MONDAY 4 DE JUNIO

FORUMS – Room 3

8:00 - 9:00	**REGISTRY**	
9:00 – 9:30	**Welcoming Session**	
	Ministry of Modernization	
	UNLP	
	International Telecommunications Union	Pablo Palacios
9:30 - 09:35	**PHOTO AND SHORT BREAKE**	
9:35 - 10:50	**Awareness Session**	
	Cybersecurity at decision taken level: Critical Infrastructure	ITC – Eduardo Cardozo
10:50 - 11:20	**Positive Technologies Security - Dan Tara**	
	Myths and reality about SS7/LTE networks security. Attacks on Critical National Infrastructure through Mobile carriers.	
11:20 - 11:40	**COFFEE BREAKE**	
11:40 - 13:00	**Discussion Table:** Cybersecurity and the Public Sector	
	Moderator: UNLP	Lia Molinari
	Ministry of Modernization	Hugo Miguel
	Boss of Advisors of the Secretary of Digital Country	Eduardo Martino
	Advisor Sub secretary Cyberdefence of Ministry of Defence	Leandro de la Colina
	Ministry of Security	Pedro Janices
	ISOC	Shernon Osepa
13:00 - 14:00	**LUNCH BREAKE**	
14:00 - 15:30	**Discussion Table:** Cybersecurity in the Private and Finance Sector s	
	Moderator: ISOC	Shernon Osepa
	ROFEX	Pablo Milano
	Central Bank of the Nation Argentina	Gustavo Pereyra
	Central Bank of the Nation Argentina	Marcela Pallero
	CSIRT Prisma Medios de Pago	Lucas Coronel
	International Telecommunications Union	Marwan Ben Rached
15:30 - 16:00	**COFFEE BREAKE**	
16:00 - 17:00	**Discussion Table:** Academy and Cybersecurity	
	Moderador: Secretary of Digital Country	Eduardo Martino
	Universidad Nacional de La Plata	Javier Díaz
	Universidad de Buenos Aires	Raúl Saroka
	FIRST	Jacomo Piccolini
	ITC Uruguay	Eduardo Carozo
17:00 - 17:30	**CLOSING SESSION**	
	Ministry of Modernization	
	UNLP	
	International Telecommunications Union	Pablo Palacios
19:00 -21:00	**SOCIAL ACTIVITY: Cocktail at Senado of Buenos Aires province**	

TUESDAY 5 JUNE

TECHNICAL TRAINING – Room 106

Capacity: 30 to 50 attendees

08:00 - 09:00	**REGISTRY**
09:00 - 10:30	**Technical Training 1:** Positive Technologies Security - Dmitry Kurbatov & Dan Tara
	Signaling security Workshop & Live-Demo of attacks on the SS7 network - History and Development of security in signaling networks (SS7/Diameter/GTP)
10:30 - 11:00	**COFFEE BREAKE**
11:00 - 13:00	**Technical Training 2:** Positive Technologies Security - Dmitry Kurbatov & Dan Tara
	Signaling security Workshop & Live-Demo of attacks on the SS7 network - Building a full scale signaling security process inside operators and regulation required to support it
	DEMO
13:00 - 14:00	**LUNCH BREAKE**
14:00 - 15:30	**Technical Training 3:** CYBR Score Comtech Telecommunications
	Cyber Defense Analyst (CDA) and lab Training: Protocol Analysis (CDA); Intrusion Detection (CDA); Incident Handling Methodology (CDA); Network Defense Analysis (CDA); Network Attack Analysis (CDA); Intelligence Gathering (VAM); Attack (VAM); Defend (VAM).
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 4:** CYBR Score Comtech Telecommunications
	Cyber Defense Analyst (CDA) and lab Training: Protocol Analysis (CDA); Intrusion Detection (CDA); Incident Handling Methodology (CDA); Network Defense Analysis (CDA); Network Attack Analysis (CDA); Intelligence Gathering (VAM); Attack (VAM); Defend (VAM).
19:00 - 20:00	**SOCIAL ACTIVITY: Visit to the Planetary UNLP**

TUESDAY 5 JUNE

TECHNICAL TRAINING – Room 107

Capacity: 30 to 50 attendees

08:00 - 09:00	**REGISTRY**
09:00 - 10:30	**Technical Training 5:** ITC Uruguay – Eduardo Carozo & Leonardo Vidal
	Cybersecurity and Internet of Things
10:30 - 11:00	**COFFEE BREAKE**
11:00 - 12:30	**Technical Training 6:** ITC Uruguay – Eduardo Carozo & Leonardo Vidal
	Cybersecurity and Smart Cities
13:00 - 14:00	**LUNCH BREAKE**
14:00 - 15:30	**Technical Training 7:** Silensec - Almerindo Graziano
	Threat Intelligence
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 8:** International Telecommunication Union - Marwan Ben Rached
	Cybersecurity at Financial Systems
17:30 - 18:30	**ONLY FOR CYBERDRILL TEAMS**
	Preparation Session: CyberServices - Csaba Virág
	CyberDrill Preparation Session
19:00 - 20:00	**SOCIAL ACTIVITY: Visit to the Planetary UNLP**

TUESDAY 5 JUNE

TECHNICAL TRAINING FIRST – Room 108

Training title: Building threat Intel pipelines.

Course level: Intermediate.

Expert: Paweł Pawliński – CERT Polonia

Paweł Pawliński is a principal specialist at CERT.PL. His past job experience include data analysis, threat tracking and automation. He is responsible for the design and implementation of the n6 platform for sharing security-related data and designed systems for large-scale monitoring of attacks on the internet. Paweł is an author of publications and trainings, with the focus the collection, analysis and exchange of information by CSIRTs.

Capacity: 30 attendees.

Pre- requisites:

1. Participants should be familiar with the operational aspects of CSIRTs/SOCs, including incident handling, analysis and mitigation. In particular, a good understanding of IoCs and other types of information used for network defense is crucial;
2. Software/hardware requirements: laptop, details TBA;
3. The hands-on part will require a laptop with a recent version of VirtualBox (virtualbox.org) and capable of running a VM with 4G of RAM and 20G disk. Alternatively, participants will be able to use their own Linux systems directly, as long as they have docker and docker-compose installed.

Abstract:

The course covers the design of processes to effectively handle variety of information useful for security operations. Participants will learn how to select sources of information and how to process it to obtain actionable conclusions. Issues related to the evaluation, collection, analysis and exchange of information will be explained. The training includes a hands-on practical part, which will introduce several open source tools for handling threat intelligence and incident-related data.

08:00 – 09:00	**REGISTRY**
09:00 - 10:30	**Technical Training 9:** Introduction of the main concepts
10:30 - 11:00	**COFFEE BREAKE**
11:00 - 12:30	**Technical Training 10:** Evaluation of information sources, collection, preparation and storage of data
12:30 - 14:00	**LUNCH BREAKE**
14:00 - 15:30	**Technical Training 11:** Toolset showcase: MISP, Intel MQ, The Hive
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 12:** Toolset showcase: MISP, Intel MQ, The Hive
19:00 - 20:00	**SOCIAL ACTIVITY: Visit to the Planetary UNLP**

TUESDAY 5 JUNE

CHILD ONLINE PROTECTION AND TECHNICAL TRAINING – Room 109

Capacity: 50 to 80 attendees

AWARNESS TO THEYOUTH ABOUT CHILD ONLINE PROTECTION	
08:00 – 09:00	**REGISTRY**
09:00 - 12:00	**UNLP** Handling Social Networks and Cyberbullying. Experiences
	ICMEC - Pilar Ramirez Child pornography, grooming, sexting y sextortion, definitions and legal aspects
	Ministry of Modernization Government and its actions
	Fundación REDES Violencia Digital
	ITU - Pablo Palacios "Child Online Protection" – General Considerations
13:00 – 14:00	**REGISTRY**
14:00 - 15:30	**Technical Training 13:** ADACSI
	Government and management of security, norms, standards and best practices on Cybersecurity
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 14:** Professional Council of Computer Science of the Province of Buenos Aires – CAPA8 - (TBC)
	Government and management of Security: The role of professionals on Cbersecurity
19:00 - 20:00	**SOCIAL ACTIVITY: Visit to the Planetary UNLP**

WEDNESDAY 6 JUNE

TECHNICAL TRAINING – Room 106

Capacity: 50 attendees

08:00 – 09:00	**REGISTRY**
09:00 - 10:30	**Technical Training 15:** Kaspersky - Andres Giarletta
	Parcheo de Capa 8
10:30 - 11:00	**COFFEE BREAKE**
11:00 - 12:30	**Technical Training 16:** Kaspersky - Santiago Pontirolli
	Local Threats, global problem. Argentina and the panorama of current threats – local view and the threats that affect Argentina and Latin America
12:30 - 14:00	**LUNCH BREAKE**
14:00 - 15:30	**Technical Training 17:** Deloitte - Julio Ardita
	Attacking Payment Application Development Companies
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 18:** Deloitte - Julio Ardita
	Cyber-Resilience in Organizations

WEDNESDAY 6 JUNE

TECHNICAL TRAINING - Room 107

Capacity: 30 to 50 attendees

08:00 - 09:00	**REGISTRY**
09:00 - 10:30	**Technical Training 19:** CyberServices , Csaba Virág
	Ransomware incident response
10:30 - 11:00	**COFFEE BREAKE**
11:00 - 12:30	**Technical Training 20:** International Telecommunication Union - Marwan Ben Rached
	Proactive Detection of Cybersecurity Incidents – Honeypots / Build a CIRT based on Open source tools
12:30 - 14:00	**LUNCH BREAKE**
14:00 - 15:30	**Technical Training 21:** ISOC Cybersecurity SIG - Julio Balderrama
	Ensuring critical infrastructure, the big challenge
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 22:** VHGroup - Emiliano Piscitelli
	Social Engineering - Hacking & Hardening HumanOS

WEDNESDAY 6 JUNE

TECHNICAL TRAINING FIRST – Room 108

Training title: Building threat Intel pipelines.

Course level: Intermediate.

Expert: Paweł Pawliński – CERT Polonia.

Paweł Pawliński is a principal specialist at CERT.PL. His past job experience include data analysis, threat tracking and automation. He is responsible for the design and implementation of the n6 platform for sharing security-related data and designed systems for large-scale monitoring of attacks on the Internet. Paweł is an author of publications and trainings, with the focus the collection, analysis and exchange of information by CSIRTs.

Capacity: 30 attendees.

Pre- requisites:

1. Participants should be familiar with the operational aspects of CSIRTs/SOCs, including incident handling, analysis and mitigation. In particular, a good understanding of IoCs and other types of information used for network defense is crucial;
2. Software/hardware requirements: laptop, details TBA;
3. The hands-on part will require a laptop with a recent version of VirtualBox (virtualbox.org) and capable of running a VM with 4G of RAM and 20G disk. Alternatively, participants will be able to use their own Linux systems directly, as long as they have docker and docker-compose installed.

Abstract:

The course covers the design of processes to effectively handle variety of information useful for security operations. Participants will learn how to select sources of information and how to process it to obtain actionable conclusions. Issues related to the evaluation, collection, analysis and exchange of information will be explained. The training includes a hands-on practical part, which will introduce several open source tools for handling threat intelligence and incident-related data.

08:00 – 09:00	**REGISTRY**
09:00 - 10:30	**Technical Training 23:** Data analysis, including fusion of information from multiple sources
10:30 - 11:00	**COFFEE BREAKE**
11:00 - 12:30	**Technical Training 24:** Practical aspects of the information exchange
12:30 - 14:00	**LUNCH BREAKE**
14:00 - 15:30	**Technical Training 25:** Automating typical tasks using open source tools
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 26:** Automating typical tasks using open source tools

WEDNESDAY 6 JUNE

TECHNICAL TRAINING - ISOC – Room 109

Capacity: 30 to 50 attendees

08:00 - 09:00	**REGISTRY**
09:00 - 10:30	**Technical Training 27:** ISOC
	Work of ISOC on Cybersecurity, projects in the Region
10:30 - 11:00	**COFFEE BREAKE**
11:00 - 12:30	**Technical Training 28:** ISOC
	Cybersecurity and Internet of Things
12:30 - 14:00	**LUNCH BREAKE**
14:00 - 15:30	**Technical Training 29:** ISOC
	Mutual agreement on Norms and Routing Security
15:30 - 16:00	**COFFEE BREAKE**
16:00 - 17:30	**Technical Training 30:** ISOC
	Cybersecurity on Wireless Community Networks

THURSDAY 7 JUNE

CYBERDRILL - Room 205

Capacity: 60 attendees.

Room shape: Distribution in "U" shape.

Technical Scenarios:

1. Unión Internacional de Telecomunicaciones;
2. Silensec;
3. CyberServices;
4. Universidad Nacional de La Plata;
5. Comtechtel (CyberScore).

Management Scenarios:

6. Kaspersky;
7. Deloitte.

8:00 - 8:30	**REGISTRY**
8:30 - 9:00	**Introduction:** International Telecommunications Union - Pablo Palacios / Marwan Ben Rached
	Introduction to the scenarios for the Cyberdrill
9:00 - 10:30	**Scenario 1:** Silensec - Almerindo Graziano
	Threat intelligence using YARA rules
10:30 - 11:00	**COFFEE BREAKE**
11:00 – 12:30	**Scenario 2:** National University of La Plata, Argentina - Einar Felipe Lanfranco
	Analysis of a cryptocurrency mining malware
12:30 - 13:30	**LUNCH BREAKE**
13:30 - 15:00	**Scenario 3:** Deloitte - Francesco Binaschi
	Cyber Crisis Management
15:00 - 15:30	**COFFEE BREAKE**
15:30 - 18:00	**Scenario 4:** Kaspersky
	Business simulation for a large bank with retail and B2B business and own ATM network. Kaspersky Interactive Protection Simulation (KIPS)

FRIDAY 8 JUNE

CYBERDRILL - Room 205

Capacity: 60 attendees.

Room shape: Distribution in "U" shape.

Technical Scenarios:

1. Unión Internacional de Telecomunicaciones;
2. Silensec;
3. CyberServices;
4. Universidad Nacional de La Plata;
5. Comtechtel (CyberScore).

Management Scenarios:

6. Kaspersky;
7. Deloitte.

9:00 - 11:00	**Scenario 5:** International Telecommunications Union – Marwan Ben Rached
	Online credit card skimming
11:00 - 11:30	**COFFEE BREAKE**
11:30 - 13:00	**Scenario 6:** CyberServices – Csaba Virág
	Ransomware Analysis
13:00 - 14:00	**LUNCH BREAKE**
14:00 - 16:30	**Scenario 7:** Comtech Telecommunications Corp - Alan Gush & Phillip Stoner
	CTF Challenge
16:30 - 17:00	Wrap-up and closing remarks
17:00 - 17:30	**COFFEE BREAKE**