

Qubit Conference

PRAGUE 21

SEPTEMBER 8-9

PROGRAM GUIDE

HYBRID EVENT

HYBRID EVENT

With the world changing, we chose a hybrid approach this year. Offering in-person and virtual experiences designed to give you a mix of opportunities for learning, networking and collaboration. Qubit Conference Prague is creating a history, we are creating a robust virtual experience to complement the on-site event.

SPEAKING BUREAU

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



PETR DVORAK

CEO

Wultra

Czech republic



ETAY MAOR

Senior Director
Security Strategy

Cato Networks

USA



MAREK ZEMAN

CISO

Tatra Banka

Slovak republic

Event Moderator: Joseph Carson,
Chief Security Scientist and Advisory CISO, Thycotic, Estonia

Event Moderator: Boris Mutina,
Senior Security Analyst, Excello/Virusfree, Czech republic

Registration

8:00 - 9:00

9:05 - 9:20

Conference Opening - *Maria Krahulecova, CEO, Qubit Security, Ondrej Krehel, Co-founder Qubit Security*

9:20 - 9:50

KEYNOTE

The New Digital Normal – Agile, Continuous, Contextual

This session will examine how long-term trends and recent black swan events have affected and accelerated enterprise IT services and architecture over the last two years. We will discuss near-term technological changes and the challenges and opportunities they present for both attackers and defenders. "Secure" is a destination that no organisation will ever reach. Security is an endless race to help your business take the greatest possible advantage of opportunities offered by technological and societal change, while anticipating the new possibilities for compromise they offer to your adversary. Chess was never this much fun!

Rik Ferguson – Vice President Security Research, TREND MICRO, UK

9:50 - 10:40

KEYNOTE

How good is the fuel powering your SOC - The importance of Threat Intelligence in modern day Cybersecurity Operations

Automation and optimization are the top priorities of modern day Security Operations Center. Threat Hunters and SOC Operators are using tools like SIEM and SOAR that are supposed to streamline processes and increase the effectiveness of cyber defence. While this is true - this only works effectively when decisions are made on data of good quality. Hence the rise of Threat Intelligence. During my keynote I will demonstrate how you can make qualified decision by having access to the biggest Threat Intelligence data provider in the world. We will look at direct threats like leaked credentials, domain abuse, data up for sale on Dark Web. I will also show how you can speed up alert triage and dramatically enhance the speed of your investigations. We will also go into the Future where we will analyze what threats might be coming our way.

Mateusz Olszewski, Sales Executive Eastern Europe, Recorded Future, Poland

10:40 - 11:05

KEYNOTE

Network Security as-a-service

One of the most profound shifts we've been hearing about is that legacy appliance-based approaches, that our customers around the globe are using to secure their networks, aren't working anymore. Evolving your network for remote work has opened it up to risks. Join today's session to discover how delivering network security at the edge - not data centers - can better protect your applications, your data, and your users.

Vijay Chauhan, Senior Product Marketing Director & Arwa Ginwala - Senior Solution Engineer, Cloudflare

11:05 - 11:25

LIGHTNING TALKS

Petr Cihelka, Sales Team Lead, Fortinet | Tomas Vlcek, Head of Cybersecurity Division, Prefis, Slovakia | Joseph Carson, Chief Security Scientist and Advisory CISO, Thycotic, Estonia | Martin Woźniak, Head of Corporate Sales & Business Development, Whalebone, Slovakia

11:25 - 11:40

COFFEE BREAK

11:40 - 12:10

Do's and Don't's managing penetration testing with clients - Case study

Both Red teaming and penetration testing should be a must in every company's security assessment. Since companies don't do such an engagement very often and in many cases it might be their first time it is very important to manage expectation and set rules of engagements properly.

Zuzana Duracinska, Project manager, LIFARS, USA

Red Team attacks, GDPR fines and COVID lay-offs? Protected without a service providers needed!

You may wonder what these 3 different topics have in common, especially that the latter were not anticipated originally. What started as an assurance control for SOC effectivity proved later to protect sensitive data better against regulatory fines. Next year COVID stroke and the insiders to be laid-off wanted to get their piece of pie before being terminated. Three very different scenarios over couple of years where Intelligence helped the CISO of the international retailer to crack on them without re-staffing his team nor adding another managed security service provider.

Petr Hnevkovsky, Cyber Security Strategist, Micro Focus

12:10 - 12:45

Outsourced personal data breach management and the Twitter case

GDPR has introduced data breach management including 72 hours deadline for the supervisory authority notification. I would like to describe the issues and the complexity of this obligation based on the Twitter case and highlight the most important takeaways from current enforcement activities.

František Nonnemann, Compliance and Operational Risk Manager, MallPay, Czech republic

What is going on in the network before ransomware occurs?

Most organisations identify a ransomware at the time the data is encrypted and there is a ransom demand "on the table". However, this is preceded by a large number of IoCs that can be effectively detected on the network in real time and thus prevent a real cyber incident.

Roman Cupka, Senior Principal Consultant | Flowmon, Kemp company & CEO | Synapsa Networks

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

12:45 - 13:45

1 - HOUR LUNCH

13:45 - 14:20

DIY risk management

When you cannot fitting tool, you need to build one yourself. We have used this DIY approach after struggling to find suitable tool. We built our risk management on top of JIRA and utilizing native JIRA functionality of custom fields and workflows.

Daniel Chromek, CISO & Adam Remias, Security Specialist II, ESET, Slovakia

Your New Hire Turned to be a Hacker

It's like a James Bond movie but for real. A case study of an under-cover read teamer hired as a junior programmer. The target has decades of experience. Cybersecurity is not a new topic. How far can the attacker get? How will the IT department react? Bring some popcorn.

Tomas Zatko, CEO, CITADELO, Slovakia

14:20 - 14:55

PANEL DISCUSSION

#1 business priority: Cybersecurity

Cybersecurity is still viewed as a technology area; here is how to make it a #1 business priority.

Moderator: Joseph Carson, Chief Security Scientist and Advisory CISO, Thycotic, Estonia
Speakers: Rik Ferguson, Vice President Security Research, TREND MICRO, UK

14:55 - 15:30

I Was Promised A Jetpack

How did we get here? The discussion will look at the promises that were made of a security future that we're still in search of today. This is analogous to the personal jetpack that we were promised in the early days of science fiction.

Dave Lewis, Global Advisory CISO, CISCO, USA

The resident evil inside your database

A data breach is an organization's worst nightmare. Your databases can be used as a pivot to infiltrate the organization or may be the target to exfiltrate sensitive data. In this talk we will explore different exploitation techniques used by attackers to attack databases. We will dive into practical real life examples captured by our honeypots around the world, such as ransom and crypto mining campaigns, malware deployment, distributed brute-force attacks, evasion techniques and slow & low exfiltration.

Sarit Yerushalmi & Ofir Shaty, Security Researchers, IMPERVA, Israel

15:30 - 16:00

What the hack

Hacking groups have changed their focus towards critical infrastructure and supply chains. The Kaseya case is just one example of a very sophisticated attack.

I will talk to you about the techniques that hackers are currently using and provide my perspective on where their focus will shift next

Michal Merta, Cyber Fusion Center Lead, Accenture, Czech republic

How to build Secure Development Lifecycle if you don't have a budget like Google's

Often, we hear a lot of information about how to build security development lifecycle at software companies and best practices from Google, Microsoft, Cisco, etc. However, there is a small nuance hidden here: not everyone has the same budget and the same opportunities. By the way, secure development in cases of DevOps, CI/CD practices is a necessary feature, even for small and medium company. During my statement I want to explore basic steps on the way of secure development, which are able to protect from 80% of threats. Besides, I'll show some useful instruments, my own practical examples and achieved goals

Roman Zhukov, Product Security Manager, Intel, Russian Federation

16:00 - 16:15

COFFEE BREAK

16:15 - 17:00

Challenges of Space Security

Our everyday life is dependent on space technologies. Thousands of satellites are orbiting the Earth and providing us crucial data which influence even the functioning of our critical infrastructure. In the presentation the biggest challenges of space security will be introduced and explained.

Tarmo Kellomäki, Director of Digital Security & Functional Safety, Huld Oy, Finland

Leaving no stone unturned

A ransomware incident is never a good start of your week. It gets even worse when you find it encrypted literally everything. Or did it? We will look at a real-world case which started with no obvious tracks to follow, but in which some active research and a dose of intuition yielded great results.

Peter Kosinar, Technical Fellow, Eset, Slovakia

17:00 - 17:30

CLOSING KEYNOTE

"Mind the Gap" or Common Incident Response Challenges

In today's increasingly cyber world organizations are more exposed than ever to potential malicious attacks. With remote workforces increasingly becoming the norm rather than the exception, organizations can expect to encounter even graver threats than they have before. The preparation an organization pursues before an event is the greatest determiner of how big of an impact a malicious event will have. Simply put, how an organization prepares for these events can spell success or doom. We will discuss common mistakes we've seen in our recent engagements and cover decisions made to facilitate a more positive outcome for our clients. Because being proactive can significantly reduce the negative impact of a security event we will also discuss preparatory steps at-risk organizations can take ahead of time (and to be honest everyone connected to the internet is at risk) or more specifically, industry best-practices for preparedness, investigation, and response.

Howard Williamson, Assistant DFIR Director, LIFARS, USA

Event Moderator : Joseph Carson, Chief Security Scientist and Advisory CISO, Thycotic, Estonia

Registration

Conference Welcome & Introduction

OPENING KEYNOTE

Cyber Chains are Forever!

We're the luckiest generation in the history of humanity. The Renaissance 2.0 of cyberspace is producing game changing technologies that will last a thousand years. In this session, Eddie Doyle will explore how blockchain will transform cyber security into an unfair fight against threat actors, helping you position yourself & your company to anticipate where this revolutionary technology will lead us.
Eddie Doyle, Keynote Speaker & Security Strategist, Check Point SW Technologies, USA

8:55 - 9:00

9:00 - 9:20

9:20 - 9:55

The Postman Always Rings Twice : Threat actors, exfiltration innovations and their patterns

2020 has been a year of stealth, exfiltration and innovation in the digital world. With the threat landscape expanding and threat actors are targeting several sectors in this digital space, the need for research and the need for innovative proactive research is the need of the hour.

Shyam Sundar Ramaswami, Senior Research Scientist, Cisco, India

9:55 - 10:20

Which legacy is good legacy? Critical infrastructure and Cybersecurity Awareness

When it comes to critical infrastructure, how a 50-year-old technology compares to a 50 thousand-year-old human? I want to show you how it is possible (without any special effort) to destabilize countries Critical Infrastructure systems.

Tino Sokic, CEO, Cybersecurity Professional, dobardan.net, CNV-IBIS Croatia

10:20 - 10:35

COFFEE BREAK

10:35 - 11:05

Ransom-wave Aware

In this session, we will introduce more clarity to these attacks imbued with skills of how to deal with detection and prevention. Most importantly, you will gain valuable skills of how to deal with ransom and ransomware cybercrime at every stage of the attack.

Alex Holden, CISO, Hold Security, USA

11:05 - 11:50

US Services and GDPR – Compliance Nightmare

The presentation will focus on personal transfers within EU and outside in the third countries. The focus will put on nature of the legal conditions and the relevant judgments (Schrems II case) affecting transfers to third parties, especially USA.

Jan Bárta, attorney, partner, AK Jan Bárta, Czech republic

CISO Club

CISO Club will be running in Slovak language
Marek Zeman, CISO, Tatra Banka Slovak republic

11:50 - 12:20

DNS – core service and attackers

Examples of real-life attacks, how and why attackers are using DNS protocol. What other threats we are facing in this area. It is not only reputation of domains. How attackers can exfiltrate or infiltrate data to networks and endpoints without detection on security stack.

Jan Rynes, Solution architect, Infoblox, Czech republic

13:00

12:20 - 13:20

1-HOUR LUNCH

13:20 - 13:40

Decoding Cyber - Supply Chain Risk Management through NIST

The challenge faced by most organizations is that supply chain risks are not well understood and most importantly not assessed before using them for critical functions. Have you assessed your suppliers? Is it time to integrate Cyber supply chain risk management into Enterprise Risk management?

Mani Keerthi Nagothu, Security Lead, Ballard Power Systems, Canada

13:40 - 14:25

PANEL DISCUSSION

Zero trust “beyond the buzzword”

Real life stories and challenges with Zero Trust

Moderator: Paul Vixie, Chairman, CEO and Cofounder, Farsight Security, USA

Speakers: Jan Adamovsky, CSO, Slovenska sporitelna, Slovakia; Petr Hnevkovsky, Cyber Security Strategist, Micro Focus, Czech republic

14:25 - 14:40

COFFEE BREAK

14:40 - 15:10

Implementing NIST Cybersecurity and Risk Frameworks

The US National Institute of Standards & Technology (NIST) provides de-facto standards for security, compliance and privacy. Session attendees will learn how to apply the NIST Cybersecurity and Risk Management Frameworks for increased security, compliance and standardization.

Ronald Woerner, Associate Professor, Information Technology, Bellevue University, USA

15:10 - 15:35

CLOSING KEYNOTE

Stop predicting the past: how to identify unknown threats

You have seen the power of the SASE architecture and the cloud transformation companies are undergoing – in this session we will explore case studies of organizations that have already started reaping the benefits of these changes. We will see how single pass engines and network based threat hunting empower security researchers and allow them to identify previously undetectable threats that fly under the radar of legacy point solutions.

Etay Maor, Senior Director Security Strategy, Cato Networks, USA

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

NETWORKING EVENTS

VIP RECEPTION

September 7, 2021

By invitation only



NETWORKING DINNER

September 8, 2021

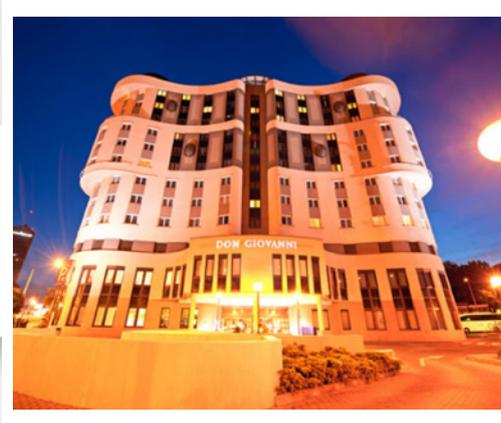


VENUE

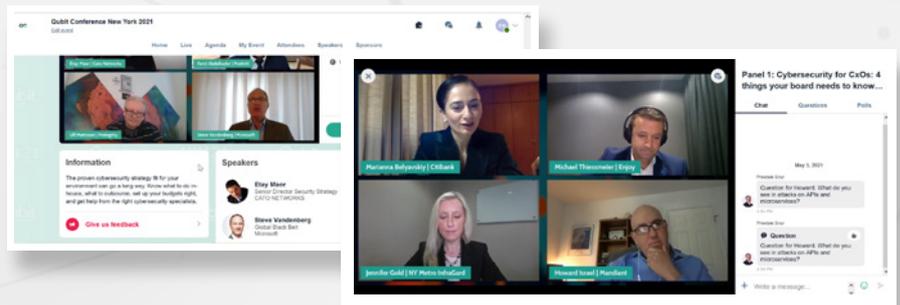


DON GIOVANNI HOTEL PRAGUE

Vinohradská 157A
130 20 Prague
Czech Republic



VIRTUAL PLATFORM: Swapcard



CONTACT

SPONSORSHIP, SPEAKERS:
SALES:
OTHER:

katarina.gambos@qubitconference.com
denisa.lavkova@qubitconference.com
info@qubitconference.com



REGISTER

SPONSORS & PARTNERS

PLATINUM SPONSORS



GOLD SPONSORS



SILVER SPONSORS



BASIC SPONSORS



SUPPORTING PARTNERS



MEDIA PARTNERS





ROMAN ZHUKOV
Product Security Manager
Intel Corporation
Russian Federation

SECURE DEVELOPMENT LIFECYCLE IMPLEMENTATION And secure development mindset

When we try to implement Security spirit into the product development, security often perceived as something unclear and only in the light of "we don't like that stuff, but we have to do it". As a result, we often end up software teams with only minimal compliance, which is far away from the nature of today's cybersecurity standoff. This course is intended to explain how to implement and continuously grow an enhanced Secure Development Mindset into all those involved in product release lifecycle. We will discuss why this is critical for almost all modern companies, how to determine the level of SDL maturity and what tailored measures should be applied. It can be valuable for companies, who really try to shift their culture. And security is a good and valued leverage to do it. At the workshop, we will learn:

- View on Security from "another" (development team) side
- How to start engaging different folks in security: from developers to marketing
- "Sold!" – how to transform security from compliance to culture
- Examples where Security can be and cannot be flexible
- Hands-on practice: assessment methodology how to figure out you really need a heavy SDL with multiple roles or only basics
- Secure development lifecycle methodology
- Architecture, secure design and threat modeling basics and hands-on practice
- Secure coding and validation basics and hands-on practice
- Security claims handling and post-release vulnerability management
- Hands-on practice: incident response and media interactions
- Product security basics for non-technical but customer-facing roles: sales, marketing and high-level managers

FORMAT

Virtual

DURATION

3 hours

ATTENDEES

Up to 30 attendees

TARGET AUDIENCE

CISO
Information security managers

PREREQUISITES:

Participants should have basic knowledge of SW development process
Basic knowledge of one programming languages would be an advantage



SHYAM SUNDAR RAMASWAMI
Senior Research Scientist –
Research and Efficacy
Cisco
India

INVESTIGATING DIGITAL DOCUMENT MALWARE LIKE A PRO A.K.A. The Professor

E-mails and attachments: A deadly duo that targets several organizations and is the main cause of cyber attacks today. Word, Excel, PDF and Images sneak in as attachments via e-mails that pose to be legitimate ones. Once they are opened, they end up dropping .exe or malicious files via macros, java scripts, macro 4.0 or steganography.

Mission: We will be decoding all these malicious documents and files via tools, manual reversing/analysis, build python scripts and other means to stop these attacks. Are you ready?

FORMAT

Virtual

DURATION

8 hours including lunch and
two 15-minutes breaks

ATTENDEES

Up to 30 attendees

TARGET AUDIENCE

Beginner and Intermediate

PREREQUISITES:

Participants will be provided with virtual machines with all the tools
and malicious software



MIKAEL MÖRK
Sales Engineer
Recorded Future

WORK EFFICIENTLY AND PROACTIVELY IN YOUR SOC WITH SECURITY INTELLIGENCE

In today's rapidly changing threat environment, knowing what is happening inside your organization is not enough. This interactive workshop covering topics including:

- Correlation and enrichment of Indicators of Compromise (IoCs) allowing for quick and confident decisions in a SIEM environment
- Automation and playbook implementation through a SOAR environment
- Incident response and proactive security work best practices
- How to monitor your threat landscape; what threat actors are targeting you, and what are their Tactics, Techniques, and Procedures (TTPs)?

FORMAT

In-person

DURATION

2 hours

ATTENDEES

Up to 20 attendees

TARGET AUDIENCE:

Security Analyst
Security Operations Analyst
Security Operations Engineer
SOC Tier 1-3/Level 1-3
Incident Responder
Security Architect

PREREQUISITES:

Participants are expected to have experience in at least some of the following:

- Using a SIEM environment (e.g. Splunk, QRadar, etc.) with log correlation, triaging, making decisions regarding escalation
- Using a SOAR environment (e.g. XSOAR, Resilient, Phantom, etc.) with some level of utilizing playbooks/workflows with enrichment
- Performing incident response (any level or extent; malware analysis, use of YARA rules, etc.)