SHOQATA E BANKAVE TË KOSOVËS
KOSOVO BANKING ASSOCIATION

CYBER AND INFORMATION SECURITY MANAGEMENT

DATE: 24 – 26 SEPTEMBER 2018
VENUE: KOSOVO BANKING ASSOCIATION

OBJECTIVES

The participants will have an overview of Cybersecurity and an understanding of how to mitigate the associated risks.
The course will:
• cover the various areas of Cyber Security
• obtained notions of user safety - individual behavior (passwords, email, mobility, social networks) and basic notions of Cyber-Security
• obtained answers to the following questions:
- **What is the purpose of CyberSecurity?**
- **How to manage security?**
- **What are the security and defense controls?**
- **What are the means to respond to security incidents?**

• understood how an attack is performed
• Reviewed the context of regional security and regulation and the specificities of the financial field (PCI DSS, mBanking, eBanking)
• reviewed ethics and standards related to Cyber Security

METHODOLOGY

Interactive seminar, Q&A

WHO SHOULD PARTICIPATE?

Directors and managers of banks, financial institutions, supervisory bodies in the areas of banking, such as IT, security, risk and compliance.
A good command of English is required!

ABOUT THE TRAINER

Hristiyan Lazarov is a seasoned cybersecurity professional with extensive experience in Incident Response and Digital Forensics. Currently, he is responsible for EMEA Digital Forensics and Incident Response operations at Deutsche Bank. Hristiyan is also part of the CERT team of Silent Breach. He successfully completed projects with global banks and organizations including American Army, McAfee, Intel Security, Iron Mountain, Raiffeisen Bank. Currently Hristiyan is a holder of prestigious industry recognized certifications CISSP, CASP, CREM, GCFA.

REGISTRATION

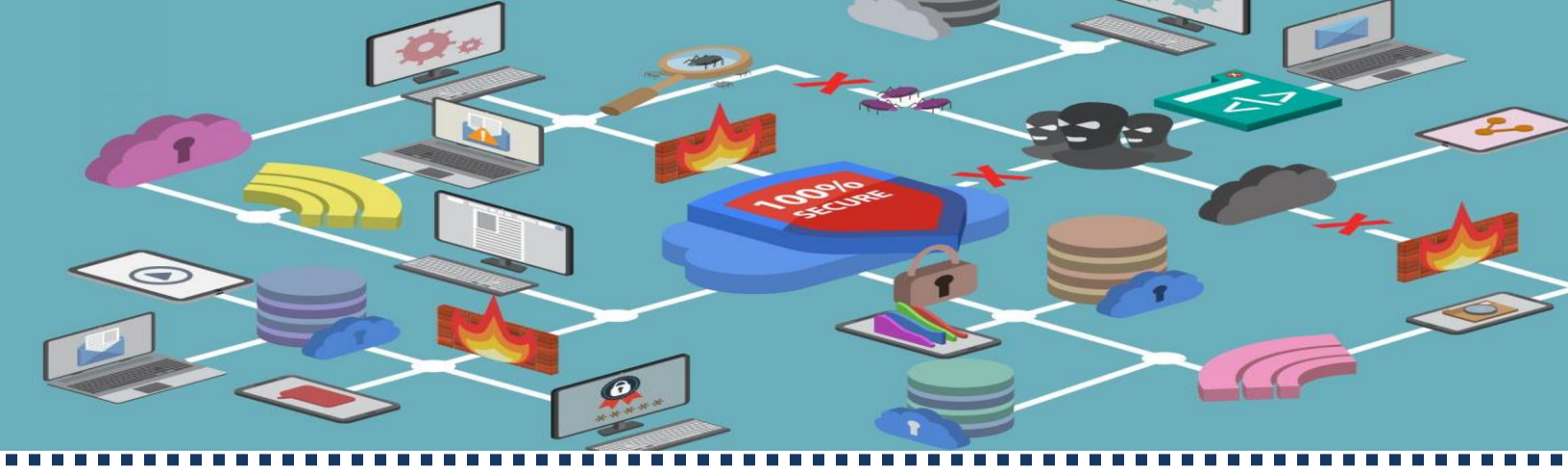
Send your filled registration forms via email at KBA, or contact us at:
kbatrainingcenter@bankassoc-kos.com or
038 246 171

DAILY SCHEDULE

09:00 – 10:30	Training
10:30 – 10:45	*Coffee break*
10:45 – 12:00	Training
12:00 – 13:00	Lunch break
13:00 – 14:30	Training
14:30 – 14:45	*Coffee break*
14:45 – 16:30	Training
16:30	*End of day ☺*

First day will start at 13.30h

Supported by
HOUSE OF TRAINING
LUXEMBOURG AID & DEVELOPMENT
ATF LUXEMBOURG



Training Content

- Presentation of House of training (1 slide)
- Presentation of Silent Breach (1 slide)
- Overview of the training course over the next couple of days
- Origins of cyber attacks
- Why do they occur?
- What are the different profiles of attackers?
- What are the different type of attacks (DDoS, data theft, ransomware, etc.)
- What is the short and long-term impact of a data breach?

- What are the counter measures of a cyber-attack?
- What is the purpose of cyber security?
- How does an organization evaluate their needs in cyber security?
- Conducting a business impact analysis
- Threat modeling and risk assessment
- Evaluating risk aversion
- Evaluating the return on investment of cyber security

- Cyber Security Governance & Compliance (PCI-DSS)
- Defining best practice security policies
- Assigning roles and responsibilities
- Planning for contingency and business continuity
- Disaster recovery planning and simulation
- Certifications (ISO 27001 and ISO 22301)

- How to mitigate risks
- Infrastructure and resources
- Determining when to best outsource cyber security (SOC)
- Penetration testing and vulnerability assessments
- User behavior and training
- Corporate policies regarding mobile, social networks, emails, passwords

- Specific challenges of the banking sector (electronic banking, mobile banking, etc.)
- Encryption and protocols
- Social hacking and its impact
- Web application security
- Questions and Answers