Post event report

Strategic Sponsors

CROWDSTRIKE

DARKTRACE

hackerone

netwrix

proofpoint.

Pulse Secure

SentinelOne

Education Seminar Sponsors

bitglass

BITSIGHT The Standard in SECURITY RATINGS

COFENSE

cybereason

Cybersel

digital shadows_

Synack

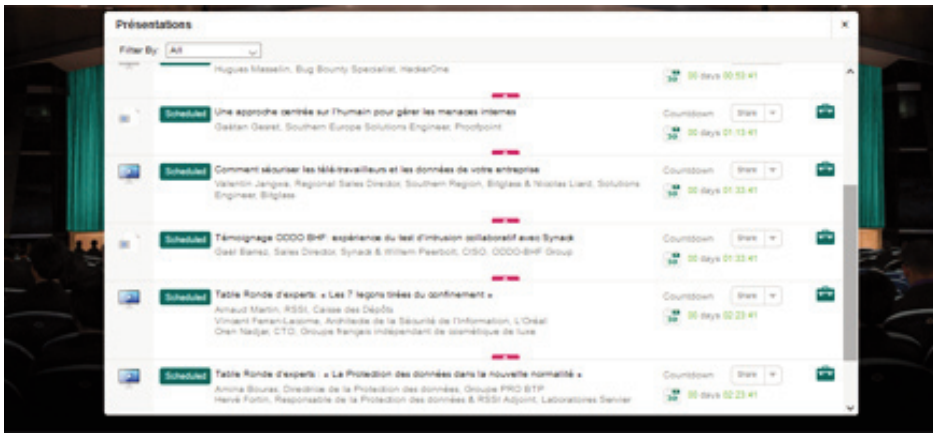
TERRANOVA SECURITY

tripwire

> “ Personally I found the event very interesting and the speakers of quality. The virtual format that you proposed turned out to be original and I think pioneer in the matter. Perhaps the future will be a mix between face-to-face and remote conferences each with its advantages. ”
>
> **Responsable Securite des Systemes d’information Groupe, Up Groupe**

Inside this report:

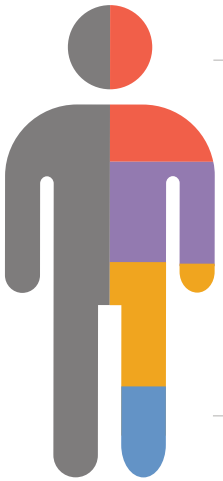
Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars



Key themes

- Securing and protecting remote employees
- Maintaining the human firewall
- Securing the customer — are your websites up to it?
- Rethinking identity and access management
- Performing critical security tasks remotely – how can CISOs regain control?
- Stuck in the cloud
- Protection versus business needs

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

Gaël Barrez, Sales Director, Synack

Mick Benatek, Business Development Manager – France, Cybersel

Amina Bouras, Chief Data Officer, PRO BTP Groupe

Yves Destrebecq, Fraud Prevention Manager, HSBC France

Vincent Ferran-Lacome, Information Security Architect, L'Oréal

Hervé Fortin, Data Protection Officer & Deputy CISO, Laboratoires Servier

Gaëtan Gesret, Southern Europe Solutions Engineer, Proofpoint

Ekbal Gharbi, Sales Engineer, Cofense

Valentin Jangwa, Regional Sales Director, Southern Region, Bitglass

Guilhem Labourel, Darktrace

Yvan Lanzada, Sales Engineer, Hermitage Solutions SARL on Behalf of Tripwire

Christophe Leautey, Regional Sales Director, BitSight

Nicolas Liard, Solutions Engineer, Bitglass

Thomas Limpens, Solution Engineer South-West-Europe, Netwrix

Arnaud Martin, CISO, Caisse des Dépôts

Hugues Masselin, Bug Bounty Specialist, HackerOne

Xavier Mell, Country Manager – France and French speaking Africa, Pulse Secure

Vincent Meysonnet, Senior Sales Engineer, Cybereason

Joel Mollo, Regional Director, South EMEA, CrowdStrike

Oren Nadjar, CTO, independent French luxury cosmetics group

Willem Peerbolt, CISO, ODDO-BHF Group

Tom Sams, Solutions Engineer, Digital Shadows

Federico Smith, Expert Consultant Cybercrime & Cybersecurity, Council of Europe

Andy Spencer, VP Sales Engineering, Cofense

Paul Steiner, Head of Compliance, La Francaise des Jeux

Jan Tietze, Director Security Strategy EMEA, SentinelOne

Theo Zafirakos, CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security

Agenda

08:00 Login and networking

08:55 Chairman's welcome

09:00 **In a digitalising world, you can't mention fraud without cybercrime**

Yves Destrebecq, Fraud Prevention Manager, HSBC France

- Main threats overview
- The relationship between cybersecurity and the fight against fraud
- Implementation of an efficient dispositive
- When technology could block the main threats: fraud monitoring, machine learning, biometrics

09:20 **The Threat hunting challenge: Detect, prevent, respond and hunt – every second, every day**

Jan Tietze, Director Security Strategy EMEA, SentinelOne

- Learn how Endpoint Detection & Response (EDR) technologies pick up where antivirus technologies leave off
- Understand why EDR should be an essential part in every Endpoint Security Strategy
- Learn how EDR auto-immunises the endpoints against newly discovered threats and provides rich forensic data, mitigates threats and performs network isolation
- Demo

09:40 **Offensive AI vs. Defensive AI: Battle of the algorithms**

Guilhem Labourel, Darktrace

Among rapidly evolving technological advancements, the emergence of AI-enhanced malware is making cyber-attacks exponentially more dangerous and harder to identify. In the near future, we will begin to see supercharged, AI-powered cyber-attacks leveraged at scale. To protect against offensive AI attacks, organisations are turning to defensive cyber AI, which can identify and neutralise emerging malicious activity, no matter when, or where, it strikes. In this session you will learn about:

- Paradigm shifts in the cyber landscape
- Advancements in offensive AI attack techniques
- The Immune System Approach to cybersecurity and defensive, autonomous response capabilities
- Real-world examples of emerging threats that were stopped with Cyber AI

10:00 **The economic cyberwar**

Federico Smith, Expert Consultant Cybercrime & Cybersecurity, Council of Europe

- Cyberwar and cybercrime: collateral damage for businesses
- The evolution of national and international law in response to the digitalisation of organised crime
- Organised crime 3.0's new methods of financialisation

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

Cybereason	Terranova Security
How to defend against the most sophisticated attackers: A MULTI-STAGE LIVE CYBER-ATTACK	**Putting your users first: How security awareness training can protect your remote workforce against increasing cyber-threats**
Vincent Meysonnet, Senior Sales Engineer, Cybereason	**Theo Zafirakos,** CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security

10:50 Networking break

11:20 **The standards of cyber-risk**

Paul Steiner, Head of Compliance, La Francaise des Jeux

- Standards and benchmarking of cyber-risk
- The relationship between cybersecurity and governance
- Cyber-risk management: how to protect the digital assets of your users

11:40 **Increasing work-from-home capacity beyond the pandemic: how to manage the security concerns**

Xavier Mell, Country Manager – France and French speaking Africa, Pulse Secure

- Despite the security concerns resulting from the recent increase in work-from-home initiatives, one-third of companies have observed productivity gains during remote work and a staggering 84% anticipate broader and more permanent WFH adoption beyond the pandemic
- This presentation will offer an in-depth perspective on WFH challenges, concerns, strategies and anticipated outcomes
- Find out the results of the 2020 Remote Work-From-Home Cybersecurity Report and learn how Pulse Secure helps companies improve secure access for remote workers

11:50 **Fighting hackers from your couch: 5 things you should know!**

Joel Mollo, Regional Director, South EMEA, CrowdStrike

- COVID-19 has reshaped our lives as we know it, how has the current global situation changed the hackers' business models?
- How has COVID-19 altered the cyber-issues that corporate leaders need to be thinking about?
- How should cybersecurity teams address cyber-attacks in this new operating environment?

Agenda

12:10 Education Seminars | Session 2

BitSight

How BitSight takes into account the the new cyber-risks induced by work from home?

Mick Benatek, Business Development Manager – France, Cybersel & **Christophe Leautey,** Regional Sales Director, BitSight

Cofense

Engaging end users in phishing defence – are your teams combat ready?

Andy Spencer, VP Sales Engineering, Cofense & **Ekbal Gharbi,** Sales Engineer, Cofense

12:40 Education Seminars | Session 3

Digital Shadows

Digital risk protection and remote working: detect threats before they strike!

Tom Sams, Solutions Engineer, Digital Shadows

Tripwire

COVID-19, remote working and e-commerce: how are companies adapting to the evolving cybersecurity challenges?

Yvan Lanzada, Sales Engineer, Hermitage Solutions SARL on Behalf of Tripwire

13:10 Lunch and networking break

14:10 EXECUTIVE PANEL DISCUSSION | Protecting data in the new normal

For the majority of companies, digital transformation has been a gradual process over the past decade – until now. With organisations being forced to pivot to digital-first ways of working, and interacting with customers, what are the implications for data governance and protection? How do we keep the business operating and prospering in this new digital world, without sacrificing on privacy or security? A discussion with:
Amina Bouras, Chief Data Officer, PRO BTP Groupe
Hervé Fortin, Data Protection Officer & Deputy CISO, Laboratoires Servier

14:30 5 things you need to know to future-proof your data security today

Thomas Limpens, Solution Engineer South-West-Europe, Netwrix

- Are you prepared for the threats your organisation will face in the coming year?
- How will you protect your sensitive and business-critical data from malicious insiders, ransomware and other attacks, and errors by overburdened IT administrators?
- Discover 5 things that can help you orchestrate IT security with your data at its core, putting you one step ahead of all these threats and helping you build an intelligent roadmap for protecting your business

14:50 Debunking #6 main myths of the Bug Bounty Program

Hugues Masselin, Bug Bounty Specialist, HackerOne
We will cover the following 'myths':

- Bug Bounty Programs are necessarily public
- Bug Bounty Programs are necessarily annual & continuous
- The only way to work with hackers is to pay them
- The Bug Bounty Program does not encourage cooperation between developers and hackers
- The Bug Bounty Program will blow my budget
- The Bug Bounty Program will encourage hackers to hack me

15:10 A people-centric approach to managing insider threats

Gaëtan Gesret, Southern Europe Solutions Engineer, Proofpoint

- Anyone with legitimate, trusted access to an organisation's systems and data can become an insider threat. So how can companies better manage this?
- How full visibility provides the necessary context to understanding and reducing insider threats without compromising user privacy and compliance
- The different types of insider threats, and what steps you can take to build your own insider threat management programme
- The acceleration of incident response: how to detect and immediately analyse unusual activity

15:30 Education Seminars | Session 4

Bitglass

How to secure your company's remote workers and data access

Valentin Jangwa, Regional Sales Director, Southern Region, Bitglass & **Nicolas Liard,** Solutions Engineer, Bitglass

Synack

Customer testimony: ODDO-BHF: Collaborative penetration testing with Synack

Gaël Barrez, Sales Director, Synack & **Willem Peerbolt**, CISO, ODDO-BHF Group

16:00 Networking break

16:20 EXECUTIVE PANEL DISCUSSION | 7 lessons from lockdown

COVID-19 has been a gamechanger for how businesses operate. It's required standard operating procedures to be thrown out and replaced with almost entirely new ways of working – and most organisations failed to anticipate a situation quite like this in their disaster recovery / business continuity planning. As we emerge from the initial crisis, what lessons have we learnt for maintaining BAU – securely! – while dealing with the unexpected? Featuring insights from:
Arnaud Martin, CISO, Caisse des Dépôts, **Vincent Ferran-Lacome,** Information Security Architect, L'Oréal,
Oren Nadjar, CTO, independent French luxury cosmetics group

17:00 Closing remarks | **17:10** Networking | **17:30** Conference close

Education Seminars

Bitglass

How to secure remote workers and data at access of your company

Valentin Jangwa, Regional Sales Director, Southern Region, Bitglass &
Nicolas Liard, Solutions Engineer, Bitglass

The world has just observed a surge in remote workers in an era where remote work was already fast approaching. In the long term, we will observe a complex environment that sees an expansion of devices, geographic points of access and access to data outside of traditional boundaries.

Join this webinar to learn how to:

- Enable the short-term surge in remote workers while preparing for a future 'normal'
- How to secure your data, applications, and web interactions from advanced threats
- Secure BYOD devices while enabling productivity
- Identify new access patterns and differentiate between malicious and benign behaviours

BitSight

How BitSight takes into account the the new cyber-risks induced by work from home?

Mick Benatek, Business Development Manager – France, Cybersel &
Christophe Leautey, Regional Sales Director, BitSight

To understand some of the new risks created by the deployment of teleworking, Bitsight:

- Provides visibility into infections and vulnerabilities occurring on home networks
- Analyses the new attack surface through assets, providers, and exposed services, including the IP of remote-working users
- Enables the identification and monitoring of the most critical third parties through continuous monitoring and configurable alerts based on criticality criteria

Cofense

Engaging end users in phishing defence – are your teams combat ready?

Andy Spencer, VP Sales Engineering, Cofense &
Ian Wallace, Sales Engineer DACH, Cofense

As the world locked down to mitigate the risks of COVID-19, many employees are still adjusting to working from home, and companies like yours are working hard to support it. However, organisations cannot completely lock down their networks. For example, phishing emails continue to evade Secure Email Gateways, with threat actors adapting their tactics to exploit the ongoing crisis. Businesses are threatened by a surge of phish related to COVID-19 and remote work. Listen in as Cofense security experts Andy Spencer and Ian Walllace provide an in-depth review of the current phishing threat landscape, as seen through the inboxes and eyes of those on the front line – your end users, the new face of your front-line phishing defence.

Highlights will include:

- Insights of various phishing campaigns that evaded SEGs and reached enterprise end users, delivering credential phish and malware
- How threat actors are using trusted services, such as online business surveys and document sharing platforms, to evade SEGs
- Expert predictions of what we will continue to see through the end of Q2 and the remainder of 2020

Cybereason

How to defend against the most sophisticated attackers: A MULTI-STAGE LIVE CYBER-ATTACK

Vincent Meysonnet, Senior Sales Engineer, Cybereason

Get inside the brains of the most sophisticated attackers and see how world-class defenders are using their skills and tools in the most efficient and smartest way. This session is delivered by Cybereason's world class security engineers who are responsible for protecting some of the world's largest organisations and have broken the news and found the solutions for some of the biggest recent cybersecurity attacks.

In this session you will witness:

- The attacker's infiltration and see the malicious operation as it moves across the entire environment
- How many opportunities an attacker has to advance the operation
- How many opportunities the defender has to destroy the attack before it reaches its target

Education Seminars

Digital Shadows

Digital risk protection and remote working: detect threats before they strike!

Tom Sams, Solutions Engineer, Digital Shadows

Today, obtaining a comprehensive view and understanding of the threats that are specific to your organisation can represent a huge challenge. For the past few years remote working has been steadily getting more and more popular, but the recent crisis has pushed numerous organisations to speed up their business transformation and cybersecurity programmes and create new strategies and processes as they go.

In this session, Digital Shadows will show you:

- Real-life examples and scenarios of unwanted risks and digital exposure
- why and how bespoke intelligence and data loss prevention technologies and are critical in today's remote worker landscape
- How the detection of such threats across the open, deep and dark web helps organisations to reduce and remediate those risks

Synack

Customer testimony: ODDO-BHF: collaborative penetration testing with Synack

Gaël Barrez, Sales Director, Synack & **Willem Peerbolt,** CISO, ODDO-BHF Group

This session will present a CISO return of experience. Willem Peerbolte, Group CISO at ODDO-BHF will share why he chose to setup a partnership with Synack instead of continuing with legacy pen testing. He will then present the outcomes for the bank, his clients, and for him. You will learn:

- Why ODDO-BHF shifted from classic pen testing to crowdsourced
- How Synack's remote security testing platform is helping to augment ODDO-BHF's internal teams
- What results and benefits the company is getting

Terranova Security

Putting your users first: how security awareness training can protect your remote workforce against increasing cyber-threats

Theo Zafirakos, CISO Coach and Professional Services, Security Awareness Speaker Terranova Security

Cybersecurity risks increase when companies adopt work from home practices with little time to prepare and inform their users of the associated risks. While some employees may have worked from home in the past, for many users, this is a new work environment, especially under the current circumstances. Cybercriminals know that many people are adapting to a new normal, in confinement, which makes it easy to fool users with emails, calls and text messages. Cyber-attackers are leveraging the fear and uncertainty created by this event to trick unwary users. In this session, learn why it's so important to maintain cybersecurity awareness training and how to mitigate these COVID-19 related cyber-risks and more specifically:

- What are the cybersecurity risks associated with the human factor when employees work remotely?
- How can users defend themselves and the organisation where they work against the increase in cyber-attacks?
- By adopting a people-centric approach: how can cybersecurity awareness create a first line of defence?

Tripwire

COVID-19, remote working and e-commerce: how are companies adapting to the evolving cybersecurity challenges?

Yvan Lanzada, Sales Engineer, Hermitage Solutions SARL on Behalf of Tripwire

Security teams are at the forefront of protecting the distributed enterprise. Cybersecurity must be integrated into COVID-driven business responses such as the shift to working from home, migratijng to e-commerce, and massively scaling delivery logistics. To learn more about how security professionals are dealing with the rapidly evolving environment, Tripwire has conducted some detailed research and we'd like to share some of the fascinating results in this session. Including:

- Emerging trends across regions, company size and job levels on how COVID-19 has impacted companies
- What are companies' biggest security concerns?
- What steps are being taken to reduce the impact of COVID-19 on their organisation's cybersecurity defences
- What technologies are available to assist with maintaining security in the new working environment