical hacking. Ron is a Dutch National with an MBA from Case Western Reserve University in High Tech Marketing.

### Mike Pitman

**CISO,  
dunnhumby**



Mike is a senior information security professional, with over 18 years' experience who has worked at CISO level at a number of national and International organisations, across a variety of industries, including public sector, manufacturing, HR, finance & retail. He is currently the CISO at dunnhumby having recently taken up the position in February 2018, where his responsibilities include security risk management, security consulting and security operations. At dunnhumby, he is leading a global information security transformation programme,

which puts the security at the heart of the business and aims to make it the differentiator from their competitors when it comes to bidding for new business. Before joining dunnhumby, Mike headed up the information security function at the John Lewis Partnership for three years and was Global CISO at Adecco prior to that.

### Atiq Raza

**Chairman & CEO  
Virsec Systems, Inc.**

Atiq Raza is the Chairman & CEO of Virsec Systems, Inc. Mr Raza is an industry veteran and has been working in engineering leadership and senior management positions for the past 32 years. He was the Founder, Chairman and CEO of RMI, which was acquired by NetLogic which in turn was acquired by Broadcom on the strength of the RMI processor. Earlier, he was Chairman and CEO of NexGen, the first company to challenge Intel in microprocessors. NexGen became a public company and subsequently was acquired by AMD. Atiq became the President and COO of AMD and served on its Board of Directors.

Atiq holds a bachelor's degree in Physics from Punjab University, a BS with Honours degree in Electrical Engineering from the University of London, and a MS degree in Materials Science & Engineering from Stanford University.

### Andy Renshaw

**Senior Director, Market Planning,  
Fraud and Identity, ThreatMetrix**



At LexisNexis Risk Solutions, Andy helps solve the complex challenges of the evolving fraud, identity and authentication market, getting to the root of business problems and architecting solutions to match. Andy brings deep industry expertise from working in the financial services industry, skilled in banking, credit analysis, fraud solutions, risk transformation, and anti money laundering. He is a driven and highly motivated leader with exceptional analytical skills and a creative approach to strategic thinking.

### Nicolai Solling

**Chief Technology Officer,  
Help AG Middle East**



Nicolai Solling is the Chief Technology Officer at Help AG Middle East. In this role, he is responsible for overseeing Help AG's professional services, support services, and technical vendor management across the region. In addition to overseeing technical services and solutions delivered in the market, he is

also involved in coordinating the enablement of teams and making sure they are good at delivering the technologies Help AG takes to market.

Since joining the company in 2008, he has successfully grown the technical team by more than 200% and has been heavily involved in the design, deployment, and operation of some of the most challenging network and security infrastructures for enterprise customers across a variety of industry sectors. Solling has been in the IT and network industry for over 20 years. He is one of the most well-known names in the industry thanks to his in-depth knowledge of cybersecurity technologies combined with his vast experience in security solutions, integration as well as pre-sales and design. He is a great speaker and has been part of multiple distinguished panels and keynote sessions both regionally as well as internationally.

As a thought-leader, he has authored numerous publications on various trends and topics in

cybersecurity. Prior to joining Help AG, Solling worked as a Systems Engineering Manager for Juniper Networks in the Nordic region. He has also worked with Cygate Denmark and Cisco earlier. The love for technology caught Solling quite early in life; he had found his passion at the age of 8, when his family got its first X86 PC machine.

### Malay Upadhyay

**Technical Head Middle East,  
Sophos**



Malay Upadhyay is the head of Sophos' technical team in the Middle East where he leads a team of engineers. He received a master's in Computer Science from the University of Technology Sydney, Australia. He has been involved in the information security field for more than 12 years and when not tinkering with security tools, Malay talks at trade shows and raises awareness of security issues at public events. □

# 11<sup>th</sup> e-Crime & Cybersecurity Congress IN ABU DHABI



“ It was great to participate in the e-Crime & Cybersecurity Congress in Abu Dhabi on the 19th September 2018. The congress was very informative, the topics were interesting, and there was a wide variety of vendors. ”

Senior IS Auditor,  
State Audit Institution

“ It was a fantastic experience attending the 10th e-Crime & Cybersecurity Congress in Abu Dhabi. As usual, e-Crime exceeded our expectations. The presentations have always been refreshing, realistic and updated according to the current trends on how to mitigate the risk of cybercrime. ”

IT Manager,  
Al Muqren Exchange

“ It was a really great event. Everything was perfect starting from the registration and presentation timings until the closing of the event. ”

Senior Officer IT Security,  
Daman

2018 sponsors included:		
Principal Sponsor		
		
Strategic sponsors		
		
		
		
Education Seminar Sponsors		
		
		
		
Networking Sponsors		
		
		
		
		
Branding Sponsors		
		

For more information, please call Robert Walker on +44 (0)20 7404 4597  
or email [robert.walker@akjassociates.com](mailto:robert.walker@akjassociates.com)

# Digital transformation escalates compliance challenges

Digital transformation is changing the face of the modern data-driven enterprise.

## Thales eSecurity reports

The 2019 Thales Data Threat Report-Global Edition found that

97% of organisations surveyed are implementing digital transformation with 37% reporting aggressive transformation.

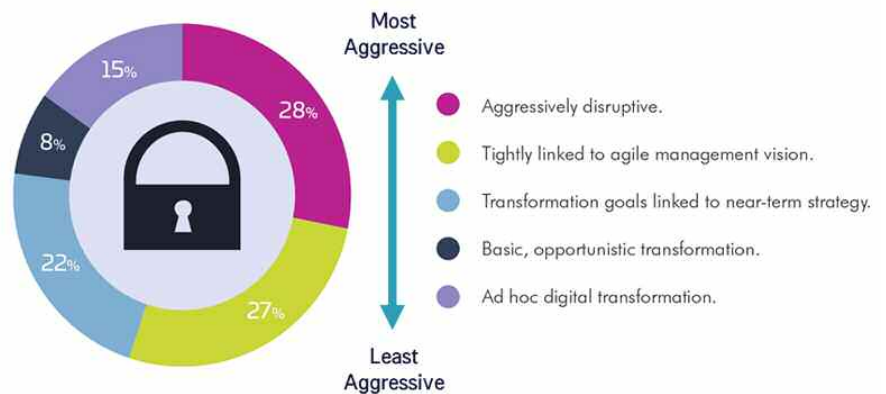
Digital transformation is essential for enterprises to serve customers better, improve operational efficiency and ultimately create key competitive advantages. However, digital transformation is also a significant vulnerability that can raise an enterprise's risk profile. The report shows that 97% of enterprises adopting digital transformation technologies use sensitive data within these new environments, but only 30% use encryption to protect data in these environments.

Leaving sensitive data unprotected in digital transformation environments such as cloud, big data, IoT, containers or mobile payments is a major threat to any enterprise. The 2019 Thales Data Threat Report also mentions that 60% of respondents said they have been breached at some time in the past, and 30% were breached in the last year!

However, digital transformation is creating a complex hybrid IT environment that is a major challenge for the protection of sensitive data. Existing platform-based security solutions cannot protect data as it flows throughout the enterprise, across multiple cloud-based and on-premises systems. Enterprises must focus on the protection of the sensitive data itself, wherever it goes. The adoption of pseudonimisation and anonymisation solutions, based on encryption and tokenisation technologies to protect an enterprise's most sensitive data, is a key component of any compliance programme to reduce an enterprise's risk.

Thales eSecurity has a proven track record of deploying advanced data security solutions and services that help enterprises comply with complex mandates such as PCI and legislation such as GDPR. Whether an enterprise is migrating to the cloud or

## Rates of data breaches by digital transformation stance



adopting containers, big data, IoT or any other transformative technology, Thales can help secure their most sensitive data and give them peace of mind to accelerate their digital transformation.

For more information on the 2019 Global Data Threat Report-Global Edition, please visit our website. And to see if your organisation is Fit for Compliance, click [here](#).

Thales eSecurity is a leader in advanced data security solutions and services, delivering trust wherever information is created, shared or stored. We ensure that company and government data is secure and trusted in any environment – on premise, in the cloud, in data centres and in big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices.

For more information, please visit [www.thalesecurity.com](http://www.thalesecurity.com)

**THALES**

# THALES

How will you secure  
your data in the cloud?

As you move to the cloud or have multiple  
cloud environments, you can rely on  
Thales to protect your sensitive data.

#CloudSecurity

[thalessecurity.com](https://thalessecurity.com)

# Threat actor – a love story

A closer look at the strange love-hate relationship we have with cyber-threat actors

**Andrew de Lange reports**

## The breach

It's 5am on a Saturday morning, you're soundly sleeping after a hectic week as CISO of a large organisation. Suddenly, the phone rings and wakes you up. The voice on the phone says one of the most dreaded phrases, "You need to get to the office right away – we've suffered a breach." As you drive to the office you run through multiple scenarios in your mind of how this has happened. In at least one of those scenarios, an Advanced Persistent Threat (APT) actor is responsible. You begin to think it *must* be a sophisticated APT, because your security controls are robust and you've taken every precaution. The board will want to know which APT is behind this. You get on the phone with your head of TI (Threat Intelligence) and instruct, "You need to find out who is behind this. Right now it's the only thing that matters."

## The love-hate relationship

When a cyber-incident strikes, we often romanticise the cause of the situation, even while we hate that it's happening. We can't help but love the idea that it was some APT (insert number here) or Fancy/Angry (insert animal here), or other famous threat actor with nation-state abilities. But something that we hate even more than being targeted is the realisation that our adversaries are not the ones we hear about in the news but rather someone we could have identified by doing our own internal research.

## The importance of research

In most cases, the actors that are targeting and eventually breach us are not the well researched APTs that we read about in security vendor reports and blog posts. The amount of research that goes into those publications is truly incredible and done by some of the most skilled cyber-threat analysts. We leverage the work done by these exceptional cybersecurity minds to have a view into the general threat landscape, usually by the industry, vertical, or geographic location we find ourselves in. But we need to apply these same techniques when we do analysis of our internal detections.

Our controls are constantly gathering signals for us, small pieces in the bigger puzzle we need to understand. Things like historical WHOIS records, SSL certificates, and more. These pieces of evidence are left behind by threat actors who are just as human and error-prone as we are. Every detection by our security controls tells a story, from the noisy big bad internet type of activity like perimeter scans and brute force attempts, all the way down to malware on

endpoints beaconing out of our networks. As an intelligence analyst these are the needles, in the stack of needles, we use to track our adversaries.

With a full-fledged threat intelligence programme, the CISO's post-breach conversation with his security team might go something like this:

- "Incident Response and Forensics team, do we know what happened?"
- "We've provided all the Indicators of Compromise (IOCs) to the TI team sir."
- "Which APT is behind this?"
- "Well sir, none. The actor behind this breach is a profile we have been tracking for a while. We created a profile for this actor when we first saw a phishing campaign eight months ago. Subsequently this actor targeted us with nine more campaigns and managed to drop keystroke logger malware onto a user's machine. The bad news is that the actor was successful in breaching us, the good news is, we know exactly who they are."

## The conclusion

Actor profiling and attribution are not always an exact science. Each security team can make this art more of a science by collecting IOCs, those, little pieces of the overall puzzle. Cyber-threat intelligence programmes are critical for gathering and analysing this evidence to determine who our real adversaries are. By practicing adversary profiling on internal detections we sharpen our skills as analysts, increase the level of known bad actors, and help prevent those frantic 5am phone calls.

Find out how cyber-threat intelligence is evolving, get the [SANS 2019 Cyber Threat Intelligence \(CTI\) Survey Results](#). □

**Andrew de Lange** is Solutions Consultant, EMEA at Anomali.

Anomali® detects adversaries and tells you who they are. Organisations rely on the Anomali Threat Platform to detect threats, understand adversaries, and respond effectively. The platform enables organisations to collaborate and share threat information among trusted communities, adopted by ISACs and leading enterprises worldwide.

For more information, please visit [www.anomali.com](http://www.anomali.com)

**ANOMALI®**

ANOMALI<sup>®</sup>



# Know Your Adversaries

Be Cybersecurity Enlightened

We help your organization become cybersecurity enlightened. With Anomali you can detect threats, understand adversaries, and respond effectively.

---

Learn more: [www.anomali.com](http://www.anomali.com)

---

# The business of information

The massive increase in cybercrime and fraud over the years has highlighted the challenges businesses face across all industries.

## Tim Ayling reports

The relentless march of technology innovation shows no sign of halting. Recent history points to a future of technology, with the continued proliferation of social media, Internet of Things, and artificial intelligence all threatening to change our landscape for good, and the winners in this new landscape will understand and prepare for the implications of this technology. The massive increase in cybercrime and fraud over the years has highlighted the challenges businesses face across all industries.

The rise of information technology in the early 1990s promised massive efficiency savings and competitive advantages that we had not seen before. In reality, organisations of all shapes and sizes invested heavily in technology and waited for the benefits.

Undoubtedly this investment did provide efficiencies that are rightly celebrated. Those that did not invest in technology often died, with widely quoted failures including Blockbuster not buying Netflix when they had the chance, and Toys“R”Us outsourcing their internet sales to Amazon – ensuring the consumer became used to purchasing toys online.

However, while efficiencies were created, competitive advantages often did not materialise. Why is that? Well, it's because organisations ignored the fact that information technology wasn't just about technology – in other words, they forgot the I in IT. In recent years we have seen the rise of the information age, where giants of the industry are information-based, rather than relying on technology. You're probably thinking of Google and Facebook as good examples of this, and you would be right. However, there are other examples that are not instantly recognised. Amazon house huge amounts of data on customer preferences; Uber know all about your movements; Airbnb know your favourite type of holiday and what you will typically spend.

Hence, people now see information as the new oil. Financial entities have also capitalised on this concept. Today online banking has become a norm, according to our [Consumer Security Risks Survey 2017](#), 76% of UAE residents regularly bank online. Consumers seem very happy to share personal information online for the convenience of being able to pay bills, transfer money and conduct other financial transactions online. This surge in online

**Companies with a strong cybersecurity strategy in place will be fit to defend themselves against any possible threats and in the end, the fittest will survive.**

transactions bring along many online dangers with it; new Kaspersky Lab research shows that banking Trojans are actively targeting online users of popular consumer brands, stealing credentials and other information through these sites. Kaspersky Lab technologies detected 9.2 million attempted attacks by the end of Q3 of 2018, compared to 11.2 million for the whole of 2017.

This abundance of data online is definitely not going to decrease, as Internet of Things is becoming the norm, with Gartner predicting 95% of manufactured goods will be connected to the internet by the end of 2020. Of course, security will not be part of the design for the majority of these goods as the rush to release new products tends to trump security. Compromising on cybersecurity will not only result in monetary losses, but can also damage brands reputation and affect consumer loyalty. Companies with a strong cybersecurity strategy in place will be fit to defend themselves against any possible threats and in the end, the fittest will survive. □

**Tim Ayling** is Global Head of Fraud Prevention Solutions at Kaspersky Lab.

Kaspersky Lab is a global cybersecurity company that celebrated its 20-year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe.

For more information, please visit [me-en.kaspersky.com](http://me-en.kaspersky.com)

**KASPERSKY** Lab



## What is great authentication?



### Legitimate User

It might be quite annoying for a legitimate user to receive an SMS with a code every time he is trying to access his digital account.



### Second Factor Authentication

- SMS
- E-mail
- Call



### Digital Account

For a business, adding second factor authentication would make user experience onerous and would create a risk of losing clientele.



### Basic Second Factor Authentication Process

- Disrupts the session
- Takes more time
- Second factor can be stolen

Nevertheless, a balance between secure authentication process and seamless customer experience is key to making both parties content with the service.

## Risk Based Authentication

Usual location, time, device etc.

Successful login

Unusual activity and behavior like a new device or unknown location

Successful login

Atypical behavior of a user signaling a high risk score

Login denied

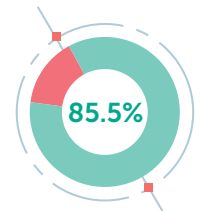
User gets benefits

- Seamless interaction with the service
- Faster transactions and purchases
- Higher level of data protection

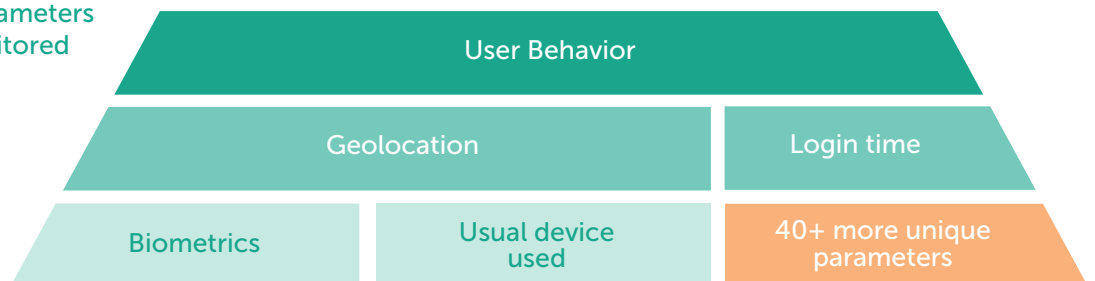
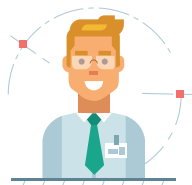
- True machine learning
- Forensic capabilities
- Reduced operational costs

Business gets more efficient

85.5% of users get to their accounts without additional verification. According to **Kaspersky Fraud Prevention** statistics.



Numerous unique parameters are continuously monitored in real-time by RBA



### Kaspersky Advanced Authentication

- Fast and seamless access to the personal account
- Preferable and handy authentication methods
- Confidence in safety of the services used.

Order your demo by contacting us at [kfp@kaspersky.com](mailto:kfp@kaspersky.com)



**Kaspersky<sup>®</sup>**  
**Fraud Prevention**

# Architecting a multi-tiered control strategy

We need to have a more profound/clear/strong view on the security solutions we need to avoid business disruption.

## SABSA reports

Information security departments are spending increasing amounts, and contributing more resources to standards compliance & security controls, and yet there's no guarantee on being safe and secure. So, the FUD being out there remains. The Fear is real supported by stories told, true or not. Uncertainty is a given for nothing really is ever certain enough. Doubt...? Although I dislike the marketing phrase "it's not a matter of if you are hacked, but when" to scare our stakeholders, I have to admit this just is the case. Nowadays with all our online services, in cloud stored data, BYOD and what more, it is just a matter of when will it hit your organisation. So we have to ask ourselves is the organisation protected and compliant where it should be?

The purpose of security is of course to avoid business disruption and ensure there is a robust, fit-for-purpose, business enabling and end-to-end solution. Being compliant is not the main goal and should not be the first priority. Also, because most of the standards are considered best-practise and not tailored to the organisation and incomplete. In the standards, we find a variety of controls to be implemented, some standards have a big overlap, others may focus a bit more in specific areas.

Yet just becoming compliant to one such standard, more or all, may still leave gaps in the solutions we provide to the stakeholders. We need to have a more profound/clear/strong view on the security solutions we need to avoid business disruption.

We can achieve this by using an architected approach towards the necessary controls. The SABSA Multi-Tiered Control strategy, is about following an engineering's approach when conducting risk assessments.

Engineers use their knowledge of science, mathematics, logic, economics, and appropriate experience or tactic knowledge to find suitable solutions to a problem. In information security, this is no different. We use our knowledge of logic, economics, politics, appropriate experience, business strategy and existing solutions to find and build the suitable security solutions to the security problems to support and enable the business.

Using our extensive security knowledge, best practice, years of experience and such when

**This defence-in-depth approach avoids concentrating only on limited best practices by looking with a more holistic approach for selecting capabilities to avoid business disruption.**

conducting risk assessments, we should be able to identify all the elements of the risks in their contexts, and determine what type of controls would fit best and where. It is at this point where we can also look at the necessary compliance requirements to match and select the appropriate controls in a proportional manner. And integrate with existing solutions inside the organisation.

An engineered approach, and applying structured thinking through the SABSA Multi-Tiered Control Strategy ensures information security contributes in a risk-proportional manner to the business. This defence-in-depth approach avoids concentrating only on limited best practices by looking with a more holistic approach for selecting capabilities to avoid business disruption. □

SABSA, the world's leading free-use and open-source security architecture development, management method and framework is changing the enterprise architecture landscape. With SABSA Chartered Security Architects in over 50 countries around the world, SABSA is transforming information security, risk management, and even compliance & audit, into 'Centres of Business Enablement'.

For more information, please visit [www.sabsacourses.com](http://www.sabsacourses.com)

**SABSA**  
COURSES.COM

# SABSA

COURSES.COM

@SABSAcourses

## Accredited SABSA Training & Business-Driven Enterprise Security Advice:

- **Articulate Security Value**
- **Traceably Meet Stakeholder Needs**
- **End-To-End & Through-Life Architecture**
- **Enable Holistic & Integrated Approach**
- **Business-Driven GRC & Policy Framework**

[sabsacourses.com](https://sabsacourses.com)

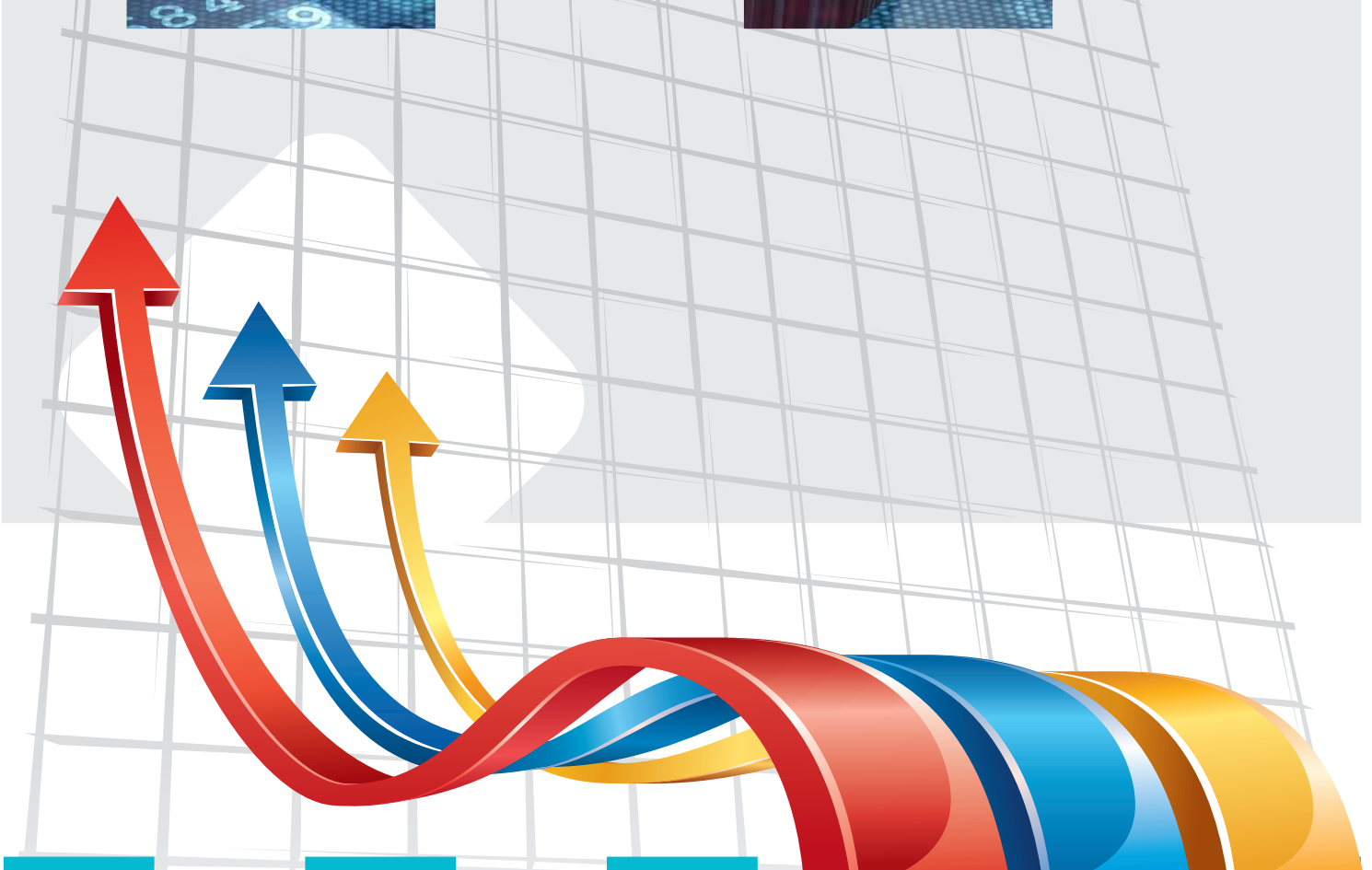
[training@sabsacourses.com](mailto:training@sabsacourses.com)

David Lynas Consulting Ltd, 17 Ensign House, Admirals Way, Canary Wharf, London E14 9XQ United Kingdom | +44 207 863 7834



NETWORK  
SECURITY  
VIRTUALIZATION

tnct



Check Point  
SOFTWARE TECHNOLOGIES LTD.

tufin



vmware™



Microsoft

# Network and security solutions

Enabling your IT Infrastructure.

**A**bout TNCT  
As an IT service-provider organisation, TNCT was established with the focus on offering professional IT services in order to address the market requirements in the Middle East and Africa regions for true value-added IT services including: educational services, technical implementation and project management services, consultancy services, as well as pre-sales and post sales technical support services.

Being a high-tech service-oriented organisation and given our skills and expertise in the network security domain we aim to deliver such value-added services with the best quality yet in the most efficient way. Our present focus is to provide these value-added services for technologies and solutions from Check Point Software Technologies within GCC and Africa regions.

## About Check Point

Check Point Software Technologies Ltd., the worldwide leader in securing the internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Over the past 19 years, Check Point's brand-name has always been linked to being a leader in IT security domain and its solutions are sold to enterprises, service providers, small- and medium-sized businesses and consumers all around the globe. 100% of Fortune 100 companies, 98% of Fortune 500 companies, 100% of Global 100 companies, and 98% of Global 500 companies are using Check Point solutions to protect their businesses.

However, due to complexities involved in implementing its solutions, professional value-added services such as training, consultancy, implementation, and technical support are heavily demanded for projects involving Check Point solutions.

## Check Point technical support models

Check Point Software Technologies generally offers direct and collaborative enterprise support models to its customers. As per direct support model customers directly contact Check Point international TAC centres for their support requests whereas the collaborative support model is facilitated through Check Point CCSP partners who in addition provide further value-added services and localised service

level agreements to meet local business needs. Furthermore, in collaborative support models, customers can only raise their technical support queries through their local CCSP service providers.

Customers usually prefer to use the collaborative support model because of service provider's local availability as well as the possibility of receiving service level agreements customised for local business needs. A local CCSP service provider can potentially provide a pool of various other value-added services such as project management, installation and configuration, consultancy, assessment, managed security services and etc. Within the GCC and Africa regions, Check Point does not provide direct enterprise support models covering localised SLA or on-site technical assistance.

## Why TNCT ?

- **Focused Check Point partner**  
As a focused Check Point Support, Training, and Sales partner, TNCT provides unmatched high-quality value-added services at pre-sales and post-sales levels aimed to not only enable the customers to acquire the best fitting network security solutions for their business needs, efficiently and effectively deploy the acquired Check Point technologies, or receive the high-quality technical support round the clock, but also, to best utilise their investment following the industry best practices.
- **Expert technical team**  
Our most valuable professional Check Point technical experts not only are fully trained and certified on the wide spectrum of Check Point technologies, but also possess deep knowledge and understanding of network and security fundamentals such as TCP/IP, routing and switching, network infrastructure services, directory services, PKI, messaging and collaboration, multi-factor authentication, security event and log management and analysis, as well as virtualised environments.
- **Expert team on Check Point licensing**  
Given the complexity of Check Point licensing, overtime our sales and technical teams have developed a very good understanding of the nature of Check Point license and contract concepts. This has greatly helped our team to

## TNCT reports

As a customer-oriented organisation, not only does the TNCT family work very closely with its customers in providing solutions to their business needs combining products, services and knowledge, but also we build an understanding at each interaction.

both propose best advisory to our customers and to be able to resolve such issues at a considerably fast pace.

- ***Sophisticated LAB setup***

Equipped with state of the art test laboratories, our technical experts simulate customer environments and replicate the problems that customers face in real world scenarios in order to determine the cause and effectively provide resolutions. The team uses the same sophisticated LAB setup to deploy and test the latest Check Point technologies, patches and updates in order to proactively prepare for upcoming inquiries from our esteemed clients.

- ***Customer-centric and service-oriented***

As a customer-oriented organisation, not only does the TNCT family work very closely with its customers in providing solutions to their business needs combining products, services and knowledge, but also we build an understanding at each interaction. As a service-oriented organisation we use our existing IT operational processes to help identify and foster innovation within IT and create awareness across our IT service and process teams.

- ***Committed to SLA and providing excellent response times***

TNCT has a rich set of service level agreements and support models designed and pre-built to address customer needs along with the possibility to tailor customised SLAs according to customer needs. Given our well-defined Technical Support Procedures and Escalation Matrix, we always aim to best deliver our services according to set service level agreements in a timely fashion. Our technical team's excellent and efficient backend

communication channel with Check Point TAC and RnD plays a key role is enabling us to comply with the provisioned SLA and response times.

- ***Industry specific experience in GCC***

Ever since our establishment, we have served our clients who are from various industry verticals such as banking and insurance, airline, oil and gas, retail, service provider, government, education... As a result we have learned and experienced business environments of such verticals which has given us the capability to better understand our clients' business nature and their mission critical applications/services.

- ***Managed security services***

Our managed security services contracts are not bounded to any ticket counts and our qualified technical team aim to pro-actively conduct real-time monitoring of customer's Check Point products covered. This way, in most cases our monitoring team can proactively determine faults and security incidents and take the necessary corrective actions via our incident response mechanism in coordination with the customer team and in accordance with the set change-management policies. □

For more information, please visit  
[www.tnctrade.com](http://www.tnctrade.com)



# How much does credential stuffing cost your business?

Credential stuffing is a relatively new problem, and it's serious.

Credential stuffing is an attack in which bad actors test credentials that have been stolen from third parties en masse on a different login application. Because users reuse passwords across online services, 0.1%–2% of a stolen credential list will typically be valid on a target site, allowing the attacker to hijack the user's account. Attackers typically use automation to conduct credential stuffing at scale. Once attackers validate credentials on a login application, they take over the customer's account to commit fraud.

Eight years ago, there wasn't even a term for the practice of testing consumers' stolen credentials against multiple e-commerce sites to see if they'll enable account takeovers (ATOs) and other forms of fraud. Now, the US consumer banking industry alone faces nearly \$50 million per day in potential losses due to credential stuffing attacks, while online retail is experiencing losses of about \$6 billion per year. While these numbers are certainly disturbing, this hasn't occurred in a US vacuum. Many global readers are now asking themselves, 'What does this mean for my company?'

Our new Credential Stuffing Calculator can help answer that question. Our calculator was developed based on the results of our 2018 [Credential Spill Report](#). This report includes comprehensive statistics on the sources, targets, internal workings and, most

importantly for the calculator, financial consequences of credential stuffing. The calculator provides an estimate of the financial risk for any company doing business with customers via a website or mobile APIs, based on the following variables:

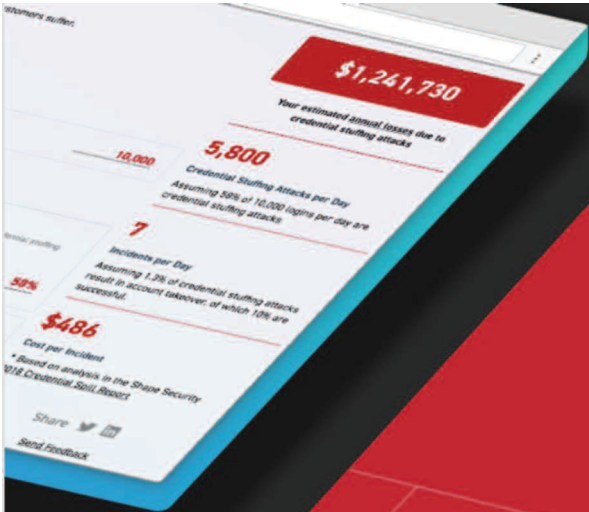
- Total daily login attempts
- Percentage of logins that are credential stuffing attacks
- Percentage of those attacks that result in an ATO
- Percentage of ATOs that result in financial loss
- Average dollar loss per ATO
- Other costs per ATO. These may include fees, consultants, investigations, financial penalties and negative impact on the brand.

## Automated for convenience

Obviously, most companies that aren't customers of Shape Security won't know what numbers to enter in the calculator's fields for variables 2 through 5. Even companies that have implemented IP blocks or other 'I am not a robot' technologies can't be sure about these numbers because today's most sophisticated (and most successful) attackers use technology that can easily defeat traditional security measures.

For this reason, our Credential Stuffing Calculator automatically fills in these variables for the four most frequently attacked industry sectors: consumer banking, retail (e-commerce), airlines and hotel

## Shape Security reports



The image shows a digital interface for the 'Credential Stuffing Calculator'. The main display shows a large red box with the text '\$1,241,730' and the subtitle 'Your estimated annual losses due to credential stuffing attacks'. Below this, several smaller boxes display intermediate metrics: '16,000' for 'Credential Stuffing Attacks per Day', '5,800' for 'Assuming 5% of 16,000 logins per day are credential stuffing attacks', '7' for 'Incidents per Day', and '\$486' for 'Cost per Incident'. A note at the bottom states '\*Based on analysis in the Shape Security 2018 Credential Spill Report'. The interface includes a 'Share' button and a 'Send Feedback' link. The Shape Security logo is visible in the bottom left corner of the interface.

# Credential Stuffing Calculator

Estimate the cost of attacks to your business

Shape protects over 1.4 billion online accounts from credential stuffing attacks. We find compromised credentials in real-time, identify botnets, and block simulation software.

chains, based on industry data we've gathered and analysed in the course of protecting literally billions of accounts. (Some users will probably be shocked at the percentage of logins in their industry that are both automated and hostile.)

In addition to the automatic fill-in feature, variables 2 through 5 can also be manually adjusted. This allows users to calculate upper and lower limits to the estimated risk, i.e. worst case and best case scenarios. This also enables users outside of the four target industries to enter values that seem appropriate.

Variable 6, Other costs per ATO, is a somewhat softer number, but these costs are often very high. For example, according to one study, a third of the companies that experienced a major data breach in 2016 lost 20% of their customers. Beyond damage to a brand's reputation, there are fines, notification costs and remediation costs for IT systems that also come into play.

#### Evaluating the result

The Credential Stuffing Calculator lets companies quantify their risk, based on statistical averages calculated from actual industry data, and gives them a ballpark number to help them decide how much they should consider spending to protect themselves (and their customers) against credential stuffing. The 2018 Credential Spill Report provides even more information to help companies understand the precise nature of the threat facing them.

Try the Credential Stuffing Calculator now.

#### About Shape Security

Shape Security is defining a new future in which excellent cybersecurity not only stops attackers, but also welcomes good users. Shape disrupts the economics of cybercrime, making it too expensive for attackers to commit online fraud, while enabling enterprises to more easily identify and transact with genuine customers on their websites and mobile apps. The world's leading organisations rely on Shape as their primary line of defence against attacks on their web and mobile applications, including three of the Top 5 US banks, five of the Top 10 global airlines, two of the Top 5 global hotels and two of the Top 5 US government agencies. The Shape platform, covered by 55 patents, was designed to stop the most dangerous application attacks enabled by cybercriminal fraud tools, including credential stuffing (account takeover), fake account creation, and unauthorised aggregation. Today, the Shape Network defends 1.7 billion user accounts from account takeover and protects 30% of all US savings. The company is headquartered in Mountain View, California, and also has offices in London and Sydney.

For more information, please visit [www.shapesecurity.com](http://www.shapesecurity.com)







**2 of the Top 10**  
Global Banks



**5 of the Top 10**  
Global Airlines



**2 of the Top 10**  
Global Retailers



**3 of the Top 5**  
Global Hotel Chains

# Security $\neq$ Friction

Shape protects your website from automated attacks and fraud while enabling a better user experience for real customers.



## The Decision Engine for Seamless Digital Business

Fighting fraud with digital identity  
intelligence from billions of transactions  
and a powerful decision platform.

### ThreatMetrix Digital Identity Network®

Harness the power of global shared intelligence from the largest network of its kind.



24b

annual network  
transactions



1.4b

unique online  
identities



4.5b

unique devices  
identified



.8b

unique email  
addresses



1.5b

mobile devices



185

countries served  
globally