Balkan Cybersecurity Days

Organised in the context of the project 'Good Governance in Cybersecurity in the Western Balkans', generously supported by the United Kingdom's Foreign, Commonwealth and Development Office.

16-18 May 2023 at Hotel Unique, Ohrid, North Macedonia

Agenda

Tuesday, 16 May Conference		
TIME	**ACTIVITY**	
8:30 – 9:00	Registration and coffee	
9:00 – 9:45	**Welcome and opening remarks** **Mr. Jeton Akiku**, Director, Agency for Electronic Communications (AEK) **Mr. Mark Downes**, Deputy Director, DCAF **Dr. Serge Droz**, Vice Chair, FIRST **Ms. Slavica Grkovska**, Deputy President of the Government for Good Governance Policies **Mr. Azir Aliu**, Minister for Information Society and Administration **Mr. Andrew Brand**, Head of Programmes, British Embassy Skopje	
9:45 – 11:00	**Panel** **Best Practices in Cyber Threat Information Exchange** Cybersecurity threat information (CTI) sharing allows cybersecurity actors to improve their cyber threat prevention. Efficient CTI requires actors to be able to detect and collect CTI and find ways of sharing it with others. In this panel, we will discuss best practices in CTI exchange and the role of actors such as national CERTs in CTI. We will also talk about the importance of CTI exchange at the national, regional, and international level. **Keynote** **Chris Gibson**, Executive Director, FIRST **Discussants** • **Nadica Josifovski**, State Advisor for Information Systems and Technologies, Ministry of Information Society and Administration, North Macedonia • **Maja Lakušić**, Cyber Security Promotion Advisor, SRB-CERT, Serbia • **Michael Hamm**, Operator and Analyst at Computer Incident Response Center Luxembourg • **Paweł Pawliński**, Principal Specialist, CERT.PL, Poland *(online)* **Moderator** **Franziska Klopfer**, Principal Programme Manager, Europe and Central Asia Division, DCAF	
11:00 – 11:30	Coffee break	
11:30 – 12:30	**Conference room 1 Plenary**	**Conference room 2 Plenary**
	UN Processes and Their Impact on Incident Response Serge Droz (FIRST)	**DDoS Attacks: How Small Networks can Defend - Practical Case of Protecting a Faculty/University from DDoS** Vladislav Bidikov (Faculty of Computer Science and Engineering, MK)

12:30 – 13:30	Lunch	
13:30 – 14:30	**Incident Handling and Security Technologies for Defending Against Cyber-Attacks on Industrial IoT** Atdhe Buja / Blent Kurtalani (ICT Academy CERT, Kos)	**Python for Effective Cybersecurity: Extracting, Analyzing, and Automating Threat Detection with YARA and Open-Source Tools** Valentin Lekov / Tino Apostolovski (CPP Services)
14:30 – 15:30	**GrapheneOS Security** Matej Kovačič (SI)	**Privacy-enhancing Technologies - Where Privacy and Cybersecurity Intersect** Mickov Saso (ASEE MKD, MK)
15:30 – 15:45	Coffee break	
15:45 – 16:45	**Process of Destroying Phishing Sites** Kristijan Angelovski (CPP services)	**Cyber Intelligence and Cyber Terrorism in the Medical Field** Emanuela Dyrmishi (IT)
16:45	Closing of the Conference	
17:30 – 19:30	Social event	
20:00	Joint dinner	

DCAF Geneva Centre for Security Sector Governance

FIRST

AEK MKD-CIRT

Foreign, Commonwealth & Development Office

Wednesday, 17 May

Training Track 1 – Security Operation Center Training 1/2 *Trainers: Blaze Grashovski (Infosoft) and Aleksandar Acev* *Conference Room 1*	
TIME	**ACTIVITY**
9:00 – 10:30	**SESSION I:** Introduction to SOC operations
10:30 – 11:00	Coffee break
11:00 – 12:30	**SESSION II:** Designing the Next-Gen SOC
12:30 – 13:30	Lunch
13:30 – 14:45	**SESSION III:** Designing the Next-Gen SOC-continuing
14:45 – 15:00	Break
15:00 – 16:00	**SESSION IV**: Building the Next-Gen SOC

Training Track 2 - Introduction to Penetration Testing 1/2 *Trainers: Renato Venzin (Oneconsult) and Tobias Pohl (Oneconsult)* *Conference Room 2*	
9:00 – 10:30	**SESSION I:** Introduction to Hacking
10:30 – 11:00	Coffee break
11:00 – 12:30	**SESSION II:** Using Kali Linux
12:30 – 13:30	Lunch
13:30 – 14:45	**SESSION III:** Passive Information Gathering
14:45 – 15:00	Break
15:00 – 16:00	**SESSION IV**: Active Information Gathering

Training Track 3 – Forensics Training *Trainer: Michael Hamm, Operator and Analyst at Computer Incident Response Center Luxembourg* *Meeting Room – 1st Floor*	
9:00 – 10:30	**SESSION I:** File System Forensics
10:30 – 11:00	Coffee break
11:00 – 12:30	**SESSION II:** File system forensics – continuation
12:30 – 13:30	Lunch
13:30 – 14:45	**SESSION III:** Windows Forensics and Memory Analysis
14:45 – 15:00	Break
15:00 – 16:00	**SESSION IV**: Windows Forensics and Memory Analysis - continuation

DCAF Geneva Centre for Security Sector Governance | FIRST | AEK MKD-CIRT | Foreign, Commonwealth & Development Office

Thursday, 18 May

Training Track 1 – Security Operation Center Training 2/2 *Trainers: Blaze Grashovski (Infosoft) and Filip Simeonov (CPP)* *Conference Room 1*	
TIME	**ACTIVITY**
9:00 – 10:30	**SESSION I:** Operating the Next-Gen SOC (Team Roles and Best practices for SOC operations)
10:30 – 11:00	Coffee break
11:00 – 12:30	**SESSION II:** Operating the Next-Gen SOC (Incident Response Planning and Execution)
12:30 – 13:30	Lunch
13:30 – 14:45	**SESSION III:** Measuring SOC Effectiveness
14:45 – 15:00	Break
15:00 – 16:00	**SESSION IV:** Case Studies of Successful Next-gen SOC Operations

Training Track 2 - Introduction to Penetration Testing 2/2 *Trainers: Renato Venzin (Oneconsult) and Tobias Pohl (Oneconsult)* *Conference Room 2*	
9:00 – 10:30	**SESSION I:** Web Application Exploitation
10:30 – 11:00	Coffee break
11:00 – 12:30	**SESSION II:** Privilege Escalation
12:30 – 13:30	Lunch
13:30 – 14:45	**SESSION III:** Know your tools
14:45 – 15:00	Break
15:00 – 16:00	**SESSION IV:** Attacking Active Directory

Training Track 3 – Intro to Jupyter and Data Science for Incident Responders *Trainer: Serge Droz, FIRST* *Meeting Room – 1st Floor*	
9:00 – 10:30	**SESSION I**
10:30 – 11:00	Coffee break
11:00 – 12:30	**SESSION II**
12:30 – 13:30	Lunch