Post event report

Strategic Sponsors

CEQUENCE SECURITY

COFENSE

Cybersel

CYCOGNITO

DARKTRACE

imperva

KnowBe4 Human error. Conquered.

PRISMA BY PALO ALTO NETWORKS

Education Seminar Sponsors

BeyondTrust

illumio

CISCO KENNA Security

ManageEngine

OPSWAT.

virtru

Networking Sponsors

aqua

corelight

zscaler

"First of all I wanted to thank you for this event, which I was attending for the first time and which I greatly appreciated. The diversity of case studies, associated with the presentation of innovative solutions in terms of IS protection, as well as the availability of suppliers to obtain more information on their products and to arrange appointments later, save precious time. The testimonies and sharing of experiences were very informative. All this orchestrated by a rigorous and very pleasant organisation. Being able to discuss with our peers, being able to consult the documentation at our own pace, sometimes with videos demonstrating the tools and presentations where we can ask these questions, is very instructive. Finally, the virtual environment we offered us was pleasant and easy to navigate. Bravo for this organisation and the quality of this event."

Group CISO & DPO, Flowbird

"Thank you for this great event, and a special mention for the welcoming team, who did a fantastic job. They were all very approachable and available. Thank you again for your efforts and the impeccable organisation of this event – best wishes for the future, and see you soon for another of the global e-Crime events."

International Marketing – Data Management, ManageEngine

"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."

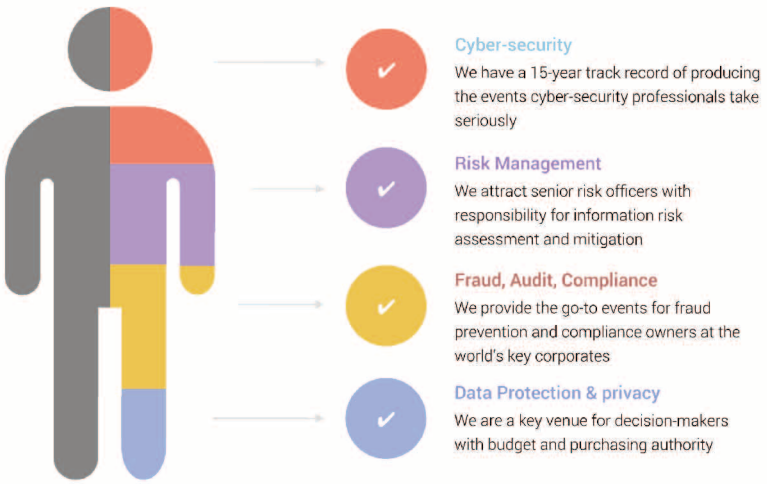
Responsable Securite des Systemes d'information Groupe, Up Groupe

Inside this report:

Key themes

- Too little time for implementation?
- Securing the citizen
- Can zero trust be done?
- Are criminals winning the ransomware war?
- Moving to Cloud Native?
- Re-engineering the SOC: from logs to automated XDR
- Securing digital currencies
- Building-in security: from DevOps to SecDevOps?
- Building better Cloud governance
- From smart machines to smart cities - securing the IoT
- Cybersecurity for business resilience
- Closing the cybersecurity skills gap

Who attended?



Speakers

Xavier Aghina, CISO, W-Ha

Karthik Ananda Rao, Chief Evangelist, ManageEngine

Bertrand Blond, Director of Cyberdefense Information Systems, Commandement de la Cyberdéfense

Yves Destrebecq, Responsable prévention contre la fraude, HSBC

Nicolas Drémont, Senior Sales Engineer, Imperva

Mouad El Kathabi, Cybersecurity Analyst, Cybersel

Carole Fromont, Country infosec Manager, Bank of America

Nicolas Imbach, Inside Sales Representative, Cofense

Jean-Paul Joanany, CISO, Action Logement

Jason Kent, Hacker in Residence, Cequence Security

Cedric Lochouarn, Prisma Cloud Sales Specialist, Palo Alto Networks

Nicolas Malbec, Head of Cyber Planning Office, Commandement de la Cyberdéfense

Sabine Marcellin, Partner, Level Up Legal

Mario Massard, Senior Systems Engineer, Illumio

Rachid Mekdoud, Sales Engineer, OPSWAT

Renaud Perrier, SVP, International, Virtru

Valentin Pourrinet, Cybersecurity Account Manager, Darktrace

Stephen Roostan, VP, EMEA, Kenna Security

Sara Sellos, Defense Sector Coordinator, ANSSI

Florence Sergent, Head of Cyber Security Project, Arval-BNP Paribas Group

Younes Tahar-Chaouch, Senior Solutions Engineer, BeyondTrust

Rehan Tinnin, CISO, BNP Paribas Wealth Management

Jelle Wieringa, Security Awareness Advocate, EMEA, KnowBe4

Agenda	
08:00	Registration & networking
08:50	Chairman's welcome
09:00	**Working with the supply chain**
	Bertrand Blond, Director of Cyberdefense Information Systems, Commandement de la Cyberdéfense • Introduction and synthetic presentation of the COMCYBER missions • Subcontracting chain, observation and transition • MINARM/SUPPLY CHAIN convention: genesis, objectives, work and achievements • Conclusion
09:20	**APIs: A key enabler of digital transformation and a security blind spot that needs protection**
	Nicolas Drémont, Senior Sales Engineer, Imperva • Understanding the challenges, risks and best practices for API Security • Building a unified approach towards Web and API Security • The 4 pillars of API protection
09:40	**The psychology behind social engineering**
	Jelle Wieringa, Security Awareness Advocate, EMEA, KnowBe4 • Ransomware attacks are becoming ever more commonplace, we'll illustrate the tricks cybercriminals use to fool you • Understand how cybercriminals leverage the power of your own mind to make you do their bidding, psychology plays a vital role in social engineering • We'll demonstrate how the way humans are programmed to operate is the root cause of the problem
10:00	**The implications of Cyberscore**
	Sabine Marcellin, Partner, Level Up Legal • What is the current Cyberscore proposal? • Who needs to do what and when? • An action plan for CISOs
10:20	**Education Seminars | Session 1**
	BeyondTrust **How do you protect IoT infrastructures from cyber-attacks?** **Younes Tahar-Chaouch,** Senior Solutions Engineer, BeyondTrust **Illumio** **Ransomware containment** **Mario Massard,** Senior Systems Engineer, Illumio
11:00	Networking break
11:30	**Fight against fraud: How to guard against fraudsters who are constantly optimising their attacks**
	Yves Destrebecq, Responsable prévention contre la fraude, HSBC • Overview of the main threats • Relationship between the fight against fraud and cybersecurity • How to implement an effective prevention system? • The contribution of technology in the fight against the main threats
11:50	**AI responds to surgically sophisticated cyber-attacks**
	Valentin Pourrinet, Cybersecurity Account Manager, Darktrace • Discover how advances in AI have enabled surgical, autonomous response capability – where humans can no longer react fast enough • Rapidly evolving cyber-attacks can strike at any time, and human security teams are no longer able to fight machine-speed attacks alone • Join Darktrace to learn how Autonomous Response takes targeted action to stop attacks in progress, without disrupting your business. It also includes examples of real-world threats, case studies and attack scenarios.
12:10	**Do you know what information your APIs are leaking?**
	Jason Kent, Hacker in Residence, Cequence Security Attend this session to fully understand the API security risks your organisation faces. Topics include: • Security risks associated with the increased use of health monitoring APIs, API specifications, and GraphQL • Compliance and governance risks related to APIs that may inadvertently expose sensitive data • Why APIs used to facilitate account login/registration and inventory lookups are more susceptible to automated attacks

Agenda

12:30 — Cybersel & CyCognito, how to defend your external attack surface, even during military conflict

Mouad El Kathabi, Cybersecurity Analyst, Cybersel

- Do you currently know your attack surface risk mean time to resolution (MTTR)?
- What tools do you use to continuously discover and test all your exposed assets across all environments?
- What methods do you use to prioritise the remediation of attack surface security issues to reduce risk exposure?
- Why is it important to continuously monitor your attack surface, especially during the rapidly changing world we are living in?
- How do you measure risk MTTR performance?

12:50 — Education Seminars | Session 2

Kenna Security	OPSWAT
Transforming vulnerability management: Benefits of the modern approach **Stephen Roostan,** VP, EMEA, Kenna Security	**File upload protection: A critical gap in web app security** **Rachid Mekdoud,** Sales Engineer, OPSWAT

13:30 — Lunch & networking

14:30 — EXECUTIVE PANEL DISCUSSION — Women in cybersecurity

Sara Sellos, Defense Sector Coordinator, ANSSI; **Florence Sergent,** Head of Cyber Security Project, Arval-BNP Paribas Group; **Carole Fromont,** Country infosec Manager, Bank of America

- Why diversity matters: the value of perspectives
- Getting better at education, recruitment and training
- How to advance women in cybersecurity today

14:50 — Supply chain security – accelerate your cloud journey with Palo Alto Networks

Cedric Lochouarn, Prisma Cloud Sales Specialist, Palo Alto Networks

Cloud has become the new normal. Supply chain security is not a new problem but its importance has significantly risen over the last 2 years. We will present Palo Alto Networks' approach to mitigate this risk and key tips for successful operationalisation.

- Cloud supply chain threat landscape: Insights from Unit 42
- How apps are built in the cloud & devops era
- Prevent from code to cloud thanks to Prisma Cloud CNAPP (Cloud Native Application Protection Platform)

15:10 — Implementing an adaptive email security architecture with Cofense

Nicolas Imbach, Inside Sales Representative, Cofense

- What is an adaptive security architecture and what are the objectives – With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation. We'll walk you through the benefits and objectives of implementing an adaptive security architecture and risk framework
- The current situation in email and phishing security – We'll share some of the latest insights from the industry and what we're seeing through our unique combination of artificial, human, and high-fidelity intelligence
- Implementing adaptive security architecture and risk framework with Cofense – We'll talk through how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity

15:30 — Education Seminars | Session 3

ManageEngine	Virtru
Cybersecurity threats to the digital transformation of businesses **Karthik Ananda Rao,** Chief Evangelist, ManageEngine	**How to fight cyber-threats with a zero trust data-centric approach** **Renaud Perrier,** SVP, International, Virtru

16:10 — Networking & refreshments

16:30 — EXECUTIVE PANEL DISCUSSION — The changing role of the CISO

Jean-Paul Joanany, CISO, Action Logement; **Rehan Tinnin,** CISO, BNP Paribas Wealth Management; **Xavier Aghina,** CISO, W-Ha

- How the evolution of the threatscape and security technology affected the role of the CISO in the last five years
- What are the most important skills and qualities that CISOs will need to possess over the next five years?
- How must the organisation and staffing of cybersecurity teams change? (bigger, smaller, skillsets, diversity?)

17:00 — Cybersecurity: the human dimension, awareness and training future cyber-combatants

Nicolas Malbec, Head of Cyber Planning Office, Commandement de la Cyberdéfense

- Transition on the shortage of talent, not only for supply chain security but also on several other subjects
- Types of jobs we need
- Recruitment, training and evolution of the cyber-combatant

17:30 — Chairman's closing remarks

17:35 — Congress close

Education Seminars	
BeyondTrust **How do you protect IoT infrastructures from cyber-attacks?** **Younes Tahar-Chaouch,** Senior Solutions Engineer, BeyondTrust	It's impossible to protect what can't be seen. Unfortunately, lack of visibility into Industrial Control Systems (ICS) is common in industries around the world, both from a remote access and vulnerability management perspective. IoT infrastructures do not always have modern cybersecurity protection. In this session, we will discuss together: • Home office – why is your IoT environment at risk? • Why is IoT vulnerability management different from IT and what to do about it? • How to manage privileged remote access and vulnerabilities while remaining productive and secure • Zero Trust Architecture and more!
Illumio **Ransomware containment** **Mario Massard,** Senior Systems Engineer, Illumio	As the working world has changed, with it has come the proliferation of devices along with moves into hybrid and cloud environments. This has created challenges for the organisation to withstand any stresses, and threats to its cyber-resources within the organisation and its ecosystem. It is increasingly important than ever for businesses to be able to prevent the spread of any breach that might occur and improve responses to them when they do. During this session we will outline how to: • Find out how to stop the spread of ransomware. • Identify potential weaknesses in your infrastructure • Improve your response to real attacks • Build a more resilient defence against future threats
Kenna Security **Transforming vulnerability management: Benefits of the modern approach** **Stephen Roostan,** VP, EMEA, Kenna Security	• Speed up security operations – leveraging 22+ real-world threat & exploit feeds, machine learning, and predictive analytics to prioritise the greatest risks based on likelihood of exploit (top 2–3%) and not CVSS, speeds up manual security investigations and risk analysis • Secure faster & easier – real-time 'next best fix' and remediation intelligence, with ticketing integration, allows IT teams to know what to patch & when, saving time & resources • Reduce resources needed – automated workflows lower organisational barriers that take up time & resources, streamlining operations provides improved SLAs and response capabilities • Utilise existing investments – agnostically aggregate all vulnerability data including network and applications scanners, pen-test data and CMDB. De-duplicate, normalise & prioritise these outputs into Kenna's simple 1–1000 risk score, for utilisation and ROI on existing investments • Collaborate & communicate – a single-platform where all stakeholders from security, IT & senior management can easily understand, quantify and act on risk • Visualise & report – create dashboards with risk meters to easily visualise risk across your attack-surface & full reporting metrics to effectively control risk
ManageEngine **Cybersecurity threats to the digital transformation of businesses** **Mr A Karthik,** Chief Evangelist, ManageEngine	Cybersecurity threats have become a common occurrence these days. With digital transformation taking over every aspect of business, IT administrators are working 24/7 to keep attacks and hackers at bay. Round-the-clock monitoring on all aspects of business security is needed to provide a safe and secure environment for both internal and external users. • Learn the top 10 security threats in the world of digital transformation • Know how to mitigate them with easy to use on-premise and on-cloud solutions • Insights on Cloud gaining momentum these days in the period of lock down across the globe

Education Seminars	
OPSWAT **File upload protection: A critical gap in web app security** **Rachid Mekdoud,** Sales Engineer, OPSWAT	Digital transformation is a must for today's organisations, resulting in a migration from paper-based to digital documents. Millions of documents are now being shared among collaborators weekly and monthly – uploaded to either a web portal, customer portal (insurance or mortgage applications) or support portal (attaching files to your support ticket). At the same time, an enormous amount of effort is invested into building high-availability, fault-tolerant systems and securing them. However, file upload remains a major attack vector and far too often is not covered by traditional web application defences. In this seminar, Rachid Mekdoud, Sales Engineer at OPSWAT will cover three types of risks to web applications and how to apply a Zero Trust model to both users and the files they upload and the devices from which these uploaded files originate. Risks from: • Threat actors who submit malicious files to gain access to the organisation's IT infrastructure • User who submits sensitive data in violation of an application's terms of service • Inadvertent hosting and distributing malicious files uploaded by a threat actor
Virtru **How to fight cyber-threats with a Zero Trust data centric approach** **Renaud Perrier,** SVP, International, Virtru	The digital world is now perimeter-less and the practice of cybersecurity is rapidly shifting from centralised, to decentralised policy controls. Up until now, Zero Trust security initiatives have focused primarily on identities, devices, networks, and apps. But what about data? Data is everyone's most valuable resource and what every attacker is after. It's constantly on the move being downloaded, shared, copied, and modified. You can't afford to lock it down, and you can't afford to lose control of it. Join Virtru as we discuss: • The importance of Zero Trust Data Access (ZTDA) • The benefits of adding policy controls that are capable of following data regardless of where it goes or how it is used • How you can rethink your cybersecurity stack with data at the core to protect your organisation's most important asset and prepare yourself to manage future cyber-threats