NATIONAL CYBER EXERCISES IN **GEORGIA**

MIROSŁAW MAJ
PIOTR SZEPTYŃSKI
MACIEJ PYZNAR

CYBERSECURITY FOUNDATION
ComCERT.PL

FUNDED BY THE EU

EU-Georgia
e-Governance
Facility Project


cyberspace
security
FOUNDATION


comCERT

IMPROVING CERT CAPABILITIES

- NETWORK MONITORING
- TRAININGS FOR THE CONSTITUENCY
- JOINING INTERNATIONAL FORAS (FIRST)
- BUIILDING CYBERSECURITY COMMUNITY
- SITE VISIT (SWICH CERT)

FUNDED BY THE EU

EU-Georgia e-Governance Facility Project

PREPARATIONS

CYBER-EXE POLSKA 2013

CYBER-EXE POLSKA 2012

PARTICIPANTS

- 14 TEAMS
  - Bank of Georgia
  - Cyber Security Bureau
  - Education Management Information System
  - Free University of Tbilisi
  - Georgian Research and Educational Network Association GRENA
  - MagtiCom
  - Ministry of Finance of Georgia
  - Ministry of Internal Affairs
  - Ministry of Labour Health and Social Affairs of Georgia
  - National Public Registry
  - Public Service Development Agency
  - Smart Logic
  - State Chancellery
  - VTB Bank

ORGANIZERS

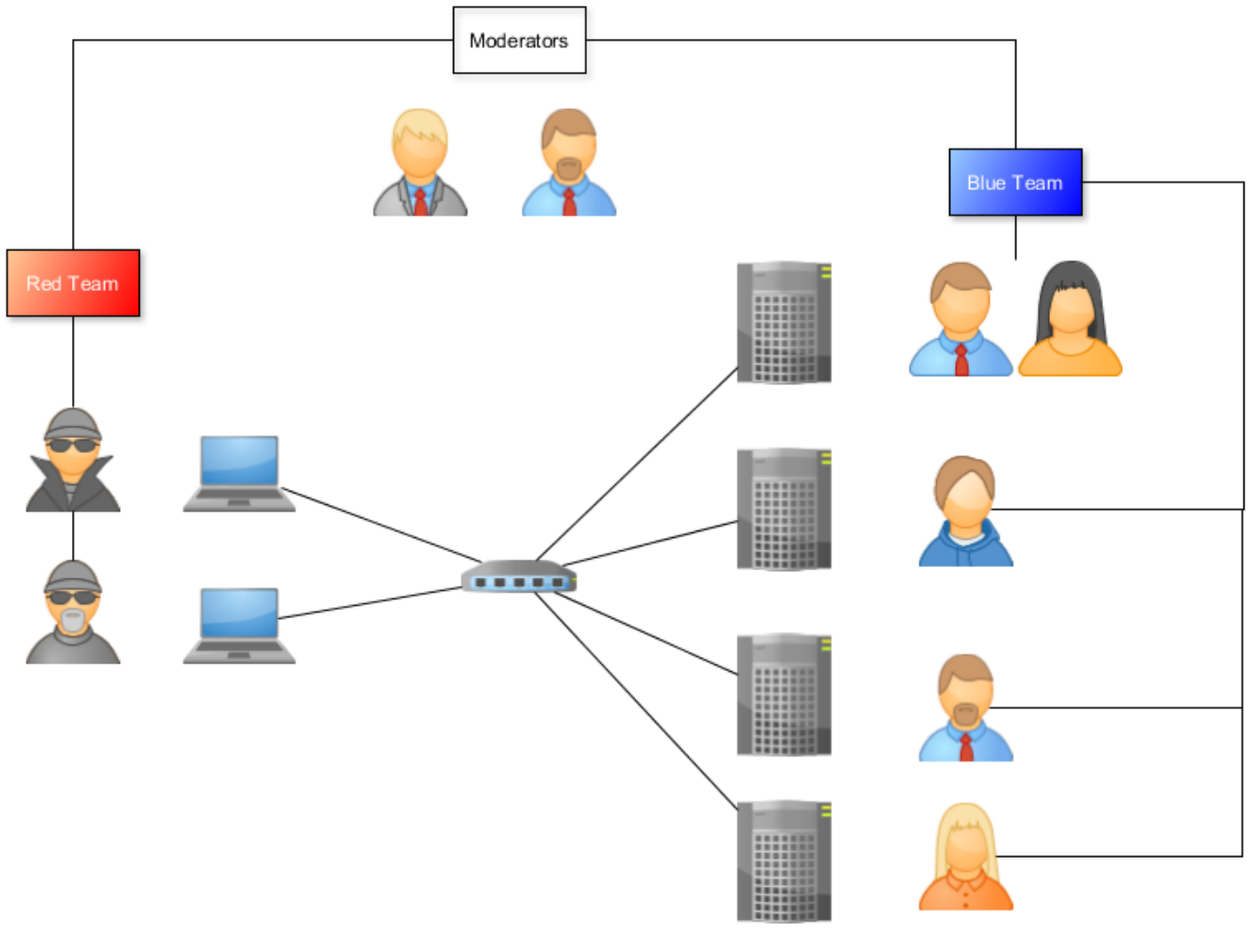
- DATA EXCHANGE AGENCY
- CERT.GOV.GE
- CYBERSECURITY FOUNDATION / ComCERT.PL
- 7 PERSONS
  - MAIN MODERATOR (1)
  - EVALUATOR (1)
  - RED TEAM TECHNICAL COORDINATOR (1)
  - RED TEAM TECHNICAL SUPPORT (2)
  - INFRASTRUCTURE COORDINATOR (1)

FUNDED BY THE EU

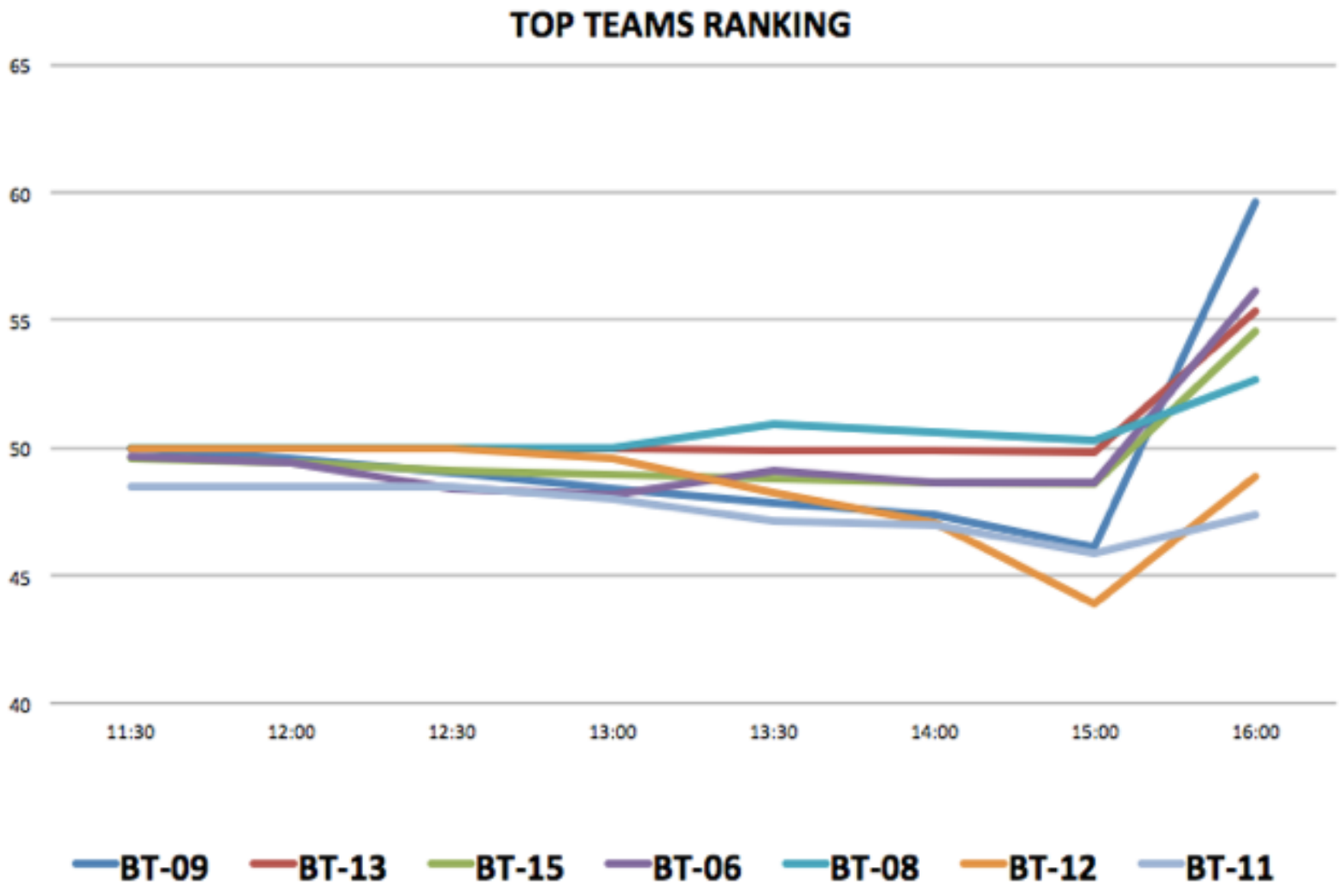
EU-Georgia e-Governance Facility Project

SCHEMA

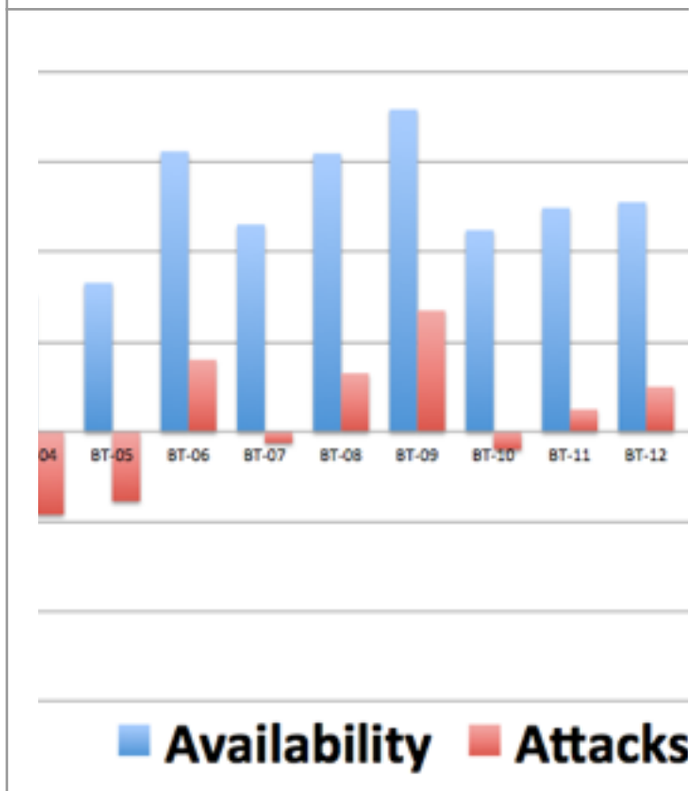
- SERVERS WITH SERVICES MUST BE PROTECTED BY BLUE TEAMS
- THEY ARE ATTACK BY RED TEAM (ORGANIZERS)
  WE DO NOT TEACH TO ATTACK!
- THERE ARE TWO MEASURES
  - AVAILABILITY
  - VULNERABILITY RESILLIENCE (ATTACKS)

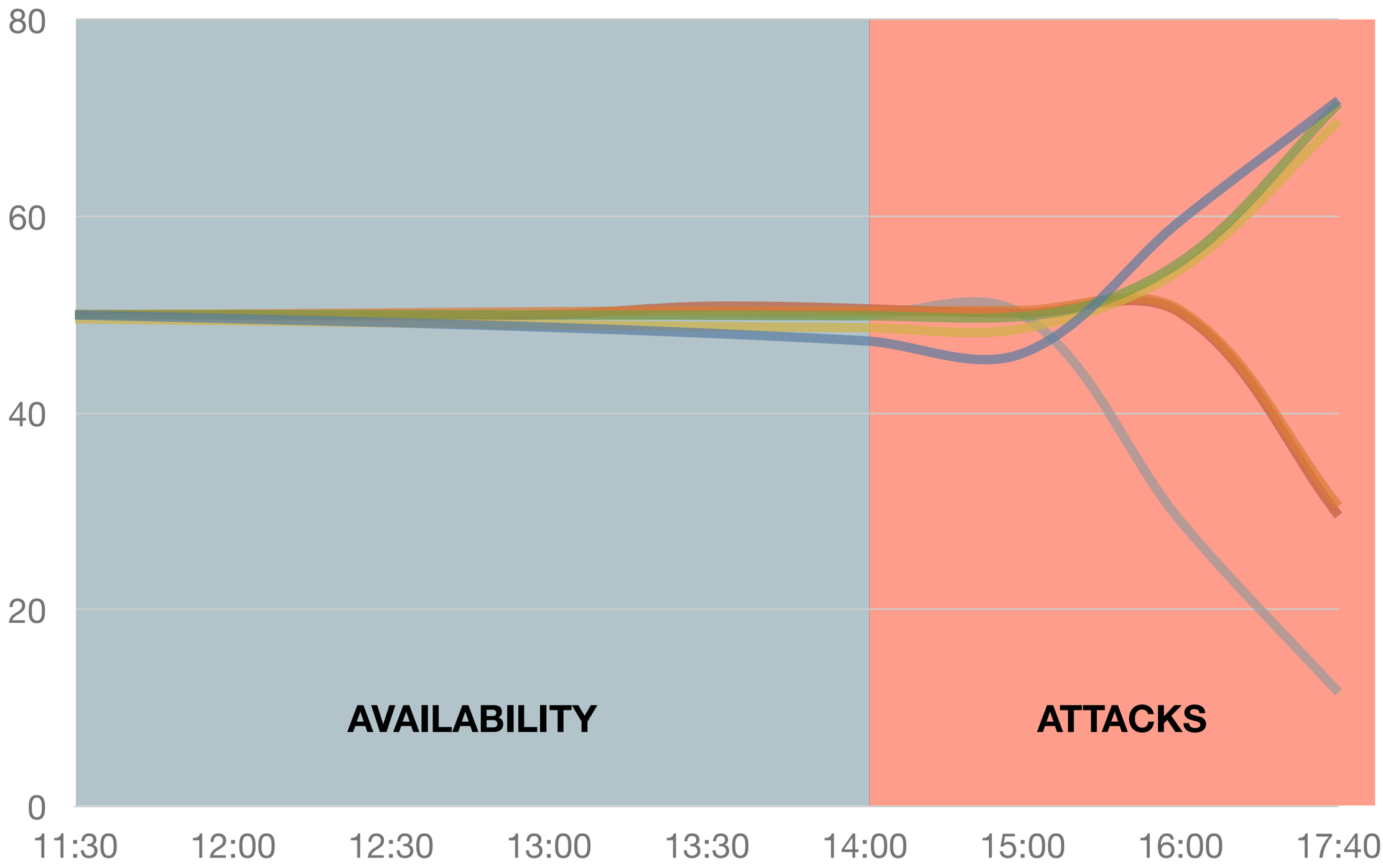


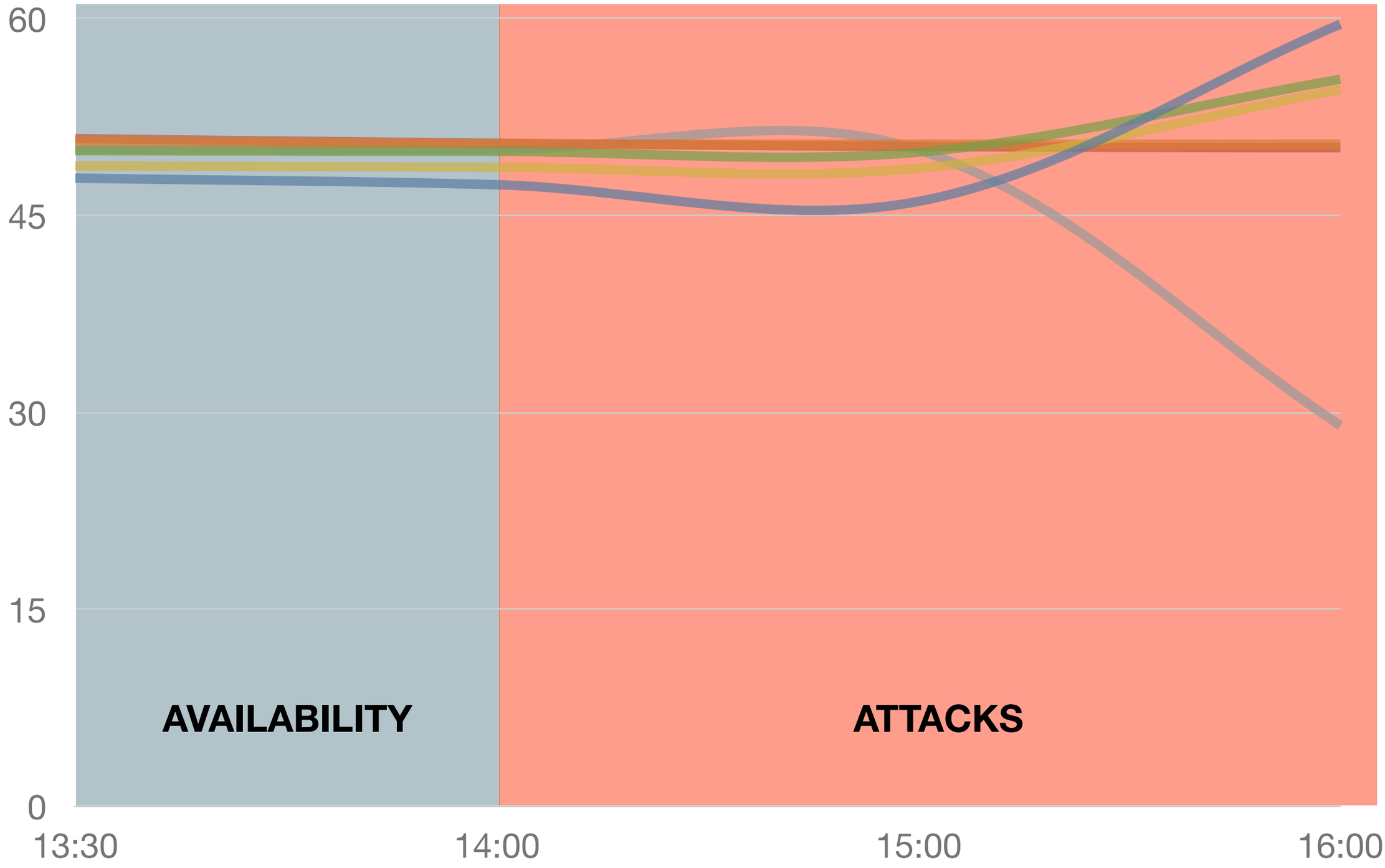
SCOREBOARD



	Team	
1	**BT-09**	71,81
2	**BT-13**	71,48
3	**BT-15**	69,68
4	**BT-06**	62,44
5	**BT-08**	61,98
6	**BT-12**	51,09
7	**BT-11**	49,85
8	**BT-05**	48,66
9	**BT-07**	46,14
10	**BT-10**	44,86
11	**BT-01**	36,36
12	**BT-04**	30,51
13	**BT-02**	29,56
14	**BT-16**	11,57




80
60
40
20
0
AVAILABILITY
ATTACKS
11:30
12:00
12:30
13:00
13:30
14:00
15:00
16:00
17:40


60
45
30
15
0
AVAILABILITY
ATTACKS
13:30
14:00
15:00
16:00

APACHE

DISTCCD

FTP

BIND

DRB

INGERSLOCK

MYSQL

PGSQL

IRCD

NFS

PHP-1

POSTFIX

RMI

PHP-2

RLOGIN

SMB-1

TIKIWIKI

VNC

SMB-2

TOMCAT

goodprotection

- TIKIWIKI
- PHP-1
- SMB-2
- PGSQL
- MYSQL
- SMB-1
- TOMCAT
- PHP-2
- RMI
- NFS

badprotection

- DRB
- DISTCCD
- POSTFIX
- IRCD
- BIND
- VNC
- RLOGIN
- INGERSLOCK
- FTP
- APACHE

BEFORE YOU TAKE YOUR DIPLOMA

- GET YOUR TEAM
- EVALUATE YOUR RESOURCES
- ORGANIZE YOUR ENVIRONMENT
- RESPECT ATTACKERS
- GET YOUR STRATEGY
- INVOLVE COOPERATION
- AQUIRE A SUPPORT

დიდი მადლობა

miroslaw.**maj**@cybsecurity.org
piotr.**szeptynski**@cybsecurity.org
maciej.**pyznar**@cybsecurity.org