Universe of Cyber Security

QuBit Conference

PROGRAM GUIDE

QuBit Conference PRAGUE 2019

APRIL 10 - 11 2019 | **HOTEL INTERNATIONAL PRAGUE**

MEET THE SPEAKING BUREAU

of QuBit Conference Prague 2019

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

RICHARD KISKOVAC

Head of Speaking Bureau, Independent Cyber Security Consultant

Slovakia

IVAN MAKATURA

Executive consultant, IBM Security Services, Chairman of Cybersecurity Association

Slovakia

PETR KUNSTAT

IT Security Consultant at Micro Focus

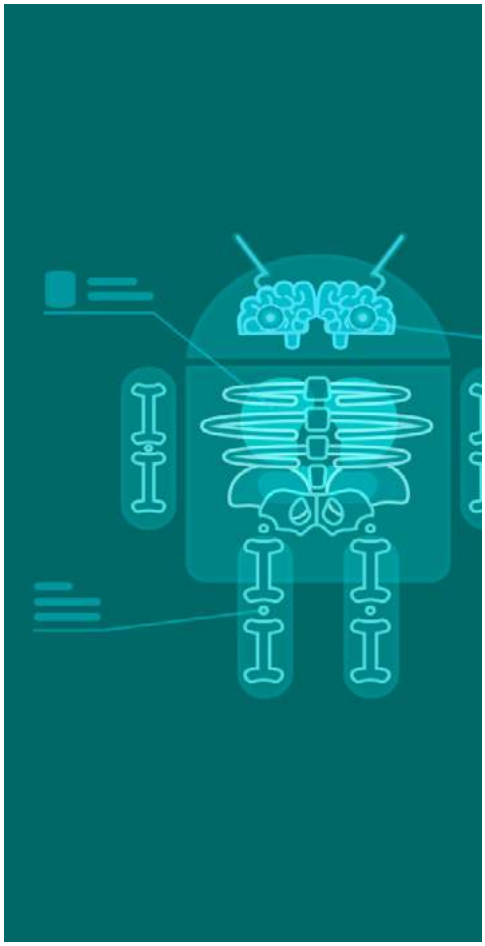
Czech Republic

VACLAV MACH

CEO of Czech Publishers' Association

Czech Republic

PRE-CONFERENCE TRAININGS



ANDROID REVERSE ENGINEERING

9 APRIL 2019 | PRAGUE

Smartphones and mobile devices are the essential part of our life nowadays. Even the attackers and criminals have realized that and they are targeted these platforms more often. While the principles of analysing and preventing this kind of malicious activities remain similar, the technologies, tools and possibilities of malware can differ.

This training covers fundamentals of the reverse engineering of the mobile applications for Android platform. We aims to decompiling and understanding the mobile apps written in Java and also the native code in shared objects, especially for ARM architecture.

We will introduce a little bit theory about development and components of the Android applications and ARM assembly. During training, the participants will see the tools suitable for behavioral analysis and instrumentaion of the suspicious samples, reverse engineering the Java apps and native code. We will spent a lot of time by practical hands- on with analysing the prepared CTF application utilizing various principles using by the real malware samples.

After this training, participants should be able to understand the design of the Android apps including the native libraries. They also sould be able to read the ARM assembly and reverse engineering the mobile apps from APK sample to Java code and/or ARM assembly services

PREREQUISITES:

The participants should:

- Be familiar with Linux command-line
- Be able to create simple programs (variables, conditions, for-cycles, functions) at least in one scripting language, e.g. Python
- Have a little bit experience with X86 assembly
- Linux laptop with at least 8GB of RAM, 20 GB of free space on HDD/SSD and installed VirtualBox (64-bit edition)

TARGET AUDIENCE:

- Malware analysts, security specialists, incident handlers, software developers and enthusiasts with technical skills

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

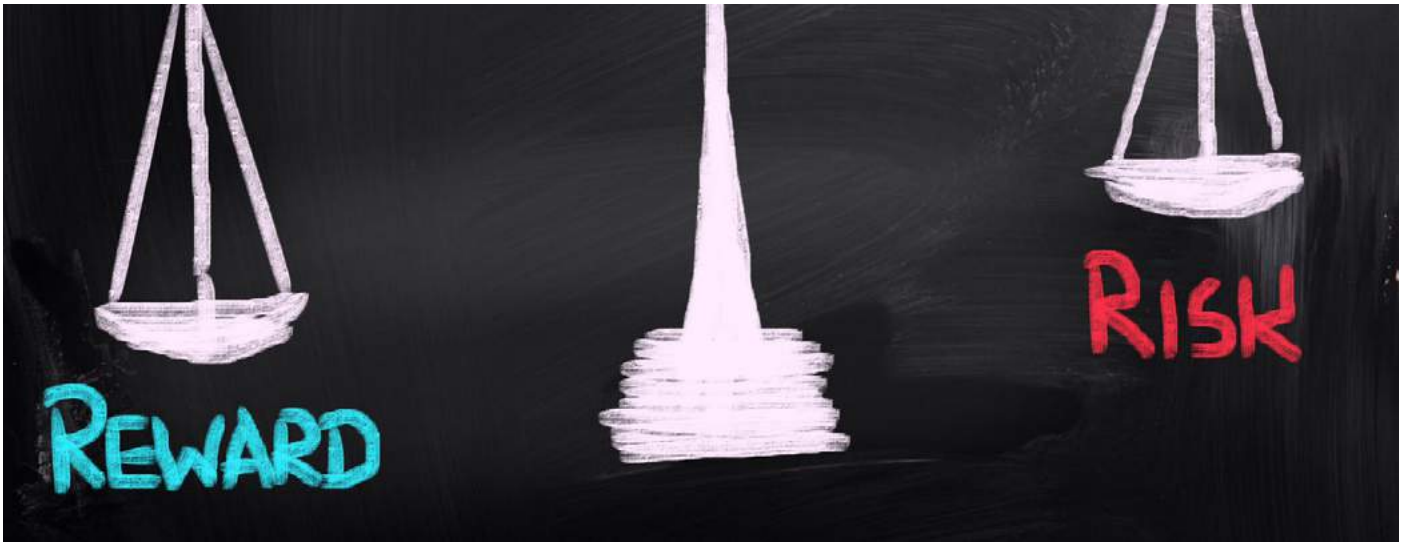
Number of attendees: Up to 20 attendees

TRAINER: Ladislav Baco & Jan Kotrady
Security Analyst, CSIRT.SK

INFORMATION SECURITY RISK MANAGEMENT WORKSHOP

9 APRIL 2019 | PRAGUE

In this course students will learn the practical skills necessary to perform regular risk assessments for their organizations. The ability to perform risk management is crucial for organizations hoping to defend their systems. There are simply too many threats, too many potential vulnerabilities that could exist, and simply not enough resources to create an impregnable security infrastructure. Therefore, every organization, whether they do so in an organized manner or not, will make priority decision on how best to defend their valuable data assets. Risk management should be the foundational tool used to facilitate thoughtful and purposeful defence strategies.



TARGET AUDIENCE:

- Security specialists, security architects, security engineers, compliance directors, manager
- Data protection officers
- Operational Risk management
- Compliance managers
- Information assurance management
- Staff responsible for IT Service Management processes

Duration: 8 hours

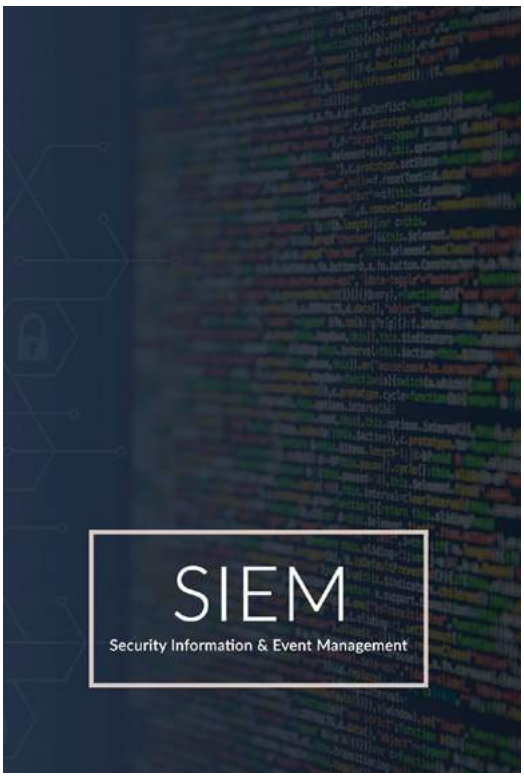
Number of attendees: Up to 20 attendees

TRAINER: Ivan Makatura

Executive Consultant at IBM Security
Chairman of the Board, Association of Cybersecurity

PREREQUISITES:

A basic understanding of information security and information security management topics is helpful for students attending this class. However a strong background in any of these skills is not a pre-requisite for the class. In the class students will be taught a step by step approach for performing a risk assessment regardless of their technical information security or management background.



SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

9 APRIL 2019 | PRAGUE

Security operations nowadays, do not suffer from a "Big Data" problem but rather a "Data Analysis" problem. Monitoring tools became an inevitable part of the IT world. Those, who do not use automatic tools for evaluating events and incidents, can't expect and guarantee adequate level of security. Let's face it, there are multiple ways to store, process and analyze large amounts of data without any real emphasis on gaining insight into the information collected.

Training provides holistic approach to security management. We aim to provide in – depth insight into SIEM technology.

All participants stand to gain valuable insights:

- In-depth knowledge of what SIEM technology is and how to implement, configure and fine-tune SIEM technology
- Solid understanding of how to use SIEM capabilities for business intelligence
- Hands-on experience with how to deploy SIEM technologies (various log types analysis, how to process unknown logs, regex practice, incident investigation a analysis, rules creation,..)
- Insight into how to monitor, identify, document and respond to security threats and reduce false-positive alerts
- Thorough understanding of compliance reporting and documentation

TARGET AUDIENCE:

- Security specialists, security architects, security engineers, compliance directors, manager
- Data protection officers
- Operational Risk management
- Compliance managers
- Information assurance management
- Staff responsible for IT Service Management processes

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

Number of attendees: Up to 20 attendees

TRAINER: Pavol Dovicovic

Head of Information Security and Infrastructure, EMM

PREREQUISITES:

Notebook with Windows or Linux, at least 8 GB of RAM

DAY 1

10 APRIL

TRACK A

TRACK B

8:00 - 8:50 **Registration**

9:00 - 9:10 **Conference Opening**

Maria Kalicakova I CEO QuBit Security | **Zdenek Hrib** I Mayor of Prague

9:10 - 10:00 **Case study: Nation State Attack APT10 – Operation Cloud Hopper** *Opening Keynote*

Ondrej Krehel I CEO LIFARS, USA

Jean Gobin I LIFARS

Nation States attacks are an alleged myth and highly underestimated by Fortune 2000 corporations. A great example is a massive covert operation called Cloud Hopper executed by the Asian threat actors, APT10. The LIFARS Incident Response Unit will demystify the military cyber operations of foreign nations and provide a classified inside into the military style cyber weapons used against enterprises. The tools, techniques, and procedures of ransomware as well as with APT10 will be presented. Detection and response will be discussed ending with cyber resiliency tips.

10:00 - 10:30 **Solution center Opening - Intro talks**

10:30 - 11:15 **Cryptocurrencies: 10 years later**

Jarek Jakubcek I Strategic Analyst, Europol

- Cryptocurrencies – natural evolution of money?
- Use and abuse of cryptocurrencies
- Crypto OpSec
- Blockchain – beyond cryptocurrencies

TBA

11:15 - 11:30 **Coffee Break**

11:30 - 12:15 **Defensive deception - a hole as a security control**

Alex Lozikoff I Brand manager, Softprom

You will know what it deception, main market trends, types and benefits of deception, major commercial solutions and open source tools, best practices and recommended tactics, see real life examples of deception and it's results.

How to Test Artificial Intelligence? Can artificial intelligence cheat us?

Marek Zeman I CISO

Peter Kopriva I Tatrabanka

The lecture will provide information on how to store hidden information in artificial intelligence and how reverse engineer works in the neural network. At the same time it will be given an example of when it was successfully broken through "clever" artificial intelligence. We introduce the reason why this type of lecture is marrated by lecturer from the financial sector?

12:15 - 13:00 **We Pass the Costs to You! An analysis of Cryptomining and Cryptojacking**

Josh Pyorre I Senior Security Research Analyst, CISCO

This presentation will walk you through a brief history of CryptoMining and CryptoJacking, how it all works and the various steps you or your organization can take to detect and stop it.

Machine learning on the field of Threat Hunting

Gergo Gyebnar I CEO, Black Cell

The presentation will give the audience a high-level overview about the related challenges and problems regarding TTP/IoC finding, parsing and finally, distribution.

13:00 - 14:00 **Lunch**

14:00 - 14:30

FIRE CHAT

JOHN FRANCHI I U.S. GOVERNMENT

14:30 - 15:15

CISO role in Enterprise *panel discussion*

Moderator: Peter Beres I SophistIT

Panelists: Charles Tango I CISO, ALTRIA

15:15 - 16:00

Evil Qubits - The Threat of Quantum Cryptanalysis Explained

Tomas Rosa I Chief Cryptologist, Raiffeisen BANK / Cryptology and biometrics competence centre

In this lecture, we focus on understanding the key elements of quantum computation. We will also review the most influential algorithms that can be used for quantum cryptanalysis. The aim is to grasp where the power of quantum computers is coming from and what can be expected with respect to weakening of our cryptographic primitives. From here, we show the way towards post-quantum cryptography, i.e. the cryptography in the era of quantum computers.

Don't Acquire Your Next Breach: Managing the Vendor Risk Lifecycle

Kabir Barday I CEO, OneTrust

In this session, you'll learn how to implement a successful vendor risk management process and explore helpful tips and real-world practical advice to improve your privacy and security programs.

16:00 - 16:15

Coffee Break

16:15 - 17:00

Cybercriminal's mind - The anatomy of a targeted attack

Jiri Vanek I Senior Security Consultant, Unicorn

What is a modus operandi of an organized cybercrime? How a targeted cyber attack goes and what are the main points of failure in defense? This presentation should give you a rough idea of what to expect when you become a target and how you should protect your company.

The Good, the Bad and the Ugly of Millions of Security Alerts

Nadav Avital I Threat Researcher Manager, IMPERVA

I'm going to discuss what exactly alert fatigue is, how we got to this position as an industry, and what are the necessary steps for an organization to solve this problem. I will also demonstrate how we were able to boil down millions of security alerts per day to a few meaningful events.

17:00 - 17:30

The Role and Mission of Government in Cyber security *panel discussion*

Panelists: Rastislav Janota I National Security Authority

Crawl, Monitor, Walk, Detect, Run like Heck, Threat Hunting

O'Shea Bowens I Founder & CEO, Null Hat Security

This session will focus on important strategies, tools, techniques and planning to consider for your hunt. We will talk about the reality of the relationship between incident response, cyber threat intelligence and threat hunting, as well as provide real world examples of identifying attacker methodologies.

17:30 - 17:45

Sophist IT diamond sponsor *Closing Keynote*

17:45 - 18:00

Closing remarks

19:30 - 23:00

RAFFLE & NETWORKING DINNER SPONSORED BY SOPHIST IT

DAY 2

11 APRIL

TRACK A

TRACK B

8:30 - 8:50 **Registration**

8:50 - 9:00 **House Keeping Notes from Organizer**

9:00 - 9:30 **Opening Keynote**

Peter. J. Ahearn I Special agent, FBI

9:30 - 10:15

From the Lab to Nmap: How the OSSTMM cut the distance between Science and Cyber Security

Rem Elnahas I Cyber Security Analyst, Security Solutions Consultants

The aim of this lecture would be to guide the audience through the core pillars of the OSSTMM 3, showing how few and basic concepts like twelve possible types of controls, limitations of a system and porosity, shared between different layers of OpSec (human, physical and telecommunication) can be used to build the skeleton for an unbiased, reproducible, measurable and effective security analysis.

Peter Kosinar I ESET

10:15 - 11:00

Using Big Data technologies to improve SIEM scalability

Gabriela Aumayr I HPE

Josef Niedermeier I HPE

In this presentation we show-case our real-life experience about transitioning from a traditional SIEM to a modern, scalable and performant big-data processing solution.

The Cyber Forensics Lab Evidence Review: Cryptocurrency 80 Million Hack and SamSam Ransomware Ring *Case study*

Ondrej Krehel I CEO LIFARS

Jean Gobin I LIFARS

From evidence and insights from actual cyber forensic cases learn the methodologies, attack vectors, Indicators of Compromise, and most importantly actionable insights for preventing these attacks.

11:00 - 11:20 **Coffee Break**

11:20 - 12:00

Hit me baby one more time - story of an ordinary spamtrap

Boris Mutina I Senior security analyst, Excello

Spamtrap is sometimes considered as a harvesting of the low hanging fruit. If you dig deeper, you can find interesting details which can turn into real treasure when protecting your organization. The presentation explains the prerequisites and setup of a spamtrap, approaches on how to have it populated and what to do with the content of it.

TBA

12:00 - 12:30

Chaos vs. Complexity: The GDPR's impact on data protection norms around the world

Eduard Goodman I GLOBAL PRIVACY OFFICER, CyberScout

This discussion will focus on the history of the GDPR and how that history lends itself expanding its influence far outside the European Union. It will also discuss different lenses by which to view both the GDPR and the changing global data protection landscape and they can be applied to global organizations.

Securing the virtualized world

Jan Marek I Solution Architect, KPCS

How Microsoft's Hyper-V Shielded VM protects customers secrets and sensitive data and how it can help you to comply with security standards and safely live in modern malware world.

12:30 - 13:30

Lunch

13:30 - 14:15

CISO and DPO–allies or enemies? A story on combining cybersecurity and dataprotection in the evolving threat landscape

Mauriche Kroos I Information Security and Data Protection Officer, Enexis Group

How to prevent "boardroom cyber and data protection fatigue" and how to bring practical and sustainable cultural changes in place in the whole organisation.

Artificial Intelligence – War of the Machines

Alex Holden I CISO and President, Hold Security

Understanding the hacker advances in Artificial Intelligence is critical to stop the new generation of cyber threats. At the same time, what techniques can we teach our AI's to examine and prevent new exploitations. Learn about historical and current AI use by both hackers and the defenders. Plus, what is next for AI advances on both sides.

14:15 - 14:45

mHealth applications

Zuzana Cih Hecko I Senior Associate at Allen & Overy

The market has recently been flooded by various health and lifestyle applications. While strict GDPR requirements related to processing of sensitive personal data would apply to these apps, soon another piece of EU legislation will impact such applications. Many apps will be considered as "medical devices" which triggers application of strict pharmaceutical regulation. This means, inter alia, that each app will need to undergo a "conformity assessment" and CE marking process to assess its safety

Cybersecurity and Blockchains - Are blockchains secure? Maximizing the potential of blockchains and Emerging Tech

Adewale O Omoniy I Associate Partner, IBM

This talk discusses using risk management frameworks, tools, methods and cybersecurity assurance standards. From experience developing multiple blockchain solutions, the speaker will discuss blockchain use cases and how to employ cybersecurity best practices. That is, adopting cyber risk management principles, introducing threat modeling, designing for privacy, depth in defense rigors while assessing against threat vectors, in order to enable and maximize the potential of blockchain and other emerging technologies adoption.

14:45 - 15:00 **Coffee Break**

15:00 - 15:30 **Breaking the silence - cyber insurance**

Rozalie Ryclova I Business Development Manager, Boxtrap

What is the state of play for cyber-insurance? How can cyber insurers and the wider cyber-security community join to deliver value to the client? And what are examples of partnerships to date?

Security Intelligence - Security Automation

Roman Cupka I Principal Consultant CEE at Flowmon Networks

Identifying and analyzing security incidents today for organizations in the public and private sectors takes 45 to 250 days in average. New legislation require incident reporting to be made immediately - within hours or days. Efficient Adaptive Security Architecture nowdays and in the close future wont be applied without effective Threat Intelligence that identifies known attackers and real-time behavioral analysis that, in combination with deep network visibility, machine learning and artificial intelligence, assesses communication in computer networks and user & network behavior. In conjunction with automation tools and classification mechanisms, it is now possible to provide mean time to incident response from months to seconds or minutes supported by native integration into SOCs and CSIRTs.

15:30 - 16:15 **Women in Technology, Risk and Cyber** *panel discussion*

Ondrej Krehel I CEO LIFARS, USA

Panelists: Jenny Boneva I Vice President, ISACA Sofia Chapter and Chairwoman of Membership Committee

Alexandra Dorcakova I Head of TC Security Operations, T-Systems

Katarina Rolna I Chief of Security & Business Continuity Management, Tatra Banka

Marianna Belyavskiy I AVP, Operational Risk, ERM at CIT Bank

Eva Skornickova I Data Privacy and Cybersecurity Advisor

16:15 - 16:30 **RAFFLE & CLOSING SPEECH**

QuBit Conference

NETWORKING EVENTS

VIP RECEPTION
9 April, 2019

NETWORKING DINNER
10 April, 2019

Sponsored by: SophistIT Streamline Your Forensic Analytics

Diamond Sponsor:

SophistIT Streamline Your Forensic Analytics

Silver Sponsor:

EMM

Supporting partners:

APWG www.apwg.org · ESAP · CYBERSTRING · education.sk kurzy | štúdiá | konferencie | hotely · HOPIN Taxíky pod palcom · ISACA Belgrade Chapter · itSMF Slovensko · ICT NETWORK NEWS · NETWORK NEWS · OWASP · sli.do