QuBit
Conference

Universe of Cyber Security

QUBIT CONFERENCE SOFIA 2019

PROGRAM GUIDE

14 NOVEMBER/ **SOFIA BULGARIA**

MEET THE SPEAKING BUREAU

of QuBit Conference **Sofia 2019**

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

NIKOLA NYAGOLOV

Principal, Consulting, ITNL Bulgaria
ISACA Member, CISA, CGEIT, PMP

Bulgaria

JENNY BONEVA

Vice President, ISACA Sofia Chapter and Chairwoman of Membership Committee

Bulgaria

BORIS MUTINA

Senior security analyst at Excello

Slovakia

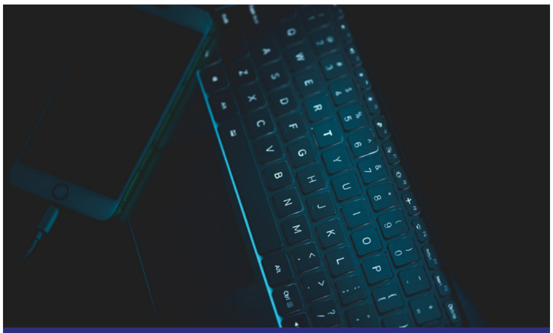
LYUBOMIR TULEV

Chief Cyber Security Operations Lead at Amatas

Bulgaria

PRE-CONFERENCE TRAININGS

HACKING DEMO



13 November 2019 | Sofia

Information and information system security is one of the most important topics today. In the era of more frequent and always different attacks, malware, ransomware, it's increasingly difficult to find the right way to defend. In order to determine the techniques and technologies needed for defending the organization, you need to know what is attacking you and how it attacks you. What hackers use, how they think and how they come to us are just some of the questions that are constantly being asked and the answer is difficult to find. This training introduces you to all types of attacks and demonstrates the techniques and how ease is to perform them, with the goal of demystifying hacking and defying the mode of defending.Topics: Walk the attendees through all the steps of one attack, from zero point to complete control. Explain all techniques and demonstrate attacks and some of the most used tools. Defining and explaining defense techniques for each of the attacks, and parts of the attack.

- **Introduction and basic concepts**
- **The evolution of hacktivism**
- **Identifying the target**
  - Passive Reconnaissance (OpenSource Intelligence, WhoIS, Metagoofil, GoogleHacking)
  - Active Reconnaissance (PortScanning, Footprint, Vulnerability Scanning)
- **Network scanning and enumeration**
- **Social engineering**
  - Phishing attacks
- **Physical security attacks**
- **Eavesdropping**
  - Sniffing
- **MiTM**
  - Session Hijacking
- **Hacking the system**
  - Metasploit
  - Creation and distribution of Trojans, Viruses
  - Stealth Trojans
- **DenialOf Service attacks**
- **Activities after exploitation**
  - Keylogger
  - Backdoor
- **Wireless hacking**

TARGET AUDIENCE:

Management/C-suite audience, CIO, CISO VP IT, VP Security, Director of IT or Director of Security Managing Principal, Partner, Director, SVP, Attorney, cyber forensic investigator, Global Risk, Manager, IT administrators, Network administrators, Information security officers

DURATION:

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

PREREQUISITES:

- Notebook with internet connection

NUMBER OF ATTENDEES:

Up to 20 attendees

TRAINER:

Aleksandar Mirkovic

CISO/DPO - Information Security Manager **Serbia**

ENTERPRISE SECURITY ARCHITECTURE

13 November 2019 | Sofia

A one-day seminar on enterprise security architecture that introduces you to the fundamentals, relationships, necessary principles and overall context for deploying and managing the discipline.

Main objectives for ESA

Enterprise security architecture is the art and science of designing and overseeing the construction of business and enterprise systems, a common information system. As a result, the systems are protected against damage, their business use without worry, and support that guarantees the ability to rely on them and is also protected against attacks.It consists mainly of two parts - enterprise risk management strategies+information security management and supervision systems. We know a lot of approaches and recommendations, but it is always an evolutionary process of medium-term / long-term nature with the necessary support for top-down management.The term Business Driven Information Security is also often used to describe the fact thatsecurity is an integral and important part of a holistic, proactive business management inall its parts. ESA builds directly on EA (enterprise architecture) and works conceptually onindicators to achieve enterprise goals, missions, services, products and partnerships in a proven and sustainable way.

THE COMBINATION OF CONTENT AND KNOWLEDGE

- Explanation of the content and importance of enterprise security architecture in a business context
- Description of the dimensions and layers of the enterprise security model
- Reference description of the usual ESA I/O documents from practice
- Matrix knowledge of individual roles - related to architecture, project management, operation
- Practical examples

TARGET AUDIENCE:	**DURATION:**
Management/C-suite audience, CIO, CISO VP IT, VP Security, Director of IT or Director of Security Managing Principal, Partner, Director, SVP, Attorney, cyber forensic investigator, Global Risk, Manager	8 hours including lunch break and two 15-minutes coffee breaks
PREREQUISITES:	**NUMBER OF ATTENDEES:**
• Awareness or practice in business and corporate architecture • Notebook with internet connection	Up to 20 attendees

TRAINER:

Lubos Fryc

Trainer, Coach, Mentor, CEO at Skill Bill, **Certification: - TOGAF® 9 / TOGAF® Essentials 2018, Czech Republic**

INDUSTRIAL CYBER SECURITY

HOW TO PROTECT CRITICAL INDUSTRIAL COMPUTER INFRASTRUCTURE?

13 November 2019 | Sofia

Industrial Cyber Security training will consist of four parts – Industrial Environment Overview, Industrial System Threats, Social Engineering a.k.a. Creating the "Human Firewall"and Applicability of the Industrial Cyber Security Standards – IEC 62443, NERC CIP, NIST SP 800-82.

Introduction to the functionalities and usabilities of industrial control systems and Distribution Control systems will be discussed in the first part. SCADA systems will be also introduced.

Industrial System Threats will be discussed in the second part of the training. Attack vectors of the Industrial Control system are the most dangerous places that shall be analyzed and protected. We will analyze the most common attacks (TriTon Malware, The Marriott Hack, Ransomware attacks, etc.). How these attacks worked?

Last few years has shown that 60% of successful attacks were delivered via Social Engineering practices. Christopher Hadnagy as on of the biggest social engineering specialist said social engineering is: "The Art of the Human Hacking". Protect your system from the most vulnerable fact, which is "human" itself. Introducing the social engineering practices and phishing emails can mitigate the risk for the attack itself.

"How to use Industrial Security Standards?" Requirements of these industrial cyber security standards we can create a plan, how to mitigate the risks in our environment.

TARGET AUDIENCE:	**DURATION:**
Industrial Security Experts, IT/OT Managers, ICS/DCS Engineers, IT/OT Admins, IT/OT Specialists	8 hours including lunch break and two 15-minutes coffee breaks
PREREQUISITES:	**NUMBER OF ATTENDEES:**
• IT Networking basics • Notebook with internet connection	Up to 20 attendees

TRAINER:

Tamas Buzgo

Chief Security Officer | DECENT, **Certified ISA/IEC 62443 Specialist,** 14 years experience in Cyber Security field - 7 years in Industrial Cyber Security, **Slovakia**

PROGRAM 14 NOVEMBER

KEYNOTE

SOCIAL ENGINEERING IN THE DARK FUTURE

Yehia Mamdouh | Sr. Penetration Testing Consultant & Security Researcher | **DTS Solution**
United Arab Emirates

In this talk, we will know how the social engineering will be in the future? How Phishing and Vishing will look like? How artificial intelligence will play a big role in those attacks? How to prepare ourselves as individuals and organizations to defend against those attacks?

THE MOST DEVASTATING CYBER SCAMS THE FBI IS FIGHTING TODAY

Dean Kinsman | Assistant Legal Attache | **FBI Bucharest** | Romania/USA

Cyber threats have quickly evolved over the past 10 years resulting in crippling attacks against small and medium sized businesses by manipulating the financial transaction system for multi-million dollar heists. This presentation will discuss the most critical defensive actions everyone must take to defend themselves against the dynamic actors behind these attacks.

CASE STUDY

HOW MACHINE LEARNING RAISES THE STAKES ON BOTH SIDES OF THE INFORMATION SECURITY BARRIER

Dimiter Shalvardjiev | CTO & CISO | **Code Runners** | Bulgaria

This talk focuses on the various ways in which ML supports both offensive and defensive information security practices - in other words, both the red and blue teams.

Case study and analysis of infected document spreaded via emails and delivering the Remcos RAT. You can see defeating the multiple layers of obfuscation and various tools and techniques in action during the livemalware analysis session. We will also dicsuss how difficult it is to perform this kind of attack and you will see it not only from the analyst point of view, but also from the point of view of the victim and the attacker.

PANEL DISCUSSION

GDPR AFTERMATH

Marko Simeonov | Legal and Compliance Officer | **AMATAS** | Bulgaria

Panelists: Kaloian Petrov | Data Protection Officer | **Postbank** (Eurobank Bulgaria AD)
Emilian Zlatev | Data Protection Officer | **Telenor Bulgaria**
Anton Ivanov | Data Protection Officer | **Allianz Bulgaria**
Anton Todorov | Data Protection Officer | **UniCredit Bulbank**
Ventsislav Karadzhov | Chairman | **CPDP**

How effectively has GDPR been applied and do you think business still fear the consequences of not following the requirements? What are the challenges controllers and processors face when protecting personal data and business interests? How do they find the balance? What are the directions for business optimizations that GDPR provides? Did the implementation of GDPR requirements help business in other aspects? What are the directions for business optimizations that GDPR provides? Did the implementation of GDPR requirements help business in other aspects?

EDUCATIONAL SESSIONS

DEVELOPMENT OF SECURE AND QUALITATIVE APPLICATIONS DELIVERED BY IMPROVED AND AUTOMATED SOFTWARE DEVELOPMENT LIFE CYCLE

Mariya Harseva | Data Security Officer | **ScaleFocus** | Bulgaria
Stoyan Iliev | Senior Security Operations Engineer | **ScaleFocus** | Bulgaria

This talk focuses on the various ways in which ML supports both offensive and defensive information security practices - in other words, both the red and blue teams.

Case study and analysis of infected document spreaded via emails and delivering the Remcos RAT. You can see defeating the multiple layers of obfuscation and various tools and techniques in action during the livemalware analysis session. We will also dicsuss how difficult it is to perform this kind of attack and you will see it not only from the analyst point of view, but also from the point of view of the victim and the attacker.

MICROSOFT'S APPROACH TO SECURE USER DEVICES

Jan Marek | **Cybersecurity Professional** | Cyber Rangers | Czech Republic

Latest Microsoft's operating system Windows 10 contains many security features that can help the user to protects his data. Let me show you the family of these technologies and how they can make user's world secure.

THE ROAD TO HELL IS PAVED WITH BAD PASSWORDS

Chris Kubecka | CEO, Security Researcher, Author of Down the Rabbit Hole An OSINT Journey | **HypaSec** Netherlands

Ever wonder what incident management is like when an embassy gets hacked, by ISIS? Come on a journey of surprisingly weak security, insider threats, a 50 million dollar extortion attempt, diplomatic immunity, city wide security lock down, all while >400 dignitary's lives dangle in the negotiation crossfire. Join Chris, the lead investigator and resolver on a super-secret squirrel adventure against ISIS & Turkish Intel in The Hague, The Netherlands. Discussing the 2014 Saudi Arabian embassy hack. Whoever said STEM was boring made it boring! Solve the crime and save lives with key takeaways from a real life cyber terrorism investigation. No classified information will be shared, some terrorists were harmed in the making of this talk.

EDUCATIONAL SESSIONS

USING BLOCKCHAIN TECHNOLOGY FOR ENERGY INFRASTRUCTURE WHILE ENSURING CYBER SECURITY

Michael John | CISO | **WePower** | Bulgaria

The talk will outline how blockchain is used in the energy sector through the tokenization of power generation and consumption data. The talk will furthermore describe the security implications of using blockchain in this domain and introduce the general security concepts of energy grids.

MIGRATING YOUR PCI DSS INFRASTRUCTURE TO AWS

Pavel Kaminsky | CEO | **Seven Security Group Ltd.** | Bulgaria

Taking corporate security to the next level with cloud through various options and architectures. The shared responsibility and PCI DSS compliance. Practical implications of applied cloud security technologies.

THREATS SEEN BY SANS INTERNET STORM CENTER

Bojan Zdrnja | Senior SANS Internet Storm Center Handler | **SANS** | Croatia

In last couple of years we have witnessed some sophisticated (and some less sophisticated) attacks that severely impacted businesses around the world, causing millions of EUR in damage. SANS Internet Storm Center has been following and analyzing various attacks for more than 2 decades. In this presentation, Bojan Zdrnja, senior SANS Internet Storm Center handler will introduce the SANS Internet Storm Center and will talk about several new emerging threats that are slowly becoming prevalent.

IT THREATS – THE REAL VULNERABILITIES FOR ICS/DCS AND SCADA SYSTEMS

Tamas Buzgo | Chief Security Officer | **DECENT** | Slovakia

I will show the IT threats from the real world based on site-experiences. Current ICS/DCS and SCADA systems are very sensitive for the security. I will present real use cases how can malwares, ransomwares and other attack vectors can cause nightmare for the Operation managers. We will discuss how could we react in case of incidents even how important is the real protection.

ICS CYBERSECURITY - TRENDS & CHALLENGES

Dan Demeter | Security Researcher - Global Research and Analysis Team | **Kaspersky** | Romania

In our connected world, new attack vectors are being discovered almost daily. Due to their nature, Industrial Controls Systems are built to last for decades, but an increasingly complex infrastructures now demands some systems be now connected either to a local network / VPN, or even worse, directly to the internet.

During our presentation we will be focusing on the current ICS threat landscape and what (we think) the future holds. We will present our vision and solutions on how you can better protect your ICS infrastructure in order to immediately react to new attacks aimed at your organization.

NETWORKING EVENTS

VIP RECEPTION

By Invitation Only.

Captain Cook Restaurant | Narodno sabranie“ 4, 1000 Sofia Center, Sofia, Bulharsko

13NOVEMBER/ **SOFIA BULGARIA**

NETWORKING DINNER

Izbata Tavern | Slavyanska“ 18, 1000 Sofia Center, Sofia, Bulharsko

14NOVEMBER/ **SOFIA BULGARIA**

Platinum Sponsor

kaspersky

Silver Sponsor

SANS EMEA

scalefocus
IT solutions for sustainable growth

Supporting Partners

amatas

a&s ADRIA
Stručni magazin za kompletna sigurnosna rješenja
The Professional Magazine Providing Total Security Solutions

bait

BILATERAL CHAMBER OF COMMERCE BULGARIA - ROMANIA

1895
БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

CBAP

CSIRT.SK
CSIRT.GOV.SK

EMBASSY
OF THE SLOVAK REPUBLIC
IN SOFIA

HIRE HEROES
BETA project of DEV.BG

ISACA®
Sofia Chapter

SeeNews
Business Intelligence
for Southeast Europe

sli.do

Media Partners

AVERIA NEWS

CYBER DEFENSE
MAGAZINE

freedomonline

NEIRONIX

ICT NETWORK NEWS
www.ict-nn.com

NETWORK NEWS
www.ITSEC-NN.com

TechEvents
online

VENUE

INTERCONTINENTAL SOFIA

4 Narodno Sabranie Sq: Sofia, 1000, Bulgaria

FOR ANY SPONSORSHIP,
SPEAKERS OR SALES INQUIRIES
CONTACT US AT
INFO@QUBITCONFERENCE.COM

REGISTRATION WEBSITE

QuBit Conference SOFIA 2019

@QuBit Conference

@QuBitCon

@QuBitCon