European Commission

Joint Research Centre

The European Commission's in-house science service

www.jrc.ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation

European Commission

On the use of emulation test-beds for increasing the realism of operational cyber exercises

T. Benoist, C. Siaterlis, A. Pérez García

Overview

1. Test-beds for CE
   a. Rationale
   b. methodology
   c. Benefits for CEs
   d. EPIC

2. Driving Cyber Exercises: EXITO
   a. Requirements
   b. Architecture
   c. Features

Rationale

- Support the paradigm shift towards more operational CEs
- Increase realism of operational CEs by embedding a technical dimension into storylines
- Increase players situational awareness
- Collect additional Exercise feedback

Methodology

- An environment for the exercise is realistically recreated on the test-bed, i.e. without using operational systems.
- The environment shall reproduce data and PSTN networks.
- Players are given access to the environment from remote locations
- The environment shall be strictly confined (e.g. phone calls, player actions, etc)
- Environment subject to scripted events and real-time interaction.
- Detailed exercise logs are stored in data repositories.

Benefits

- During the preparation phase:
  - Test various crisis scenarii/timelines
    e.g. conception of competitive (e.g. Red vs Blue team) and collaborative scenari
  - Test conceptual & technical procedures
  - Test mitigation strategies
  - ➔ Helps evaluating and writing sound realistic storylines

- During the exercise:
  - Real-time monitoring of the exercise (e.g. Zabbix)
  - Real-time monitoring of players (phone logs, players' log)
  - Provides exercise moderators with additional information to steer the storyline

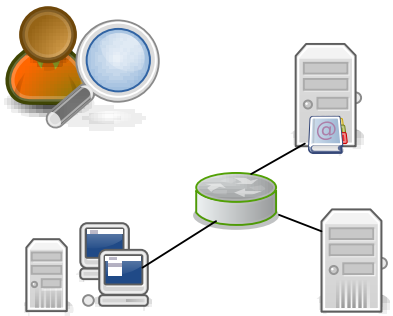
Benefits

- After the exercise:
  - Additional feedback through exercise intelligence reporting
  - Possibility to replay the exercise
  - Possibility to reuse exercise topologies

➔ useful to write lessons-learnt, improve procedures, convert previous exercise topologies into training material, etc.

How?

Traditional

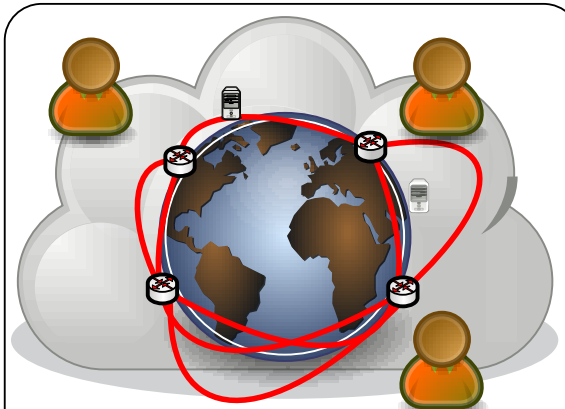


Ad-hoc testbeds

Simulators

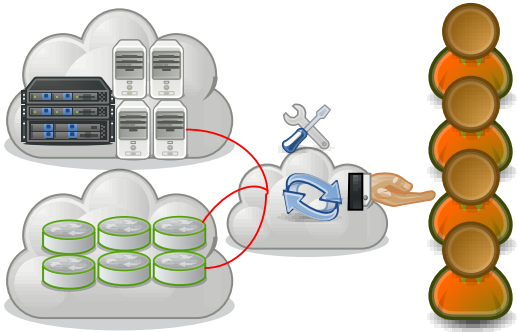
EPIC

Recent



Overlay testbeds

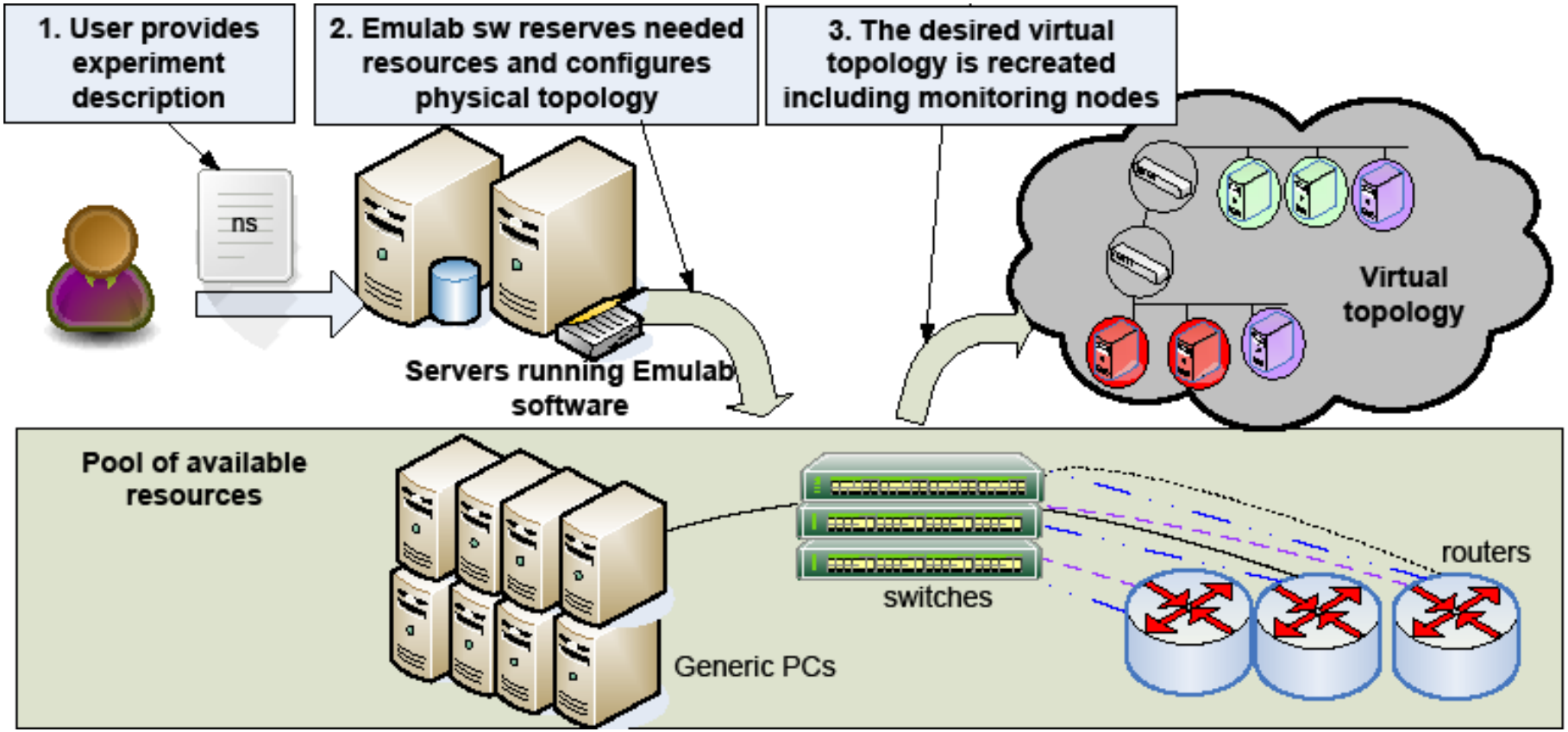
(on top of existing infrastructures)



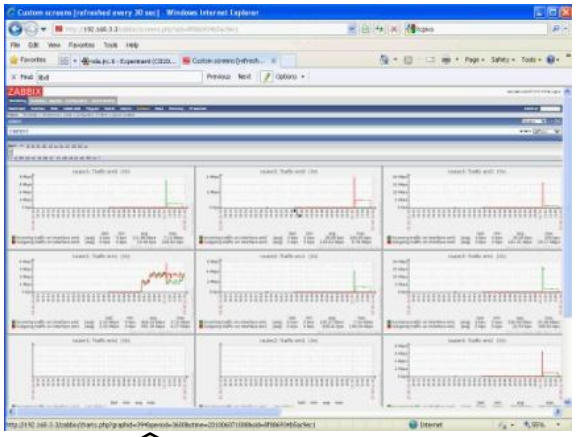
Emulation testbeds

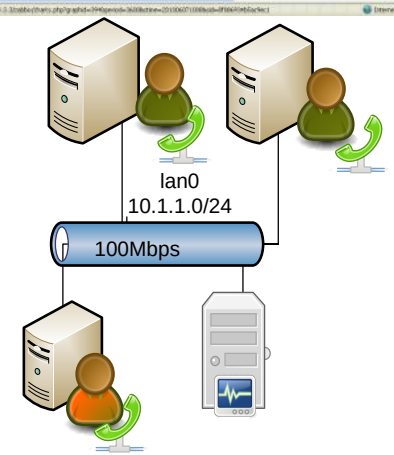
(dedicated physical resources)

EPIC

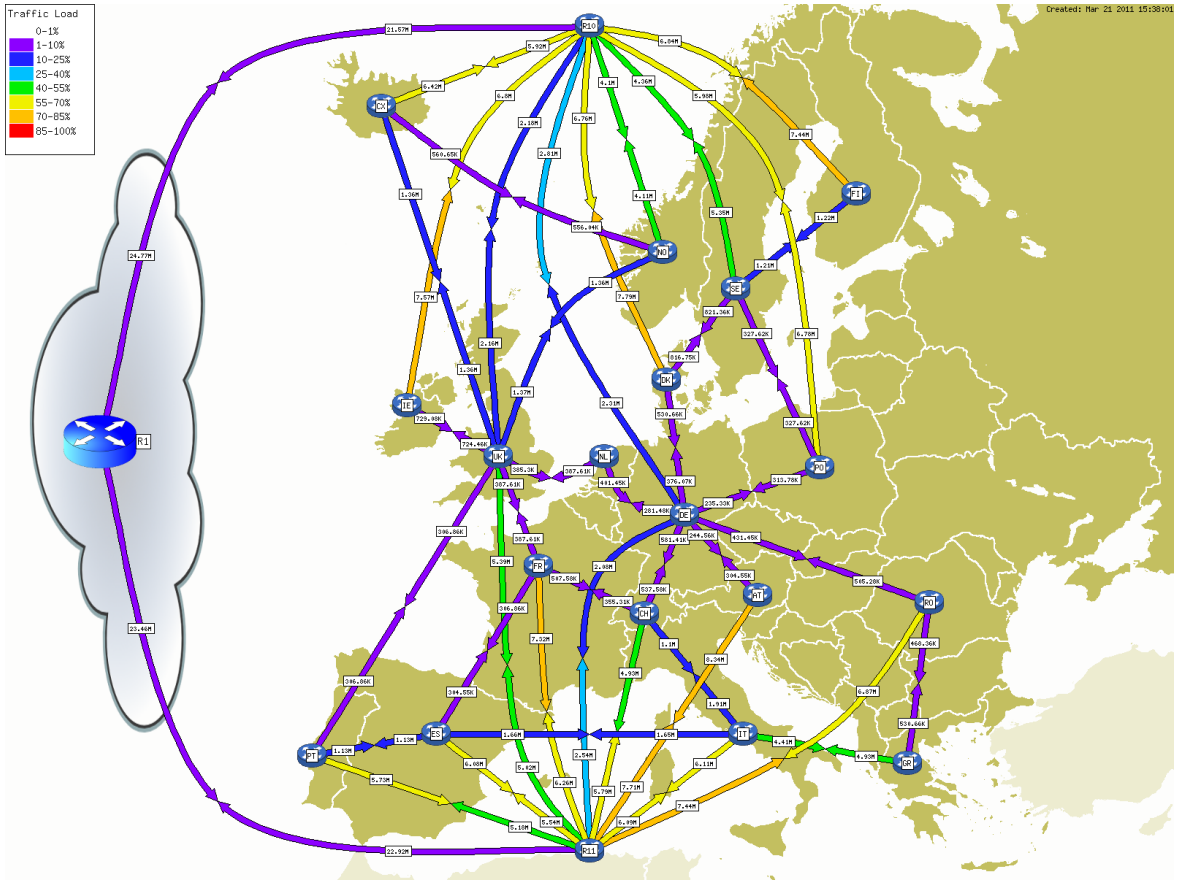

1. User provides experiment description
2. Emulab sw reserves needed resources and configures physical topology
3. The desired virtual topology is recreated including monitoring nodes
ns
Servers running Emulab software
Virtual topology
Pool of available resources
switches
routers
Generic PCs

EPIC Example: BGP MiM attack





Voice communications / PSTN



Overview

1. Test-beds for CE
   a. Rationale
   b. methodology
   c. Benefits for CEs
   d. EPIC

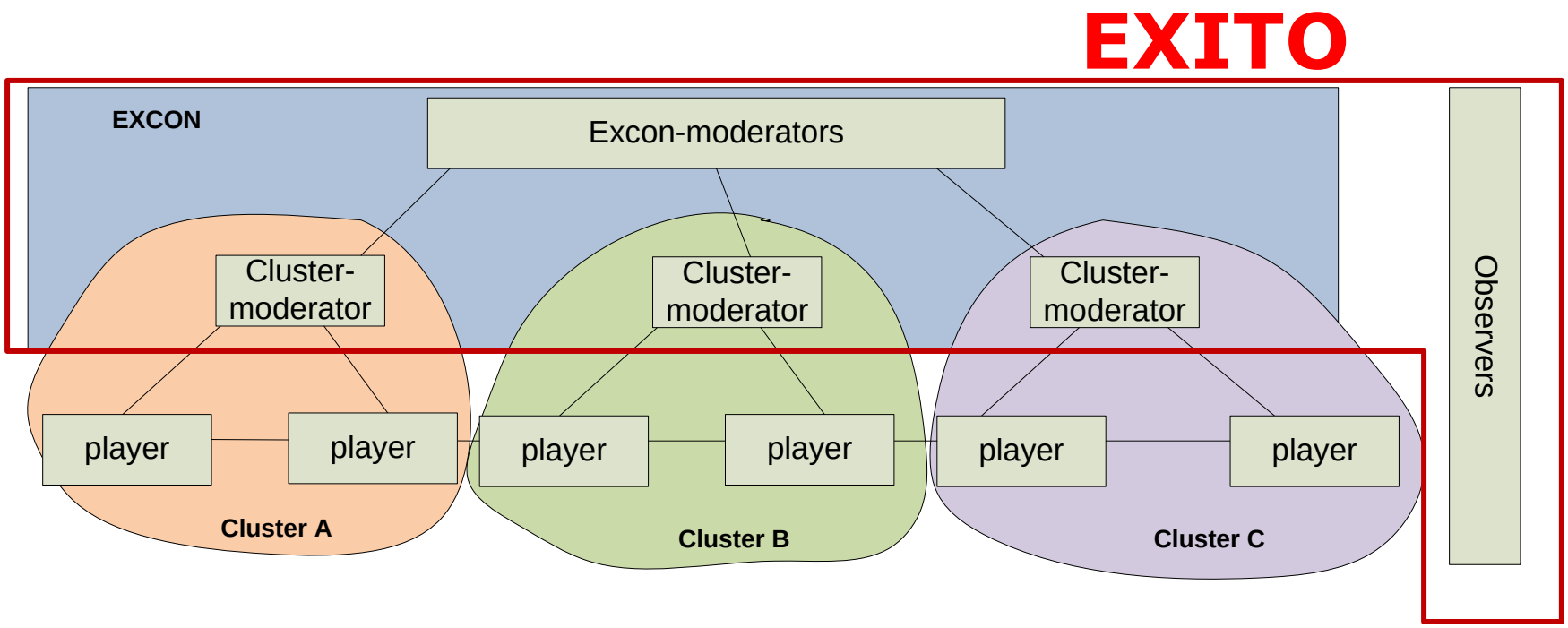
2. Driving Cyber Exercises: EXITO
   a. Requirements
   b. Architecture
   c. Features

Requirements for EXITO

The Exercise event Injection Toolkit shall ***"Facilitate large scale distributed exercise playing though event injection and data collection"***

- Need to organize exercise stakeholders across various roles
- Maintenance of a MaSter Event List (MSEL) representing the scenario
- Scenario control
  - what event from the MSEL is injected and when
  - Keep track of past events
- Event Management - what happens when an event is injected
- Feedback collection platform

Architecture: hierarchical model



- EXCON: centralized location for overall management
- Clusters: independent and parallel groups
- Cluster-moderator: manages a single cluster's participation

Events

- The scenario is composed of **events**
- Events have a set of attributes:
  - injection_offset: from the exercise start time in minutes
  - group_id: in order to group events for bulk injection
  - type: Exercise related, CERT, International Media, Intelligence, CIIP Incident, Law Enforcement
  - necessity: Mandatory, Optional
  - cluster: cluster identification or ALL
  - sender: supposed sender of the event within the exercise scenario
  - recipient: intended players for this event
  - title
  - description
  - attachment

Offset	Group_id	Type	Necessity	Cluster	Sender	Recipient	Title	Description	attachment
0	1	Exercise related	Mandatory	ALL	EXCON	All players	Beginning of exercise	Good afternoon, this is an EXERCISE! The mechanism for the …	File.pdf

Features - Data & Data Access Rights

- **MSEL**

Full list of scenario events

Ideally designed and set up before the exercise

Managed and visible only by the EXCON-moderators

Table: master_list

Edit	View	Inject	group	offset	injection_time	country	type	sender	recipient	title	attachment
			1	0	2010-11-04 10:00:00	ALL	Intelligence	Undercover agent	Intelligence agency	Attack threat very high	master_list.pdf
			2	10	2010-11-04 10:10:00	ALL	Exercise related	EXCON	All	End of Phase 1, start of phase 2	
			3	20	2010-11-04 10:20:00	ALL	CIIP Incident	Incident Handling Officer from IIS Operator	Crisis cell	Incident 1 at IIS	
			4	30	2010-11-04 10:30:00	ALL	CERT	EXCON	CERT	Results of first analysis delayed	
			5	40	2010-11-04 10:40:00	ALL	Law Enforcement	Team deployed at HQ	Law Enforcement agency	First results from investigation at sensitive server	
			6	50	2010-11-04 10:50:00	ALL	International Media	Europe News	Watch center	Announcement of the list of countries involved	

pages

- **Event List**

Contains events injected during the exercise

Limited views for Cluster-moderators (only own events)

Table: event_list

Edit	View	Delete	Mail	type	sender	recipient_list	country	injection_time	title	attachment
				Exercise related	EXCON	All	ALL	2010-11-17 16:23:28	End of Phase 1, start of phase 2	
				Intelligence	Undercover agent	Intelligence agency	ALL	2010-11-17 16:23:25	Attack threat very high	master_list.pdf

pages

- **Feedback repository**

Includes the status reports generated by the Cluster-moderators

Limited views for Cluster-moderators (only own reports)

Full access for EXCON-moderators

Main source for post analysis

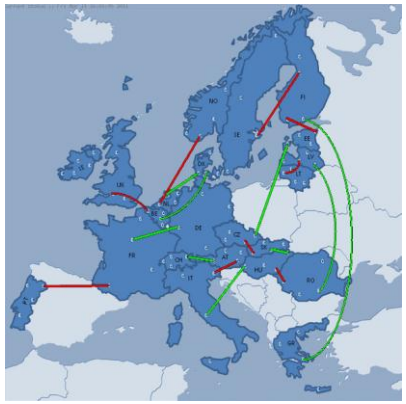
Table: status_list

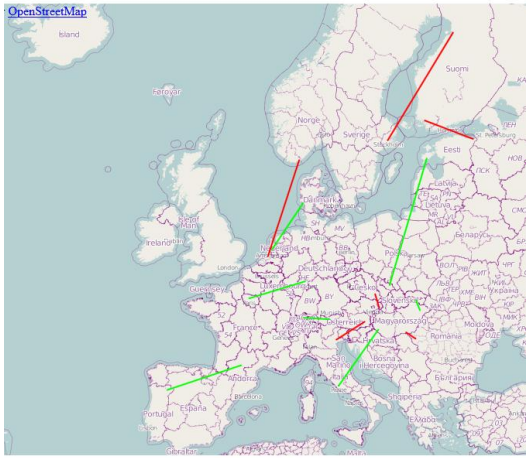
Edit	Clone	View	Delete	country	situation2date	actions2date	assessment	issues	created
				drupal	What has happened since last status report, in chronological order: inputs, events, etc, e.g. 3/4 links down. Traffic to country X has been rerouted through Y.	What has been done since last status report, in chronological order, e.g. Traffic related actions: I have asked player x to reroute traffic / Player x has requested from me to reroute traffic. Information requests: I have requested from player x the following info / Player x has requested the following info from me. Information dissemination: I have provided to player x the following info / Player x has provided the following info to me.	No issue	Is the exercise progressing smoothly or should EXCON intervene? e.g. questions, misconceptions from players, clarifications made, problems of scenario.	2010-11-17 15:40:04

pages

Joint Research Centre

Features - Exercise map

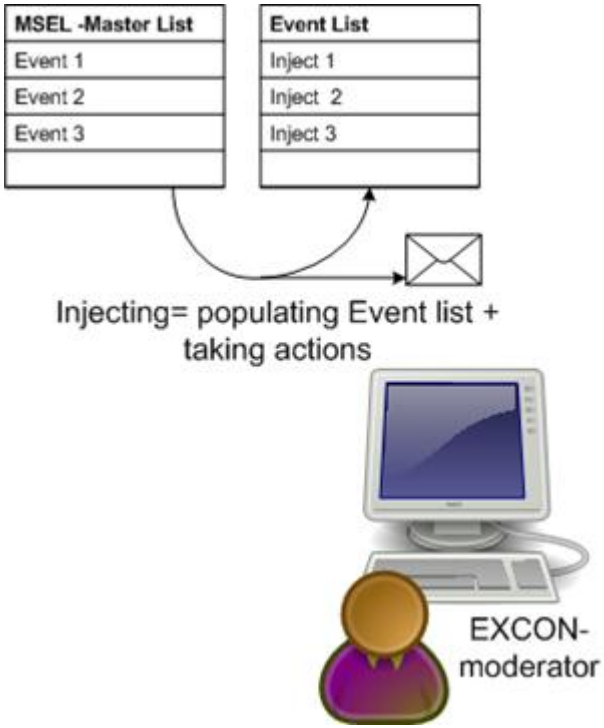




- Provides visual information of the exercise topology
- Managed and updated by the EXCON-moderators
- Typically not visible for Players (but possible)
- Consists of three elements:
  - The background image
  - The Information eXchange Points (IXP)
  - The links between IXP
- Supports WeatherMap, KML, OpenLayers

Information flows: Injection of Events

- Executed by the EXCON-moderators
- Events are copied from the MSEL to the Event list
- Accompanied with one or more actions:
  - mail to the Cluster-moderators
  - Exercise map update
  - 3rd Party RESTful Webservice calls (openPublish, statusnet, etc).
  - EPIC script (attack tool, traffic generator,…)
- Cluster-moderators are responsible of forwarding the information to the Players



Injection of Events (II) - EXCON

EXITO the EXercise event Injection TOolkit - Exercise Portal

Home

mod1

- Discussion
- ECB
- ECB write access
- Master list
- Events list
- Status list
- Event + Status list
- Downloads
- Map
- Map points
- Map links
- User variables list
- Exercise variables
- My account
- Log out

Autoupdate events: On

Current Time (CET)

Master list

This table contains the complete list of Events that the EXCON-moderators can inject into the exercise.

Table: master_list

GroupID

Inject all events matching the GroupID in the box

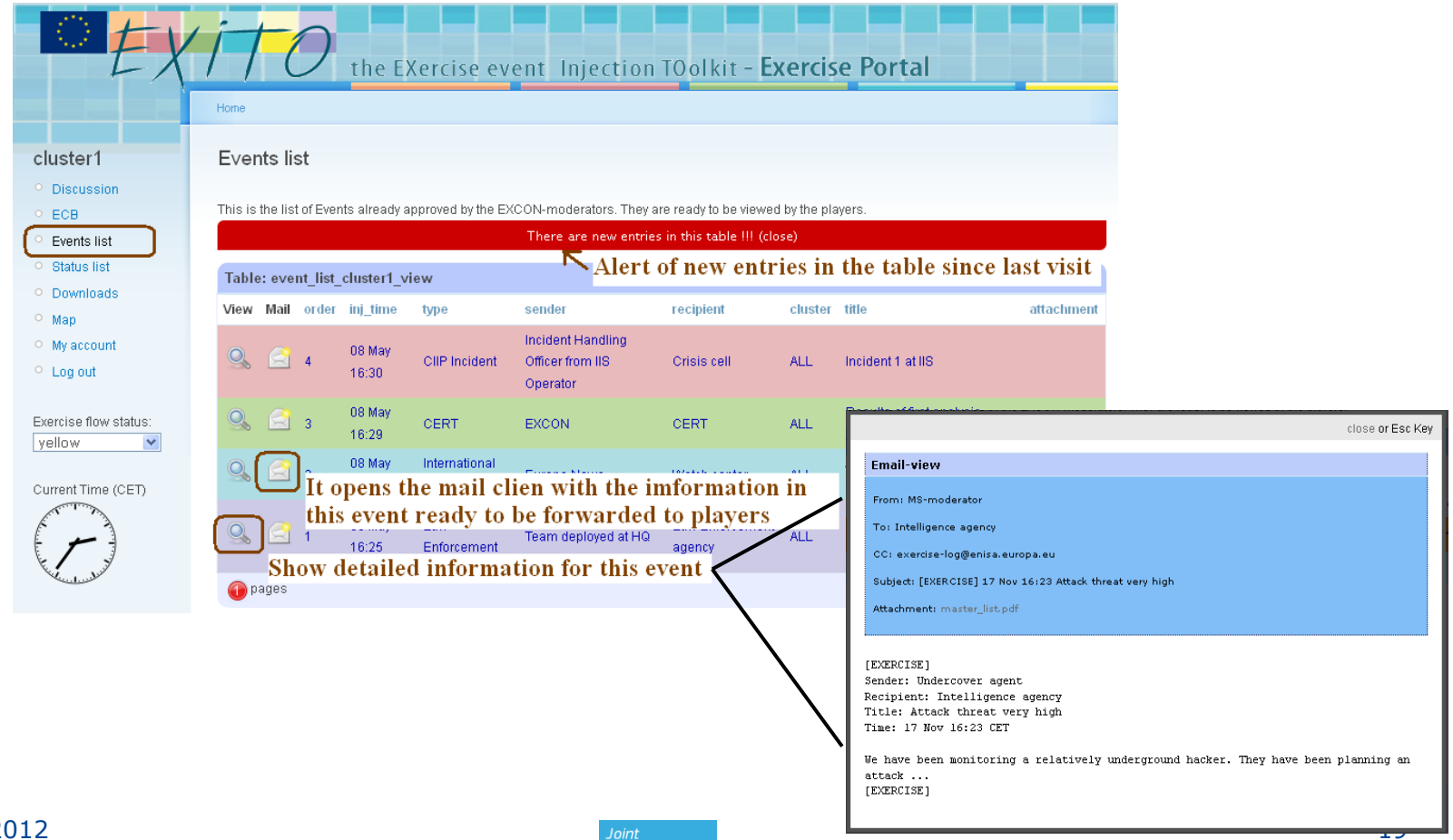
Edit	View	Inject	group	offset	injection_time	cluster	type	sender	recipient	title	attachment
			1	0	2012-04-27 15:30:00	ALL	Intelligence	Undercover agent	Intelligence agency	Attack threat very high	master_list.pdf
			2	10	2012-04-27 15:40:00	ALL	Exercise related	EXCON	All	End of Phase 1, start of phase 2	
			3	20	2012-04-27 15:50:00	ALL	CIIP Incident	Incident Handling Officer from IIS Operator	Crisis cell	Incident 1 at IIS	
			4	30	2012-04-27 16:00:00	ALL	CERT	EXCON	CERT	Results of first analysis delayed	
			5	40	2012-04-27 16:10:00	ALL	Law Enforcement	Team deployed at HQ	Law Enforcement agency	First results from investigation at sensitive server	
			6	50	2012-04-27 16:20:00	ALL	International Media	Europe News	Watch center	Announcement of the list of countries	

Inject this event into the Event list

injetion_time is auto-calculated based on the offset and the exercise_start variable

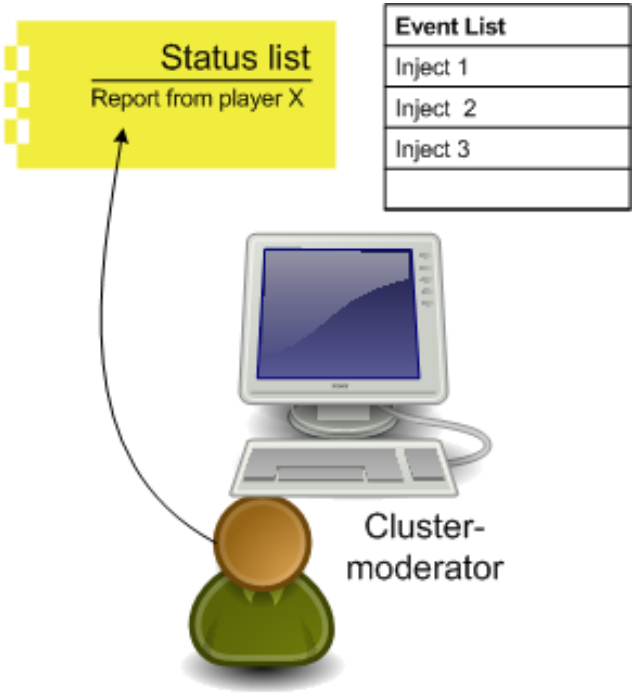
1 pages

Injection of Events (II) – Cluster Mod



Information flows: Feedback from clusters

- Cluster-moderators gather information form Players and fill in a **status report**
- Status reports are generated periodically, on demand or according to exercise's requirements
- All status reports are logged for post analysis
- Cluster Moderators can also provide live-feedback through 'traffic-light' status indicator



European Commission

Cluster–moderators fill in Status reports

EXITO the EXercise event Injection TOolkit - Exercise Portal

Home

cluster1

- Discussion
- ECB
- Events list
- Status list
- Downloads
- Map
- My account
- Log out

Exercise flow status: yellow

Status list

These are the Status Reports already submitted to the system.

Table: status_list_cluster1_view

Add new status report

Clone	View	cluster	Campo1	Campo2
		cluster1	What happened since last status report.	What has be status repor

1 pages

Adding New Record

Assessment: No issue

Status description

Actions taken

Issues details

Submit Close

Joint Research Centre

European Commission

Cluster-moderators provide feedback to EXCON moderators

EXITO the EXercise event Injection TOolkit - Exercise Portal

Home

cluster1

- Discussion
- ECB
- Events list
- Status list
- Downloads
- Map
- My account
- Log out

Exercise flow status:
yellow
green
yellow
red

Events list

This is the list of Events already approved by the EXCON-moderators. They are ready to be viewed by the players.

Table: event_list_cluster1_view

View	Mail	order	inj_time	type	sender	recipient	cluster	title	attachment
		4	08 May 16:30	CIIP Incident	Incident Handling Officer from IIS Operator	Crisis cell	ALL	Incident 1 at IIS	
		3	08 May 16:29	CERT	EXCON	CERT	ALL	Results of first analysis delayed	
			08 May	International		Watch center	ALL	Announcement of the list of countries involved	
		1	08 May 16:25	Law Enforcement	Team deployed at HQ	Law Enforcement agency	ALL	First results from investigation at sensitive server	

1 pages

Feedback provided to EXCON-moderators regarding flow status for this cluster

European Commission

EXCON-moderators have a quick view of status provided by Cluster-moderators

EXiTO the EXercise event Injection TOolkit - Exercise Portal

Home

mod1

- Discussion
- ECB
- ECB write access
- Master list
- Events list
- Status list
- Event + Status list
- Downloads
- Map
- Map points
- Map links
- User variables list
- Exercise variables
- My account
- Log out

Autoupdate events: On

User variables list

This is the current status of user variables.

Table: userstatus_view

View	Edit	uname	varname	varvalue
		cluster1	userstatus	yellow
		cluster2	userstatus	green
		cluster3	userstatus	red
		cluster4	userstatus	green
		cluster5	userstatus	green
		mod1	userstatus	green
		mod2	userstatus	green
		mod3	userstatus	green

1 pages

Extra Features

- A discussion page is available for all users to share information and experiences
- EXCON-moderators can provide the users with files through the downloads page
- Observers see a timeline made of injected events and submitted status reports
- EXITO is fully integrated into EPIC

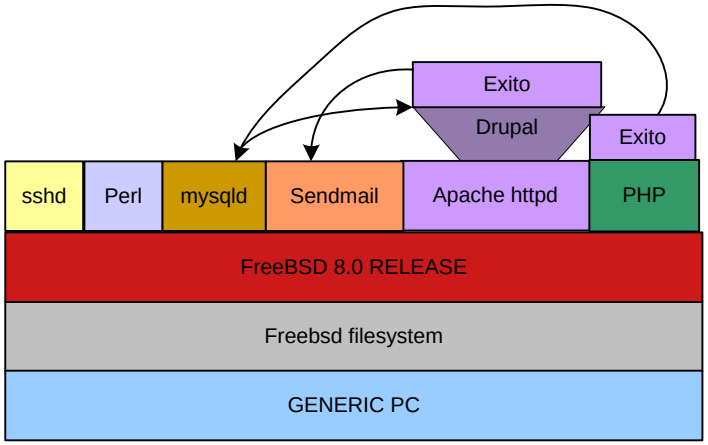
European Commission

Showcase: Cyber Europe 2010

- 4th November 2010
- EXCON & Cluster moderators in a centralized location
- 22 Member States (clusters)
- 12 observers
- 80 remote players from Computer Emergency Response Teams (CERT), Ministries, National Regulatory Authorities, Law enforcement and Intelligence agencies
- MSEL with 320 events
- 185 status reports were collected

Under the hood

- OpenSource Architecture:
  - PHP Web application
  - leverages CMS FW(Drupal)
  - FreeBSD OS
  - Apache web server
  - MySQL database



- EUPL License

How do I get EXITO?

- Format:
  - Live CD for initial testing
  - Virtualbox appliance (fully working environment)
  - Source code (Drupal + EXITO + mysql scripts) for deployment, customization and running exercises

- Procedure:
  - Fill in request form
  - Accept EULA
  - Download software**

    http://sta.jrc.ec.europa.eu/index.php/exito-request-form

** The release is in a beta level