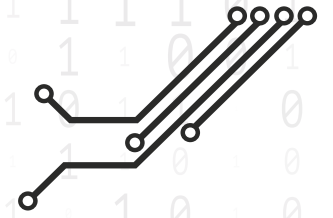




Universe of Cyber Security



# QUBIT CONFERENCE

# PRAGUE 2020

**First** virtual edition

23-24 SEPTEMBER

PROGRAM GUIDE



# MEET THE SPEAKING BUREAU

## of QuBit Conference **Prague 2020**

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



### Head of Speaking Bureau

#### IVAN MAKATURA

CEO of Slovak Cyber Security Competence and Certification Centre

**Slovakia**



#### ROMAN CUPKA

Principal Consultant CEE & Country Manager at Flowmon Networks, CEO & Co-Founder at Synapsa Networks

**Slovakia**



#### MIKE GOEDEKER

CEO and Founder at Hakdefnet International

**Germany**



#### ETAY MAOR

Chief Security Officer at IntSights

**USA**

# SECURITY OPERATION CENTER

LEARN HOW TO FIGHT EVER CHANGING CYBER THREATS AND  
KEEP YOUR ENVIRONMENT SAFE



Security Operations Centres are used to monitor and detect threats to the organization. Majority of all breach victims learn of a compromise from third-party notifications, not from internal security teams. Similarly, most of them are often caught by surprise. Therefore, executives demands that their security teams provide enhanced security activities to stop these threats.

How should organisations build and evolve their security operations centre to manage current and

emerging threats? What capabilities does a security operations centre require to deliver value? This training clearly defines what the Security Operation Center is and provides you with insights on what measurable benefits it provides to your organization. In this workshop, a spin-off to the last year series dedicated to SIEM technology, participants will oversee not only theory but also a practical hands-on training where their network will be under attack. They will be taught various strategies to help defend against several attack scenarios. Participants will take part of multiple discussions on building, operating, and maturing a successful security operation center. Speaker will share his practical and innovative approach and techniques he used to enhance the key operational functions of a SOC: network monitoring, incident response, threat intelligence, forensics and self-assessment.

## TARGET AUDIENCE:

CISO, Information security managers, Compliance managers, SOC managers, OT Risk managers, Cyber threats investigators, System Administrators, Senior Security Engineers, Individuals working to implement Continuous Security Monitoring or Network

## DURATION:

8 hours including lunch break and two 15-minutes coffee breaks

## PREREQUISITES:

- Laptop with PDF Reader installed

## NUMBER OF ATTENDEES:

Up to 20 attendees

## TRAINER:



### Pavol Dovicovic

Security Consultant and former CISO

[REGISTER FOR TRAINING](#)

# **THREAT HUNTING**

## **WINDOWS HOSTS**



Chosen chapters from threat hunting were built to accelerate transition from reactive security operations to proactive security operations. In this course you learn how to proactively detect attackers in Windows environment in a network and find basic sets of evidence of their presence.

Incidents happen. The question is not whether, but when. Maybe next month. Maybe next week. Maybe today. Or... is it already happened? It is better to be prepared for these situations in advance. Use proactive

approach and detect security breach early. Then take containment action and remediate the incident.

During this training the participants will see most common techniques used by attackers when they got access to the victim network – we will introduce adversary tactics and techniques based on real-world observations.

The participants will see various post-exploitation scenarios, including information gathering and data collection, communication with command and control servers, credential dumping and privilege escalation, internal network reconnaissance and lateral movement, achieving persistency and defense evasion.

Moreover, we will focus to detection of introduced techniques and attacker presence in the network. The participants will have an opportunity to get hands-on experiences with tools and procedures for searching and investigating the network and endpoints to detect and isolate these advanced threats.

### **LEARNING OBJECTIVES:**

- Identify necessary sources of data needed for threat hunting
- Learn how to use comprehensive set of tools tactics and procedures for systematical threat hunting

### **WHAT SHOULD YOU TAKE FROM THIS TRAINING:**

Extension of your professional skills as a security specialist to threat hunting, know the difference between forensics and threat hunting and obtain a mindset of threat hunter as opposite from standard security operations.

## COURSE STRUCTURE:

- Threat hunting vs. Digital Forensics Analysis
- Threat hunting process in Windows host
- Attack vectors / TTP of Attacker – case studies
- Persistence mechanisms of attackers/ malware and their detection
- Security model of Windows systems / Authentication / GPO and common vulnerabilities
- Types of lateral movements and detection possibilities
- Windows Logging and auditing capabilities, use cases and setup guides
- IOC in standard attacks, where to find them and how to interpret them
- Automating detection of IOC in multiple hosts with / without domain
- Sniper threat hunting forensics in Windows environment

**Course level:** Intermediate to professional  
**This will be a technical training.**

### TARGET AUDIENCE:

Incident handlers, Forensics analysts, Malware analysts  
Security specialists with technical skills

### DURATION:

8 hours including lunch break  
and two 15-minutes coffee breaks

### PREREQUISITES:

#### The participants should:

Be familiar with Windows PowerShell (beginner level),  
have a little bit experience with Windows Forensics,  
bring a Windows laptop with at least 16GB of RAM, 100  
GB of free space on HDD/SSD and installed VirtualBox  
64-bit edition. VMWare should be also fine; however,  
it is not fully tested with our environment.

### NUMBER OF ATTENDEES:

Up to 20 attendees

















### TRAINER:



#### Lukas Hlavicka

Director of Digital Forensics & Incident Response Department, LIFARS

[REGISTER FOR TRAINING](#)

9:00 - 9:05		<b>Conference Opening</b> Maria Kalicakova   Co-founder of QuBit Conference
9:05 - 9:20		<b>Cyber Security for Leaders in Today's Digital World</b> <i>Opening Keynote</i> Boris Mutina   Senior Security Analyst, Virusfree.cz   Czech republic Thousandfold aspects of cybersecurity could become useless in the leader's hands. In the complex topic to which the cybersecurity evolved within the past years, it seems to be almost impossible to transform the threats, risks, and policies to a piece of valuable business information. At the same time, all information must be protected which often seems like an obstacle. So the cybersecurity needs to be molten, cast, and machined to
9:20 - 9:40		<b>Threat Intel Research - how to look for dirt and find gold</b> <i>Case Study</i> Jean Gobin   CISO and Forensic investigator, LIFARS   USA This session presents a few applied cases using both open and proprietary data sources where we will start from a simple indicator and see how we can generate several more."
9:40 - 10:05		<b>EXECUTIVE DILEMAS: Steal These Ideas</b> Stefan Hager   Security Consultant, DATEV eG   Germany Whether you're a newcomer to infosec or a seasoned veteran, you might have noticed that defending stuff is not the easiest of tasks if done right. Here are some ideas aimed to improve upon technical, organisational and other challenges one might encounter in all kinds of companies.
10:05 - 10:25		<b>Lessons learned in OT Security from COVID-19 and How to Thrive in the "New Normal"</b> Chris Sandford   Director Industrial Cyber Security Services, Applied Risk   United Arab Emirates <ul style="list-style-type: none"> <li>Operational environment changes, variability in risks and vulnerabilities and other challenges posed by COVID-19 to industrial environments</li> <li>How organizations need to prepare in order to restore the same operational state once the crisis is passed</li> <li>Incident Response Planning: adapting to the "new normal" and managing risks</li> </ul>
10:25 - 10:30		<b>Coffee Break</b>
10:30 - 11:00		<b>AWS Security: Sweet dreams vs reality</b> <i>Case Study</i> Tomas Zatko   CEO, Citadelo   Slovakia This talk is a guide through some of the most common vulnerabilities in AWS deployments and ways how hackers exploit them. Come to have a look from hacker's point of view. It helps you to become a better defender.
11:00 - 11:25		<b>WiFi Pineapple - WIFI AUDIT, Targeted MitM, Credential Harvesting, and More Fun</b> Joseph Carson   Chief Security Scientist & Advisory CISO, Thycotic Most organization employees and other individuals, be it in an office environment or working remotely at home, at a café, or while traveling, will find themselves confronted with an unfamiliar Wi-Fi network. Hopefully, they'll ask that all-important question: Is this Wi-Fi safe to use?
11:25 - 11:50		<b>Why digital transformation is a security operations challenge</b> Roman Cupka   Principal Consultant CEE & Country Manager, Flowmon Networks   CEO & Co-Founder at Synapsa Networks   Slovakia The transfer of employees from the corporate environment to "home office" has shown us that it is possible to manage business efficiently also remotely. On the other hand, he brought new experience in the field of crisis management and indicated how the approach to cyber and information security will evolve during the digital transformation. Migration into the clouds, use of third-party business agile tools and finally lack of expert human resources ... all of these will be main challenges for daily security operations.
11:50 - 12:30		<b>Lunch</b>
12:30 - 12:50		<b>Would you try a new vaccine straight on yourself?</b> Yosi Shneck   SVP, Head of Cyber entrepreneurship and business development, Israel Electric Corp.   Israel In order to protect your organisation from cyber risks, significant mitigation steps should be taken. These include the ability to test, validate, and approve before making any modifications to your systems or components, especially to the core production systems of your business. As unbelievable as it sounds, most of the system modifications are done directly on your production system without a prior validation or examination, just as if you are trying out a new vaccine on yourself.
12:50 - 13:25		<b>Towards Quantum-Resistant Banking Applications</b> Tomas Rosa   Chief Cryptologist, Raiffeisen Bank International   Czech Republic & Petr Dvorak   CEO, WULTRA   Czech Republic On a typical banking application based on Diffie-Hellman protocol over elliptic curves, we show what it takes to substitute this scheme by a similar protocol from the area of post-quantum cryptography. We focus on similarities as well differences that need to be obeyed carefully.
13:25 - 13:55		<b>5G, Apps, Bots, IoT, AI &amp; the Upcoming Cyberwars!</b> Edwin Doyle   Global Security Strategist, Check Point   United States The convergence of cellular & Wi-Fi through 5G will exacerbate the challenge of scaling security at the speed of data. In preparation for the upcoming cyberwars, it's time we start looking at the Cloud to deliver security services to meet the hyperscale demands of Apps, IoT & BOTS.
13:55 - 14:20		<b>How Slovakia prepares for digital totalitarianism of the Chinese type</b> Pavol Luptak   CEO, Nethemba   Slovakia
14:20 - 14:25		<b>Coffee Break</b>
14:25 - 14:50		<b>Information Security / Data Protection Implications for Strategic Management</b> Jindrich Kalisek   Attorney at Law, DPO, KKCG Group   Czech republic A: Information security and personal data protection have numerous not-so-obvious implications for both strategic and operational management of business corporation. Why is it vital for business owners and managers to adopt, ensure and promote high standards of information and data security, integrate those standards within all business and managerial processes and what are common failures of such integration?

14:50 - 15:15

### Embracing the NIS directive for digital service providers









Daniel Chromek | CISO, Eset | Slovakia

- approach on adopting the DSP requirements over multiple services through the whole service life-cycle (creation, change, dismissal)
- risk-based approach is recycled from ISO 27001
- IRP adjustments and training were needed
- troublesome points of the legislation at SK

15:15 - 15:45

### Preparing For a Breach - the Cybercriminal Perspective Closing Keynote

Etay Maor | Chief Security Officer, Intsights | USA

9:00 - 9:30	 <b>Why Cyber Risk Intelligence Matters</b> <i>Opening Keynote</i> Mike Goedecker   CEO & Founder, Hakdefnet International   Germany This talk focuses on three things. 1. What is the value of security an risk intelligence to the average person 2. Why is cyber risk intelligence important and what kind of information does it collect 3. Using our OpenSource Framework and Codename Divinity to find low hanging fruits like default credentials.
9:30 - 9:50	 <b>EXECUTIVE DILEMAS: Risk management &amp; governance</b> Kritika Kotnala   Chief marketing officer, CIA   India Risk Management & governance in an organization is an important parameter to consider for implementing the business process. Under this one of the most important concepts is the Single Source of Truth as part of the information architecture that helps to ensure federal use of data and
9:50 - 10:20	 <b>How to negotiate with hackers? Emoji, WhatsApp and a little bit of flattery</b> <i>Case Study</i> Moty Cristal   CEO, NEST   Israel By speaking to the hackers and negotiating with the "bad guys", Cristal explained how he dealt with the scenario. Communication was key, exchanging WhatsApp messages with the hackers to find out their motivations and incentives.
10:20 - 10:45	 <b>The E-mail Story</b> Boris Mutina   Senior Security Analyst, Virusfree.cz   Czech republic While we see the expansion of all possible technologies related to cybersecurity, email security is often solved by a box. This presentation shows the evolution of the email in brief and the security measures and standards available to secure it. Also, we will uncover the most frequent threats and abusers in CEE area.
10:45 - 10:50	 <b>Coffee Break</b>
10:50 - 11:25	 <b>Ransomware remediation</b> <i>Case Study</i> Lukas Hlavicka   Director of DFIR services, LIFARS   USA Ladislav Baco   Senior Security Consultant and Malware Analyst, LIFARS   USA The real battle with attacker - Case study of Mid-level client with multiple geographically separated sites, which was attacked by group of cyber criminals utilizing multiple attacks against victim, last of which was ransomware.
11:25 - 11:50	 <b>Defense Evasion - Code Obfuscation</b> <i>Case Study</i> Jan Marek   Cybersecurity Professional, Cyber Rangers   Czech republic PowerShell as the builtin automation engine and scripting interface is the primary abused component of the Windows operating system by hacker to do the evil. In this session I will cover different techniques of code obfuscation and how it is (un)detected by Windows OS security features and antivirus.
11:50 - 12:15	 <b>Privacy-Preserving with Homomorphic Encryption</b> <i>Case Study</i> Ioan Popovici   Chief Software Engineer, Avelgo   Romania Doing computation on encrypted data is not only possible, but it tends to be required more and more by today's privacy critical ecosystems. What are the scenarios where this is required? How to tackle the common challenges while adopting Homomorphic Encryption? Let's find out.
12:15 - 13:00	 <b>Lunch</b>
13:00 - 13:30	 <b>Cloud Risks Management</b> Damir Savanovic   Research Fellow, Cloud Security Alliance   Spain The objective of this presentation is to identify and examine gaps that have been introduced over the last 10 years by the phenomena succinctly known as Cloud Computing, and how the core concepts of effective risk management can still be artfully applied.
13:30 - 14:10	 <b>Dissecting and Comparing differents Binaries to Malware Analysis</b> <i>Case Study</i> Filipi Pires   Global Research Manager, Hacker Security   Brasil Demonstrate differents kind of structures in the binaries as a PE (header and your sessions), ELF (header and your sessions), PDF(header/ body/ cross-reference table/trailer), explaining how each session works within a binary and where it would be possible to "include" a malicious code.
14:10 - 14:15	 <b>Coffee Break</b>
14:15 - 14:45	 <b>Physical acquisition from iOS devices. New approaches and possibilities.</b> Alexey Shtol   Senior System Architecture Engineer, Elcomsoft   Russia I will discuss the two innovative jailbreak types: the rootless jailbreak and the newest generation of jailbreaks based on the unpatchable bootrom exploit. Both of these jailbreak types have their share of pros and contras.
14:45 - 15:10	 <b>Messaging Layer Security: Towards a New Era of Secure Group Messaging</b> Raphael Robert   Head of Security, Wire   Germany Discusses message encryption protocols, its current ecosystem, and why it's still not a solved problem in the corporate setting. While personal messaging systems have been adopting Signal, corporate messaging has not massively moved in that direction due to technical challenges, such as scalability.
15:10 - 15:30	 <b>Virus Harvesting Czech eObčanka (eID Card) Identities</b> <i>Case Study</i> Martin Pozdena   Senior Information Security Consultant, Auxilium Cyber Security   Czech republic Jan Recinsky   CSOC manager, WardenSec   Czech republic There are new eID cards to support public sector digitalization efforts in Czech Republic. Our talk would introduce the system, explain how citizen's identities could be stolen during authentication and demonstrate PoC virus covertly stealing online eID identities of fully unaware citizens.
15:30 - 15:35	 <b>QuBit 2020 and future</b> <i>Closing Keynote</i> Ondrej Krehel   CEO, LIFARS   USA





# SPONSORS

## QUBIT CONFERENCE PRAGUE 2020

**First virtual edition**

### PLATINUM SPONSOR:



### SILVER SPONSOR:



### SPONSORS:



## SUPPORTING PARTNERS:



## MEDIA PARTNERS:



# QUBIT CONFERENCE PRAGUE 2021

## SAVE THE DATE

**JUNE 2-3, 2021**  
CONFERENCE

**JUNE 1, 2021**  
PRE-CONFERENCE WORKSHOPS

PRAGUE, CZECH REPUBLIC