

QUBIT CONFERENCE

# PRAGUE | 22

MAY 25 - 26

## PROGRAM GUIDE



# SPEAKING BUREAU

Every year, Qubit Speaking Bureau handles the most important part – to find and put together an impressive list of speakers and topics.



**JOSEPH CARSON**

Chief Security Scientist  
and Advisory CISO

**Delinea**  
Estonia



**ETAY MAOR**

Senior Director  
Security Strategy

**Cato Networks**  
USA



**BORIS MUTINA**

Senior Security Analyst

**Excello**  
Slovakia



**MAREK ZEMAN**

CISO

**Tatra Banka**  
Slovakia



**Marek Zeman**  
Chief Information Security Officer  
Tatra banka



**Jozef Úroda**  
ICT and Security Risk Manager  
Tatra banka

## HOW TO IMPLEMENT RISK MANAGEMENT IN AN ORGANIZATION

The goal of the workshop is to show practical ways how to implement security risk management in your organization. We will present the importance of ICT risk management in terms of organizational management and the best utilization of resources in the organization. We will use practical simulations in which we define and test the entire risk management life cycle. We will learn how to set up risk management processes so that the information security and business area would be interconnected, and at the same time understandable for the top management in the organization.

## KEY TAKEAWAYS

- Introducing risk management as an essential process for managing an organization
- Demonstration of practical implementation of risk management in the organization (in accordance with EBA/GL/2019/04)
- ICT Security risk as part of the overall risk profile
- Setting KPIs in risk management with reference to risk appetite and risk tolerance
- The way of reporting and escalation at different levels of the organization
- Practically approached asset inventory as an essential part of ICT risk management
- Risk management, which is understood by both the IT administrator and the board member

## PRE-REQUISITES

- *No need to bring anything, just attend.*

### FORMAT

In - person

### DURATION

8 hours total

### NUMBER OF ATTENDEES

Up to 20 attendees

## TARGET AUDIENCE

CISO (Chief Information Security officer), CSO (Chief Security Officer), ICT Risk manager, Security officer, role responsible for defining the security policy, role responsible for methodical security management, information security consultants



**Joseph Carson**  
Chief Security Scientist (CSS)  
& Advisory CISO  
Delinea, Estonia

## INTRODUCTION TO HACKING GAMIFICATION

### LEARNING HACKER TECHNIQUES

Staying up to date and learning hacking techniques is one of the best ways to know how to defend your organization from cyber-attacks. Hacking gamification is on the rise to help keep security professionals up to date on the latest exploits and vulnerabilities. This workshop is about helping you get started with hacking gamification to strengthen your security team whether it is about understanding hacker techniques, pentesting or incident response.

- In this workshop, you'll learn strategies and resources ethical hackers use at each stage of an ethical hack:

### KEY TAKEAWAYS

- How to perform system and service enumeration on endpoints
- Discover vulnerabilities and modify exploit payloads to obtain initial access
- Perform Reverse Shells
- Basic Knowledge on how to use BurpSuite
- Create Payloads
- Privilege Escalation Techniques

### PRE-REQUISITES

- *Your own Laptop that can run kali Linux*

You can download Kali Linux from here, the best option is to choose a Virtual Machine either VMWare or VirtualBox.

<https://www.kali.org/get-kali/>

You can download VirtualBox from here

<https://www.virtualbox.org/>

Familiar with Linux however the trainer will help walk through each of the steps so only basic Linux knowledge is sufficient.

### FORMAT

In - person

### DURATION

5 hours total

### NUMBER OF ATTENDEES

Up to 20 attendees

### TARGET AUDIENCE

IT Security Professionals, IT operations, Incident Response Teams, Beginner Pentesters, Systems Administrators, Infrastructure Management, Workstation Management, Professionals looking to move into security roles

Event Moderator: Joseph Carson

Event Moderator: Boris Mutina



### Registration

#### CONFERENCE OPENING

*Maria Krahulecova, CEO, Qubit Security*

#### OPENING KEYNOTE

*Rastislav Janota, Director, National Cyber Security Centre (SK-CERT) at National Security Authority, Slovakia*

#### OPENING KEYNOTE

*Karel Rehka, Director, National Cyber and Information Security Agency, Czech Republic*

#### OPENING KEYNOTE

*Ondrej Krehel, Chief Scientist & Fellow, Cyber Risk & Resilience Services, LIFARS a SecurityScorecard Company, USA*

#### KEYNOTE

#### Stop Chasing, Start Defending: Preventing Ransomware with Zero Trust

An increasing number of MSPs have reported being victims of ransomware attacks. Cybercriminals are exploiting MSP products and services, including remote monitoring and management (RMM) tools. These tools are often accessed through software vulnerabilities or brute force attacks. Is your MSP prepared to protect against ransomware? Join Ben Jenkins, ThreatLocker Senior Solutions Engineer as we discuss what you can do to prevent cybercriminals from carrying out an attack.

*Ben Jenkins, Senior Solutions Engineer, ThreatLocker, UK*

#### CASE STUDY

#### The First 48 Hours

The first 48 hours after a cyber incident are the most critical time for an organization that has been the victim of a cyber crime. Who? What? Where? How? Why? These are questions every business that has been a victim of a cyber crime want answers to as fast as possible. This presentation will go through the steps that need to be taken to stabilize the victim's environment, preserve the potential evidence, deal with the threat actors, and mitigate the situation.

*Larry Slusser, Sr. Director of Professional Services  
Leonard Neagu, Managed Defense Manager  
LIFARS, a SecurityScorecard company*

#### COFFEE BREAK

#### OPENING KEYNOTE

#### A New Approach: Redefining Security Validation in Today's World of Endless Threats

If you take a look back, the security industry focused on manual penetration testing and traditional vulnerability scanning to evaluate an organization's cyber risk and overall security resilience. This is just no longer something that is sustainable with how organizations operate in the digital world. Attacks have become so sophisticated that security teams are realizing that traditional approaches are no longer setting up teams for success and that compliance-focused approaches aren't indicating the true readiness of an organization against ransomware and other advanced threats, thus seeing a need for automated security validation to testing the integrity of all cybersecurity layers.

*Shak Ahmed, UK, Ireland and CEE Pre Sales Team Lead*

#### Data Security: From "Need To Know" to "Need To Share"

Organizations are moving from a risk-averse approach of data sharing to data-sharing-first approach. We will discuss the causes for this change, and whether this change is good for security and data teams. Finally, we'll discuss data security platforms and best practices for data democratization.

*Ben Herzberg, Chief Scientist, Satori, Israel*

#### Anatomy of Supply Chain Attack (Detection and Response)

Vendor of a Helpdesk system was breached and attacker managed to embed a malicious code into the product source code base. Next product build was released with a backdoor implanted and deployed by the customer base.

*Pavel Minarik, Vice President, Technology, Progress Software, Czech Republic*

*The program guide is subject to change.  
Some of the sessions are solely virtual.*

## EXECUTIVE TRACK

## TECHNICAL TRACK

Event Moderator: Joseph Carson

Event Moderator: Boris Mutina

12:15 - 13:00

### Improving Risk Management with Cybersecurity Testing

Secure development lifecycle includes different activities for achieving a secure product or solution, but unexperienced development teams can easily get lost. We will discuss the advantages of a centralized approach to cybersecurity testing and share best practices on setting it up.

**Terézia Mézešová, Cybersecurity Team Leader, Siemens Healthineers, Slovakia**

### How ML is Used to Find Command and Control Channels?

When lights go out in IT systems of the critical infrastructure in a city thanks to ransomware attack, how can machine learning with its models and underline math help to detect attacker?

**Gregory Cardiet, VP Security Engineering, International, Vectra, USA**

13:00 - 14:00

LUNCH

14:00 - 14:35

### Connecting Development and Cyber Security with DevSecOps

**Daniel Joksch, CEE Solution Design Leader, EMEA Solution Design Security Services, IBM, Czech Republic**

14:35 - 15:20

### Flying Low - a Look at Some Sophisticated and Stealthy Attacks in the Region

"It is no surprise that in last few years we are witnessing a number of attacks that are slowly becoming more sophisticated and stealthy.

While there will always be opportunistic attackers that are simply going for the low hanging fruit (and they will always be the majority), we started observing dedicated attackers who want to remain as stealth as possible.

At the same time, once such attackers become active, the damage they create can be overwhelming.

This presentation will show technical details about several incidents that Bojan and his team worked on. Specifically, we'll take a look at a very novel attack against the SWIFT connected systems that was identified in a bank, and a devastating attack against a cryptocurrency exchange.

What's interesting about both of these cases is that attackers invested a significant amount of time into understanding their target's business processes, before they actually launched the attacks."

**Bojan Zrdnja, Chief Technical Officer, INFIGO IS, Croatia**

### Demystifying Supply Chain Intrusions

Supply chain intrusions represent one of the most concerning but also most hyped intrusion vectors for cyber impact scenarios. This presentation will focus on the methodology behind supply chain intrusions, examining critical attacker decision-points for successful execution, while also identifying opportunities for defenders and asset owners to detect, deter, or defeat such efforts. To illustrate these concepts, we will explore several examples to varying degrees of detail, ranging from the NotPetya destructive event to the Nobelium-linked SolarWinds campaign to more recent items in Ukraine and in ransomware operations. You will learn a more nuanced and complete understanding of supply chain intrusion methodologies and how to usefully counter such attacks.

**Joseph Slowik, Threat Intelligence and Detections Engineering Lead, Gigamon, USA**

15:20 - 15:35

COFFEE BREAK

15:35 - 16:20

### Cybercrime Offender Prevention: Understanding Cybercriminal Career Pathways: to Deter, Divert, Degrade or Disrupt

Cybercriminal Career Pathways, youth cybercrime and interventions utilised by Law Enforcement to reduce entry and engagement in all levels of Cybercrime. Interpretation of Digital Responsibility and necessity for Private Sector engagement alongside academic findings on the efficacy of initiatives.

**Gregory Francis BEM JP, Consultant, 4D Cyber Security Ltd, UK**

### Anatomy of the CodeCov Breach

In this session, Andy Thompson will dissect and analyze the recent supply chain attack on the DevOps tool CodeCov. He'll break down what happened, how it happened, and most importantly cover how cybersecurity best practices can prevent such attacks in the future.

**Andy Thompson, Threat Researcher, CyberArk Security Labs, USA**

**EXECUTIVE TRACK**

**TECHNICAL TRACK**

Event Moderator: Joseph Carson

Event Moderator: Boris Mutina

16:20 - 17:05

**[Re-]Enabling Women in Technology:  
Lessons from the Past  
for an Inclusive Future**

Computing and cyber are male-dominated fields. Yet software development started out as exclusively women's work. Learn about how industry changes caused women to leave the field, especially in post-Communist nations, and how to tap into women workers' potential to combat the talent shortage.

**Beatrice Zhang, Threat Detection Engineer, Datadog, France**

**From Zero to Full Domain Admin:  
The Real-World Story of a  
Ransomware Attack**

Following in the footsteps of a cyber-criminal and uncovering their digital footprint. This is a journey inside the mind of an ethical hacker's response to a ransomware incident that brought a business to a full stop, and discovering the evidence left behind to uncover their attack path and the techniques used. Malicious attackers look for the cheapest, fastest, stealthiest way to achieve their goals. Windows endpoints provide many opportunities to gain entry to IT environments and access sensitive information. This session will show you the attacker's techniques used and how they went from zero to full domain admin compromise that resulted in a nasty CryLock ransomware incident.

**Joseph Carson, Chief Security Scientist (CSS) & Advisory CISO, Delinea, Estonia**

17:05 - 17:40

**CLOSING KEYNOTE  
Bring Me to a True A  
The Power of Cyber Rating**

Cyber risk management is key for any organization in the world. Identifying cybersecurity risks internally is not enough anymore; cyber experts need to look at the cybersecurity hygiene of their 3rd parties. SecurityScorecard helps you to size and prioritize the risk as it appears to act on the weakest link and remediate efficiently. During this keynote you will be able to understand how to report to all stakeholders inside and outside your organization in a pragmatic manner.

**Yves Mimeran, International Channel Director at SecurityScorecard, France**

## EXECUTIVE TRACK

## TECHNICAL TRACK

Event Moderator: Joseph Carson

Event Moderator: Boris Mutina

<p>9:00 - 9:30</p> <p>◆</p>	<p><b>Zero Trust: Separate the Wheat from the Chaff</b></p> <p>A new hype called Zero Trust is about, or is it? Correctly implemented, the Zero Trust provides a rock-solid security foundation for your business. In this talk, I will explain Zero Trust for executives, what pitfalls to avoid, and how to spot vendors misusing the ZT term to their advantage.</p> <p><b>Vladimir Jirasek, Founder &amp; CEO Foresight Cyber, Foresight Cyber C14, Czech Republic</b></p>	<p><b>Practical Defense Evasion</b></p> <p>Malicious actors today have to overcome considerable barriers against cyber attacks. Learn the various techniques these bad guys use to successfully execute their code, eliminate anti-malware solutions, bypass network restrictions, escalate privileges, or make it difficult for internal security teams to detect and respond.</p> <p><b>Jan Marek, Co-founder   Ethical Hacker   Forensic Investigator, Cyber Rangers, Czech Republic</b></p>
<p>25min + panel discussion</p> <p>9:30 - 10:00</p> <p>◆</p>	<p><b>Cyber security Talent Crisis: Today and Tomorrow</b></p> <p>The cyber security talent shortage is no longer a security problem but a global crisis as all of us are under attack. Insufficient staffing, funding and understanding of this problem will make this worse in the next years.</p> <p><b>Codrut Andrei, Application Security Manager, Romania</b></p>	<p><b>Cameras, CASs &amp; Clocks: Enterprise IoT Security sucks - A Story of Two Million Interrogated Devices</b></p> <p>Working globally with Fortune 500 enterprises and government agencies we've interrogated over two million production IoT devices. The presentation is based on the analysis of over two million Enterprise Internet of Things (IoT) devices. It outlines security challenges and risk mitigation techniques.</p> <p><b>Brian Contos, Chief Security Officer, Phosphorus Cybersecurity, USA</b></p>
<p>10:00 - 10:30</p> <p>◆</p>	<p><b>PANEL DISCUSSION</b></p> <p><b>Cybersec Talent Crisis</b></p> <p><b>Moderator: Joseph Carson</b></p> <p><b>Panelists: Marek Zeman, Beatrice Zhang</b></p>	
<p>10:30 - 10:45</p> <p>□</p>	<p>COFFEE BREAK</p>	
<p>10:45 - 11:30</p> <p>◆</p>	<p><b>Philosophizing the Security in the Apps World</b></p> <p>Try to apply philosophy methods to the Mobile apps security subject domain. The best approach to combat biases and go to the core is philosophizing the subject. I propose to look closer at the security and its perception by users of mobile Apps.</p> <p><b>Sergiy Yakymchuk, CEO, Talsec, Czech Republic</b></p>	<p><b>"Dumb and Dumber"</b></p> <p>In the age of sophisticated attacks of the 21st century, is there any room left for those who prefer brawns over brains? The answer will shock you... not. Look into important cases of past and current malware which went the destructive way.</p> <p><b>Peter Kosinar, Technical Fellow, Eset, Slovakia</b></p>
<p>11:30 - 12:15</p> <p>◆</p>	<p><b>Why Do Companies Need Tabletop Exercises?</b></p> <p>Tabletop exercises offer companies an opportunity to try to work together as a team in times of crises and see what could be improved and which parts of the crises the company is managing well. We will show the most common mistakes that companies are making in exercises and during the major breaches. Who will be making the decision in your company whether to pay or not to pay the ransom and based on which information decision will be made.</p> <p><b>Zuzana Duračinská, Offensive Security Department Team Lead, LIFARS, a SecurityScorecard company, USA</b></p>	<p><b>Cryptocurrency Crime, Investigation and Crime Prevention</b></p> <p>Over the last few years we observed a significant increase in cryptocurrency adoption. Quite understandably, the growth attracts legitimate users as well as criminals. During this session we will discuss several examples of cryptocurrency crimes, how law enforcement agencies and the private sector fight these and what should users do to keep their funds safe.</p> <p><b>Jarek Jakubček, Director of Investigations, Binance, Netherlands</b></p>
<p>12:15 - 13:15</p> <p>□</p>	<p>LUNCH</p>	

The program guide is subject to change.  
Some of the sessions are solely virtual.



Event Moderator: Joseph Carson

Event Moderator: Boris Mutina

13:15 - 13:25

**Introduction of Project LOCARD**

**Zoriana Dmytryshyna, Director of Institutional Relations, APWG, EU**

13:25 - 14:10

**Engaging your Board and Senior Leadership**

Sharing experience as someone who has engaged all levels within large & mid-size companies, Rays presented to governments, ministers, and board directors. Discussing lessons learned with examples of what will be asked from Board Directors & Senior Leaders at this level & how to avoid Bear Traps.

**Ray Stanton, Global Executive Partner, Strategy, Risk & Compliance, IBM, UK**

**The Growing Problem of Leaked Credentials - How Adversaries Find and Use Secrets to Break into Our Systems**

Secrets like API keys are sprawling through the internet at an alarming rate. In 2021 a research project uncovered 6 million leaked secrets publicly. This presentation reviews that research and uses recent breaches to show how adversaries discover and exploit secrets to breach organizations.

**Mackenzie Jackson, Security Advocate / Head of DevRel, GitGuardian, France**

14:10 - 14:55

**The Social Dilemma**

I will be discussing how social media causes issues for people and companies. This discussion looks at the research we have done into interest groups, propaganda, and unethical practices that social media utilizes to produce fake narratives that trap people, attack teenagers, and force them to be hyper sexually active as well as create an environment of aggression.

**Michael Goedeker, CEO and Founder Hakdefnet International, Germany**

**Traps and Gaps of EoT (Email Zero Trust)**

Emailing world applies the EoT best practices and standards for decades. Which are the key technologies, their efficacy compared to MITRE ATT&CK TnT's, and practical impacts on the balance between security and deliverability?

**Boris Mutina, Senior Security Analyst, Exello/Virusfree, Czech Republic**

14:55 - 15:25

**CLOSING KEYNOTE  
Cyber Threat Observations**

Cyber threats increase in volume and sophistication each year, even taking advantage of the COVID-19 pandemic. See how the FBI views these threats and works to increase awareness to mitigate them.

**Paul Vitchock, Assistant Legal Attaché, Federal Bureau of Investigation, USA**

**DAY2**  
26 May  
2022

# ADDITIONAL CONFERENCE EVENTS



## 12th meeting

Start at 10:30 AM

Conference room JUPITER, 2nd floor

CISO Club represents the independent Slovak - Czech community of CISOs (or similar positions), who discuss the most important cybersecurity topics and challenges. Club members and participants are involved in active, problem-solving discussions, share their experiences and create practical tools that move this area forward.

**CISO Club will be running in Slovak language.**  
**Seats are limited!**

- Comparison of Cloud services from the perspective of security AWS / Azure / Google
- The process of using Cloud Compliance security
- SOC and the use of Threat Intelligence in practice, SW for Incident Management  
- practical experience with deployment, operation
- Experience with the operation of Pentera and similar tools in companies
- Changes in standards: NISv2, new ISO 27002
- A new look at ICT security given the events around us

### FORMAT

In - person

### DURATION

3 hours

### NUMBER OF ATTENDEES

Up to 25 attendees

### Chairman

#### Marek Zeman

CISO Tatrabanka

Marek has more than 20 years of experience with IT security. He focuses on database security, ICT risk management, behavioral metrics, analysis, evaluation and correlation of unstructured data, security of artificial intelligence. Marek is constantly increasing awareness of information security by introducing new educational approaches.

## Bonus virtual sessions

### From SEH Overwrite with Egg Hunter to Get a Shell

Rodolpho Concurde Netto, Penetration Tester

### How to Secure Your Software Supply Chain - Practical Lessons to Protect Your App

Feross Aboukhadijeh, CEO, Socket

### Insider Threat: What is Social Engineering?

Crux Conception, Founder, Professor, Crux Conception

*The program guide is subject to change.  
Some of the sessions are solely virtual.*

14 June  
2022

# VIRTUAL TRAINING



**Ladislav Baco**  
Network Analyst  
ESET

## TARGETED THREAT HUNTING

Incidents happen. The question is when? And maybe even better question is not when it will happen, but what if it has already happened. The attack could be stealthy and undetected yet. However, we can assume that the attack is still ongoing. Now, with this mindset, let's focus on our possibilities. How we can detect the attack and verify our hypothesis? The answer is Threat Hunting. We will take steps to prepare for the Threat Hunting such as sharpen our detection techniques based on host and network artifacts. Then, we should be able to detect the attacker's footprint in the (lab) environment, putting the traces together and investigate the (simulated) cyber attack.

## KEY TAKEAWAYS

- Discussing various Threat Hunting approaches and strategies
- Introducing Threat Intelligence basics
- Collecting and prepare Indicators of Compromise and detection signatures
- Detecting host-based and network-based intrusions
- Performing targeted Threat Hunting based on relevant Threat Intelligence data

## PRE-REQUISITES

*The participants should:*

- Be familiar with Windows OS
- Be familiar with Linux OS (basic Linux knowledge is sufficient)
- Have a computer with at least 16 GB of RAM, 40 GB of free space on HDD/SSD and installed
- VirtualBox (64-bit edition)
- Have an active unfiltered network connection
  - lab virtual machines and training data will be provided in advance
  - during training we will use several online resources and cloud services

## FORMAT

Virtual

## DURATION

5 hours, including 2 coffee breaks

## TARGET AUDIENCE

Security Specialists, Incident Responders, Blue Teamers, SOC Analysts, Forensic Investigators, Malware Analysts

# NETWORKING EVENTS

## VIP RECEPTION

May 24

Hotel Orea Pyramida

*Attendance by invitation only.*



## NETWORKING DINNER

May 25, 19:30

Klášterní Pivovar Strahov  
Strahovské nádvoří 301,  
Praha 1

# WHY TO ATTEND QUBIT CONFERENCE PRAGUE 2022

Considering attending this immersive conference event? Read why our delegates recommend you join Qubit cybersecurity community:

*"One of the most amazing things about being at Qubit Conference is the people, ranging from private, to industry, to academia to individuals in cybersecurity arena. It's a fantastic opportunity to meet, greet and collaborate."*

**David Hitchcock, Assistant Legal Attaché at FBI**

*"Qubit creates a very distinguished event for professionals in the central region of cybersecurity community."*

**Ondrej Krehel, VP, DFIR Services at LIFARS, a SecurityScorecard Company, USA**

*"Events like Qubit Conference is how you meet the colleagues working on the same problem that you are. You get perspective that you may not get every day."*

**Charles Tango, CISO at Altria**

## CONNECT WITH THE MOST UP-TO-DATE INFORMATION

Experience the atmosphere of **"community spirit"** where cyberspace professionals come together to explore the latest news in the rapidly evolving field of cybersecurity. You will gain a profound understanding of the technologies and solutions in cybersecurity that will fit your organization's needs and provide immediate **long-term benefits**.

## EXPLORE AND EXCHANGE IDEAS

Offered are various opportunities to **interact with peers and experts** in the field, to learn, debate, exchange and explore best **innovative ideas** in cybersecurity development. Share valuable insights and experience solutions that could make a **great impact** on your organization and your career path.

## RECEIVE PRACTICAL KNOWLEDGE

Along with the traditional panel discussion formats, offered are also various **interactive sessions** covering a wide range of topics where you'll learn about the new crucial cybersecurity trends, threats and solutions which can be put into practice right away in your organization or business.

## DISCOVER THE LATEST TECHNOLOGY

We open the door to cybersecurity technology from a number of **the top world's leading vendors**. At the Expo hall we offer the options to interact with demos, connect directly with vendors, attend **sponsor briefings** and sessions and gain a better understanding of the newest cybersecurity technologies and solutions that present a **valuable asset** to any organization or business.

*The program guide is subject to change.  
Some of the sessions are solely virtual.*

# SPONSORS

## PLATINUM SPONSORS



## GOLD SPONSORS



## SILVER SPONSORS



## BASIC SPONSORS



## SOLUTION CENTER



# PARTNERS

## SUPPORTING PARTNERS



## MEDIA PARTNERS



# VENUE

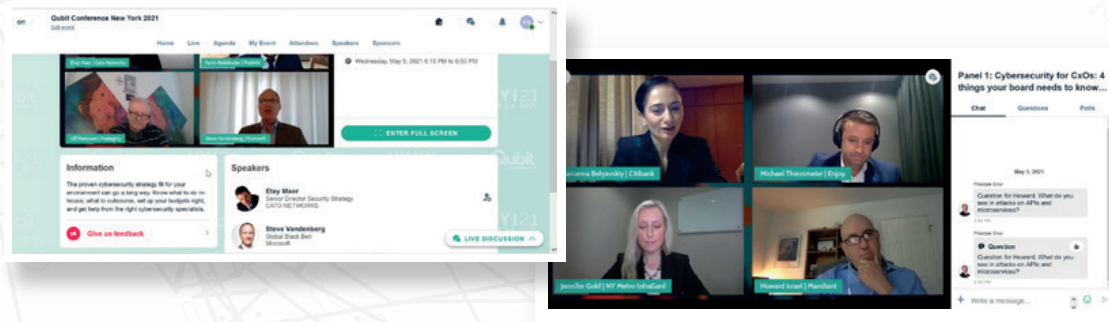
## OREA Hotel Pyramida Praha

OREA Hotel Pyramida  
Bělohorská 24  
169 00 Prague



# VIRTUAL PLATFORM

Cannot attend in-person? Join us virtually via Swapcard.



# CONTACT

**SPONSORSHIP, SPEAKERS:**  
**SALES:**  
**OTHER:**

[katarina.gambos@qubitconference.com](mailto:katarina.gambos@qubitconference.com)  
[denisa.lavkova@qubitconference.com](mailto:denisa.lavkova@qubitconference.com)  
[info@qubitconference.com](mailto:info@qubitconference.com)



**REGISTER**