Post event report

Strategic Sponsors

CRYPSYS secure computing

CYLANCE

DARKTRACE

42

NSFOCUS

paloalto NETWORKS

PHISHME

proofpoint

tenable network security

VERISIGN

WhiteHat SECURITY

Education Seminar Sponsors

CARBON BLACK ARM YOUR ENDPOINTS

esentire

Flowmon Driving Network Visibility

PCI-PAL Securing Payments

Networking Sponsors

WEBROOT

“ I really appreciated the diversity of themes presented at the e-Crime & Cyber Security event. It was dense although not too heavy, very topical and it is perfectly organised. ”
BNP Paribas

“ Thank you very much for organising the event, it was excellent, including the food and the intensity of the presentations. 20 minute presentations is perfect, without time to wander off. I also had several good conversations and I'm taking much more with me than I expected. The conference provided a broad range of perspectives on the main issues we are facing now, not only based on technology but also taking people into consideration. I found that contrasting those different approaches was thought provoking and inspiring and I'm taking away a number of ideas that I want to test asap. It is definitively worth attending! I enjoyed that the presenters were not only vendors but also practitioners from different industries, and that not even the vendors took a selling approach in their presentations. Thank you very much again for the invitation to attend this conference, I found it extremely valuable. ”
International Criminal Court

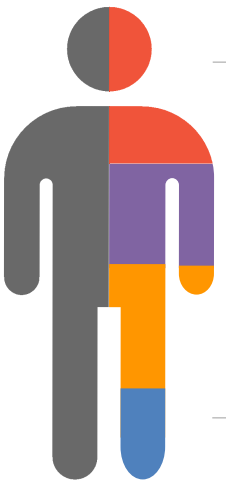
“ Thank you for the excellent congress yesterday, my compliments for the quality. I really appreciated the quality of the programme and the ability of the programme to cover so many diverse aspects. In addition, my compliments for the chairman who was able to manage it strict on time while at the same time providing useful additional insights and thoughts. ”
Philips

Inside this report:

Key themes

- The pros and cons of cloud solutions
- Keeping up with the regulators
- Cyber security and the financial services sector
- Securing employees with the right technology

Who attended?



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

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

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

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Lies Alderlieste, CISO, Nederlandse Spoorwegen

James Barham, Divisional Managing Director, PCI-PAL

Rogier Besemer, TIBER Project Lead, Dutch Central Bank

Adenike Cosgrove, Senior Product Marketing Manager, Proofpoint

Johan den Hartog, Sales Engineer Benelux & Nordics, Tenable

Plamen Dimitrov, Global IT Security Manager, Jacobs Douwe Egberts

James Dowell, Sales Engineer, Verisign

Mike Goldgof, Vice President Marketing, WhiteHat Security

Petra Haandrikman, Team Leader, Dutch National High Tech Crime Unit

Wim Hafkamp, CISO, Rabobank

Jim Hansen, COO, PhishMe

Jurre Horsels, CISO and Privacy Officer, Coöperatie VGZ

Ronald Kingma, CISSP, Access42

Daniel Kollberg, VP Northern and Eastern Europe, Palo Alto Networks

Ton Maas, Digital Coordinator, Dutch National High Tech Crime Unit

Richard Meeus, VP Technology EMEA, NSFOCUS

James Morgan, Cybersecurity Account Executive, eSentire

Vincent Ossewaarde, PCI-DSS QSA and CEO, Fortytwo Security

Tomas Sarocky, Area Manager Western Europe, Flowmon Networks

Simon Thornton, Director, Cyber Intelligence and Resilience at Euroclear

Hayley Turner, Cyber Security Account Executive, Darktrace

Jim Walter, Senior Research Scientist, Cylance

John D Wood, Cb Defense Regional Manager, Europe, Carbon Black

Agenda

08:00 Registration

08:50 Chairman's welcome

09:00 **Cyber resilience in the financial services**

Joint presentation between **Wim Hafkamp,** CISO, Rabobank and **Rogier Besemer,** TIBER Project Lead, Dutch Central Bank

- Introduction to the Dutch TIBER project (Threat Intelligence Based Ethical Red teaming)
- Goal of TIBER: To heighten the cyber resilience of the Dutch core financial institutions
- Case study on heightening cyber resilience through Red teaming: Rabobank

09:40 **Preventing cyber security breaches is possible**

Daniel Kollberg, VP Northern and Eastern Europe, Palo Alto Networks

- Detection and remediation is not enough, it's too late
- Manual response is time-consuming
- Handle known threats and deal with unknown threats

10:00 **Exploring the capabilities and economics of cybercrime**

Jim Walter, Senior Research Scientist, Cylance

- The current attacker community
- Tactics and capabilities being leveraged against targets across the globe
- The mechanics behind financial-based cybercrime and nation state espionage
- Some of the scary attacker capabilities we are seeing today
- Why we still aren't seeing the broad scale destructive attacks everyone has been predicting for years

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

Carbon Black	Flowmon
Decoding ransomware: How to reduce your risk of attack	**Is an attacker hidden in your network?**
John D Wood, Cb Defense Regional Manager, Europe, Carbon Black	**Tomas Sarocky,** Area Manager Western Europe, Flowmon Networks

11:00 Refreshments and networking break

11:30 **Secure third-party management**

Jurre Horsels, CISO and Privacy Officer, Coöperatie VGZ

- Capacity issues securing your IT environment
- The changing role and perspective of your organisation and managing third-party suppliers
- Solutions: Managing the difficulties along the way

11:50 **Phishing – technology alone can't solve this problem**

Jim Hansen, COO, PhishMe

- Phishing has been well established as the top entry method for hackers trying to access corporate networks. Yet, in spite of record spending on security technology, data breach reports continue to highlight the substantial lag between incident occurrence and detection
- That technology – those investments – are failing while organisations continue to neglect their last and best line of defence. Organisations need to make it harder for attackers by leveraging a resource they already have: their employees
- Employees hold the key to fortifying the last line of defence and providing IT and security teams with critical real-time attack intelligence

12.10 **The Enterprise Immune System: Using machine learning for next-generation cyber defence**

Hayley Turner, Cyber Security Account Executive, Darktrace

- How new machine learning and mathematics are automating advanced cyber defence
- Why 100% network visibility allows you to detect threats as they happen, or before they happen
- How smart prioritisation and visualisation of threats allows for better resource allocation and lower risk
- Real-world examples of unknown threats detected by 'immune system' technology

12.30 **2016 iDefense cyber threats and trends**

James Dowell, Sales Engineer, Verisign

Each year, enterprises around the globe dedicate increasing levels of time, budget and labour in identifying, preventing and mitigating online threats. The cat-and-mouse game of cyber security means that new trends emerge almost daily, requiring at-risk organisations in all industries to stay ahead of these new and evolving risks to revenue and reputation. Verisign iDefense® Security Intelligence Services has observed the following notable threats and trends:

- Cyber criminals migrating to the 'DarkNet'
- The rise of ransomware as a service
- An increase in the operational security of hacktivist operations
- Trends in distributed denial of service (DDoS) attacks against a widening field of victims across all industries.
- Critical vulnerabilities in prominent software applications have increased in potential for exploitation and level of impact in 2016, likely setting the stage for a new wave of breaches to make headlines

Agenda

12:50 **EXECUTIVE PANEL DISCUSSION** | **Cyber threats and threat intelligence**

Ton Maas, Digital Coordinator, Dutch National High Tech Crime Unit
Simon Thornton, Director, Cyber Intelligence and Resilience at Euroclear
Plamen Dimitrov, Global IT Security Manager, Jacobs Douwe Egberts
Richard Meeus, VP Technology EMEA, NSFOCUS

13:10 **Fighting the next generation of targeted BEC attacks**

Adenike Cosgrove, Senior Product Marketing Manager, Proofpoint

Business Email Compromise (BEC) attacks that impersonate executives and business partners to trick your employees are the biggest cyber threat to organisations today. This is not news. But what may surprise you is that the vast majority of BEC attacks are preventable. According to Gartner, Secure Email Gateways are struggling to address social engineering attacks with no payload. Well, things are changing. New technology can now surpass 'people' and 'process' initiatives to proactively protect your email channels while removing the guesswork for users. Learn about:

- The identity deception challenge – why spoofing works!
- Current BEC trends and attack methods
- Advances in technology to identify and block BEC attacks before they reach the inbox

13:30 Lunch and networking

14:30 **Driving digital: The changing landscape of cyber security in transport**

Lies Alderlieste, CISO, Nederlandse Spoorwegen

- Introduction to the transport cyber security landscape
- Transport companies are not the same as banks – or are they?
- Digital risk drivers in the trainworld

14:50 **Security testing in an agile world**

Johan den Hartog, Sales Engineer Benelux & Nordics, Tenable, co-speaking with **Ronald Kingma,** CISSP, Access42

- Integrating security into agile development processes
- Automating application performance and security testing
- Security and privacy by design

15:10 **Defeating cybercrime: The case for continuous security assessments**

Mike Goldgof, Vice President Marketing, WhiteHat Security

Research show that web application attacks are the number one source of data breaches, and the problem is growing. This session provides practical advice on protecting your web applications including:

- Assessing the threat landscape and measuring the risk to your business
- Vulnerability statistics compared by industry to benchmark your own organisation
- Building the business case for continuous security assessments

15:30 **Education Seminars | Session 2**

eSentire **Managing cyber security in a volatile world** **James Morgan,** Cybersecurity Account Executive, eSentire	PCI-PAL **Securing cardholder data for phone payments – challenges and solutions for merchants** **James Barham,** Divisional Managing Director, PCI-PAL

16:10 Refreshments and networking break

16:30 **Ransomware: The real threats**

Petra Haandrikman, Team Leader, Dutch National High Tech Crime Unit

- What you need to know from a law enforcement perspective
- The need for greater collaboration between public and private
- The complications of attribution
- What are the solutions?

16:50 **What would MacGyver do? Staying in control of security while working on your core business**

Vincent Ossewaarde, PCI-DSS QSA and CEO, Fortytwo Security

- Information security and CISO involvement for SME and large enterprises
- Ways to translate compliancy, strategic and tactical policies in operational activities
- Keeping the balance between core business and information security
- A practical, hands-on, unbiased approach to cyber security

17:10 **Security through times of change: How to manage cyber security strategy through business transformation**

Plamen Dimitrov, Global IT Security Manager, Jacobs Douwe Egberts

- Security best practices during company transformation
- How to maintain security during and after company acquisition or split
- Best practices and tips how to manage security during the time of company acquisition and merger

17:30 Conference close

Education Seminars	
Carbon Black **Decoding ransomware: How to reduce your risk of attack** **Presenter:** John D Wood, Cb Defense Regional Manager, Europe, Carbon Black	2016 has been 'the year of ransomware.' Numerous organisations have been forced to pay ransoms to regain access to critical files and systems. But ransomware attacks are not a new phenomenon; why are they booming now? Simply put, ransomware works. Everyone is dependent on the online world. That access makes all of us potential targets for ransomware. Attackers will target anything (and anyone) with access to data that can be monetised – no one is immune. What attendees will learn: • How combining new and existing technologies can provide for a new approach in raising the security posture of an organisation • What you can do today to minimise the ransomware risk to your organisation
eSentire **Managing cyber security in a volatile world** **Presenter:** James Morgan, Cybersecurity Account Executive, eSentire	What attendees will learn: • What is managed detection and response, and how can it defend your network from sophisticated cyber attacks? • Why technology is not the answer to cybersecurity: Combining people, process and technology • Going beyond the traditional cyber security approach on perimeter defences: Today's attacks are cleverly disguised, proving that even with an arsenal of layered technology, attacks can still perforate the perimeter • Discover next generation endpoint protection for today's advanced threats
Flowmon **Is an attacker hidden in your network?** **Presenter:** Tomas Sarocky, Area Manager Western Europe, Flowmon Networks	Today's security tools are focused on prevention and protection against threats and attacks. There are several tools on the market providing this solution. However, the modern approach should be very different. Detection and reaction on security breaches should be the main focus of secured networks. And the best way to detect an event is to monitor what is happening in the network. Do you really know what, who, where and how is doing? What attendees will learn: • Why your current cyber security tools are not enough • How to upscale your data security into the next level • What you can find out in network traffic monitoring • What are the possibilities in network monitoring • How network monitoring and diagnostics will improve your security
PCI-PAL **Securing cardholder data for phone payments – challenges and solutions for merchants** **Presenter:** James Barham, Divisional Managing Director, PCI-PAL	Securing cardholder data in a contact centre environment can be a far greater challenge than online/e-commerce. Contact centres are people heavy and typically involve a multitude of systems storing every aspect of data handled on a phone call, with sensitive data handled at every turn. This includes call recording devices, desktop CRM and commerce platforms, call tracking and reporting systems. So what is the best approach to securing this environment to PCI DSS, and why are so many major merchants doing this? What attendees will learn: • Why are customers using contact centres and what is the importance to merchants? • The size and scale of the challenge presented to merchants taking payments by phone • Methods by which merchants have historically protected cardholder data in the contact centre – is it enough? • What's in scope…have you thought of everything? • What is the impact of a breach and how to avoid it?