Post event report

PROTECTING DATA
e-Crime & cybersecurity
BENELUX
MANAGING RISK

The 7th e-Crime & Cybersecurity Europe Summit

6th December 2017 | Amsterdam

Principal Sponsor

IBM Resilient

Strategic Sponsors

DARKTRACE

➡42
Fortytwo Security

[I]
INTIGRITI
ETHICAL HACKER PLATFORM

PHISHME

Education Seminar Sponsors

BITSIGHT®
The Standard in SECURITY RATINGS

Carbon Black.

clearswift
RUAG Cyber Security

MICRO FOCUS®

Networking Sponsor

VERISIGN®

Key themes

The pros and cons of cloud solutions

Keeping up with the regulators

Cybersecurity 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

Stoffel Bos,
Corporate Information Security Officer
ProRail

Cosmin Broasca,
Information Security Officer
Rabobank

Ennio Di Rosa,
Business Development Manager
Darktrace

Jaap Halfweeg,
Chief Information Security Officer
SVB Sociale Verzekeringsbank

Carlo Hopstaken,
Group Information Security Office
UBS

Rob Huikeshoven,
Senior Sales Engineer, Benelux,
Southern & Eastern Europe and
South Africa
Carbon Black

Stijn Jans, Founder
intigriti

Simon Jenner,
Chief Information Security Officer
Booking.com

John Kennedy,
Global Head of Pre-Sales Engineering
Clearswift

Evert-Jan Korving,
Information Security Officer
ProRail

David Mount,
Cyber Security Expert
PhishMe

Vincent Ossewaarde, CEO
Fortytwo

Tycho Schmidt,
Regional Technical Sales
IBM Resilient

Bruce Schneier, CTO at **IBM Resilient**
and special advisor to **IBM Security**

Jean-Francois Simons,
Chief Information Security Officer,
Brussels Airlines

Boudewijn van Lith,
Identity, Access & Security
Sales Consultant
Micro Focus

Maarten Van Wieren PhD,
Managing Director Cyber Risk
Aon Netherlands

Dan Vasile,
Information Security Manager
VEON

James Warriner,
EMEA Channel Sales Manager
BitSight Technologies

Agenda

08:00	Breakfast networking and registration
09:00	Conference welcome

09:10 — **We are losing the war on cyber: What can we do differently and how can we win?**

Simon Jenner, Chief Information Security Officer, Booking.com
- Why are we losing?
- Can new technology change the game?
- How to deal with resource/talent scarcity
- What should be the focus/priorities and how do you set up for success?
- What can you do today and what are the non-negotiables?

09:30 — **The 2017 phishing threat landscape**

David Mount, Cyber Security Expert, PhishMe
- High-profile leaks and mature malware tools in phishing emails and how this has led to the resurgence and emergence of ransomware and botnet malware
- What is meant by the 'phishing threat landscape', how attackers have evolved this and the risks that poses to the enterprise
- What your enterprise can do in the face of all this, and goals for a holistic, comprehensive and agile defence

09:50 — **Managing cyber risk quantitatively – experience from the field**

Maarten Van Wieren PhD, Managing Director Cyber Risk, Aon Netherlands
- Short introduction into cyber risk quantification
- Practical applications of cyber risk management
- Lessons learned and challenges remaining

10:10 — **Agile security and orchestrated response**

Bruce Schneier, CTO at IBM Resilient and special advisor to IBM Security
- How organisations can thrive in an age of pervasive threats
- The evolution of security incident response and rise of automation and orchestration
- Orchestrating response in an uncertain world
- Aligning prevention, detection, and response

10:30 — **Education Seminars | Session 1**

Carbon Black	**IBM Resilient**
Speed stops breaches: Find out how to build a high-speed SOC	**How to respond to cyber incidents faster, smarter, better: An introduction to the Resilient Incident Response Platform**
Rob Huikeshoven, Senior Sales Engineer, Benelux, Southern & Eastern Europe and South Africa, Carbon Black	**Tycho Schmidt,** Regional Technical Sales, IBM Resilient

11:10	Networking and refreshments break

11:40 — **A security risk management paradigm shift**

Dan Vasile, Information Security Manager, VEON
- Security as an abstract concept
- Calculating and managing risks related to information security under the current paradigm
- How can we do a better job?
- Security for applications and managing the associated risks

12:00 — **The Enterprise Immune System: Using machine learning for next-generation cyber defence**

Ennio Di Rosa, Business Development Manager, 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

Agenda

12:20 — **Bug bounty programme, the next level of security testing**

Stijn Jans, Founder, intigriti; and **Jean-Francois Simons**, Chief Information Security Officer, Brussels Airlines
- Where does it fit in your security process?
- What to expect from your programme

12:40 — **Education Seminars | Session 2**

Carbon Black	Micro Focus
Speed stops breaches: Find out how to build a high-speed SOC **Rob Huikeshoven,** Senior Sales Engineer, Benelux, Southern & Eastern Europe and South Africa, Carbon Black	**Identity is the new security** **Boudewijn van Lith,** Identity, Access & Security Sales Consultant, Micro Focus

13:20 — Lunch and networking

14:20 — **Protect your mission-critical infrastructure in an open world**

Stoffel Bos, Corporate Information Security Officer; and **Evert-Jan Korving,** Information Security Officer, ProRail
- Your network should be closed, but it is mandatory to share information
- Your network should be closed, but for cost-saving purposes you have to allow remote control and maintenance
- You need to use new techniques, but the mandatory European standards are 15 years old

14:40 — **How did Jonah escape the GDPR?**

Vincent Ossewaarde, CEO, Fortytwo
- How PCI DSS is related to the GDPR and how you can demonstrate GDPR-compliance by doing PCI DSS.
- How GDPR relates to PCI DSS
- The lessons learned with PCI DSS will facilitate the way to GDPR
- Business knowledge and scope of regulations

15:00 — **Education Seminars | Session 3**

BitSight Technologies	Clearswift
Cybersecurity ratings: How external independent ratings are driving information security benchmarking and vendor risk management **James Warriner,** EMEA Channel Sales Manager, BitSight Technologies	**Threat approach from cybercriminals and how to tackle them** **John Kennedy,** Global Head of Pre-Sales Engineering, Clearswift

15:40 — Networking and refreshments break

16:00 — **The cyber payment fraud threat landscape**

Carlo Hopstaken, Group Information Security Office, UBS
- Provide an overview of the current threat actors in the payment landscape
- Their modus operandi to breach internal banking operations
- Which cyber defence measures are recommended to limit the risk of unauthorised payments being executed?

16:20 — **EXECUTIVE PANEL DISCUSSION** Information security regulation and its implementation

Cosmin Broasca, Information Security Officer, Rabobank

Jaap Halfweeg, Chief Information Security Officer, SVB Sociale Verzekeringsbank

Dan Vasile, Information Security Manager, VEON

16:50 — Closing remarks

17:00 — Conference close

Education Seminars

BitSight Technologies

Cybersecurity ratings: How external independent ratings are driving information security benchmarking and vendor risk management

James Warriner, EMEA Channel Sales Manager, BitSight Technologies

Cybersecurity ratings are transforming how organisations evaluate cyber risk and security performance by employing the outside-in model used by credit rating agencies.

These ratings are helping organisations answer questions on the prioritisation and effectiveness of their cybersecurity investments, making comparisons with their peers and gaining insight into the risks suppliers, 4th parties, subsidiaries and acquisitions are adding.

What attendees will learn:

- What is a cybersecurity rating?
- Why are external, independent and continuous ratings important?
- How are the ratings calculated?
- How are ratings used for benchmarking and vendor risk management?
- Use cases employing the BitSight cybersecurity ratings platform

Carbon Black

Speed stops breaches: Find out how to build a high-speed SOC

Rob Huikeshoven, Senior Sales Engineer, Benelux, Southern & Eastern Europe and South Africa, Carbon Black

For most organisations, cybersecurity resources and budgets are at a premium. Unfortunately, attackers have little empathy for your bottom line. Cybersecurity in today's environment requires a concerted focus on stopping an array of both malware and non-malware cyber attacks. Critical to your organisation's success is the ability to orchestrate, automate, and empower existing security resources to stay one step ahead of attackers and prevent emerging threats.

Attend this session to gain a unique insight into the challenges faced by today's security teams and how forward-looking organisations are constructing their next-generation security operations centres (SOCs).

What attendees will learn:

- How you can better focus your security investments
- Best practices for using integrated threat intelligence
- Effective endpoint security management to minimise the impact of any breach
- What it takes to become a high-speed SOC

Clearswift

Threat approach from cybercriminals and how to tackle them

John Kennedy, Global Head of Pre-Sales Engineering, Clearswift

Today's security platforms are relying on signature based or sandbox technologies to detect the ever changing ransomware threat. This approach is still fallible with 'virtual aware' threats and 'time based' threats going undetected. See how an award winning 'game changing' technology can protect organisations whilst allowing business communication.

Introducing adaptive redaction technology that meets business requirements from stopping security threats as well as visible and invisible data leaking from the organisation's network. This new technology bridges the gap between business requirements and IT requirements to secure the network.

What attendees will learn:

- How Clearswift can integrate with existing solutions to add adaptive redaction
- How adaptive redaction addresses real business issues from security to visible and invisible data leakage

Education Seminars

IBM Resilient

**How to respond to cybersecurity incidents faster, smarter, better:
An introduction to the Resilient Incident Response Platform**

Tycho Schmidt, Regional Technical Sales, IBM Resilient

The Resilient Incident Response Platform (IRP) empowers cybersecurity teams to orchestrate their incident response processes, and respond to and resolve incidents faster, more effectively, and more intelligently. The Resilient IRP is the leading platform for orchestrating and automating incident response processes.

This demonstration will showcase the Resilient IRP's ability to enable complete IR orchestration and automation – aligning security teams' people, process, and technologies into a single hub for incident response by understanding the capabilities of the solution.

What attendees will learn:

- Achieve greater intelligence and efficiency by integrating your existing security technologies, including SIEMs, EDR, threat intelligence, and more
- Adapt to real-time incident conditions with Resilient Dynamic Playbooks – ensuring a fast and complete response to all incident types
- Build, configure, and maintain your own IR action plans within hours or days

Micro Focus

Identity is the new security

Boudewijn van Lith, Identity, Access & Security Sales Consultant, Micro Focus

The days when perimeter security was enough to protect your business have long passed. It's time to figure out how to manage user identity in this increasingly complex world. We are all familiar with the multitude of businesses across the globe that have suffered massive data breaches, resulting in a loss of customer trust and operational chaos. Sixty-three per-cent of confirmed data breaches are a direct result of weak, default, or stolen credentials. Insider breaches are also a major culprit, most of which are unintentional. So what can you do? How can you prevent data breaches from compromising your organisation? To guard against the myriad of insider threats, come and learn about the critical components of pro-tection in this digital world: identity governance, access management, and privileged user management. Identity context is crucial to effective insider threat detection. You will also find answers to important questions such as 'What resources does an identity have access to?' 'Is this normal or expected based on the individual's role?' and 'What is the level of risk associated with a given identity?'

What attendees will learn:

- The role of identity in your security strategy
- Where to start: you don't need to eat the whole elephant at once
- How to prepare for and protect yourself against insider threats