Jornadas PSCIC

I Jornadas Técnicas de Protección de Sistemas de Control en Infraestructuras Críticas

ENISA - First International Conference Cyber Crisis Cooperation Cyber Exercises

Paris

27th of June 2012

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Isdefe

Content

Jornadas PSCIC

Content

CNPIC Isdefe

Jornadas PSCIC

Background

- **Isdefe** (http://www.isdefe.es/), in collaboration with the **National Centre for Critical Infrastructure Protection** (**CNPIC**, http://www.cnpic.es/) of the Spanish Ministry of Interior, has conducted during last April and May 2012 a series of practical sessions, **nationwide** and **cross-sector**, to reinforce and test the skill acquisition for the Protection of **Control Systems** in **Critical Infrastructures**, as well as to assess their processes and procedures.

CNPIC Isdefe

Jornadas PSCIC

Content

CNPIC Isdefe

Aim of the Workshop

- Introduce the **cyber threat** of **Control Systems in Critical Infrastructures** to participants, making them aware of the related **risks**.
- **Train operator's staff**, technically and **hands-on**, addressing previously identified **skill gaps**, such as Risk Assessment and Management, Incident Response and Situational Awareness within Control Systems in Critical Infrastructures.

Jornadas PSCIC

Content

CNPIC Isdefe

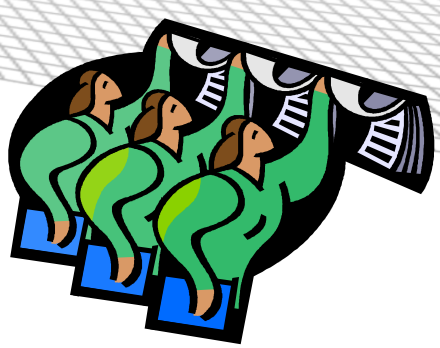
Jornadas PSCIC

Targeted Audience

- Limited to **Energy, Nuclear and Transport Strategic Sectors**, given their importance and that they come within the European **Directive 2008/114/EC**.
- **20 teams** were invited to participate:
  - Including **major Spanish companies** which operate Critical Infrastructures in those sectors. (16 teams)
  - As well as some governmental departments, with sectorial responsibilities in protecting Critical Infrastructures: **Ministry of Development**, **Ministry of Industry, Energy and Tourism**, **Nuclear Security Council** and **National Intelligence Centre**. (4 teams)

CNPIC Isdefe

Jornadas PSCIC



Targeted Audience: Profiles

- **Systems** and **security administrators** in **ICT departments** of critical infrastructure operators.
- **Technical staff** dealing with **control systems management** in critical infrastructure.
- **Directors of security** departments of energy, nuclear and transport strategic infrastructures companies.
- **Managers** and **technical staff** in **governmental agencies** with responsibility for Critical Infrastructure Protection.

CNPIC Isdefe

Jornadas PSCIC

Content

CNPIC Isdefe

Jornadas PSCIC

Workshop Scheme

- **Opening Session,** in which were presented objectives, profile of participants and scheme of the technical sessions. It was a face session, held at the Isdefe premises (11/04/2012).
- **Two Practical Sessions**, which took place in 2 consecutive days (17 and 18/04/2012) over a virtualized scenario. They were remote sessions and each team attended from their own premises. All participants were connected through an interactive web conferencing service over Internet.
- **Closing Session**, in which the results and conclusions of the workshop were presented. It was a face session, held at the Isdefe premises (08/05/2012).

CNPIC Isdefe

Workshop Scheme: Sessions Content

1st Practical Session: Management of Security Incidents in CIs

Objectives:

- Introduce national regulatory framework on Critical Infrastructure.
- Raising awareness of the threats (real cases).
- Implementing techniques of monitoring and managing security incidents.
- Raise awareness of the importance of sharing information.
- Secure architecture design.

Workshop Scheme: Sessions Content

1st Practical Session: Management of Security Incidents in CIs

Used Tools:

- **OSSIM** (SIEM) for monitoring events.
- **Wiki** for recording incidents and sharing information.

Workshop Scheme: Sessions Content

2nd Practical Session: Risk Assessment and Management

Objectives:

- Raise awareness of the risk assessment, its utility and practical application.
- Become familiar with the process of risk management.
- Spreading the benefits of good risk assessment.
- Using the **MAGERIT methodology.**

Workshop Scheme: Sessions Content

2nd Practical Session: Risk Assessment and Management

Used Tools:

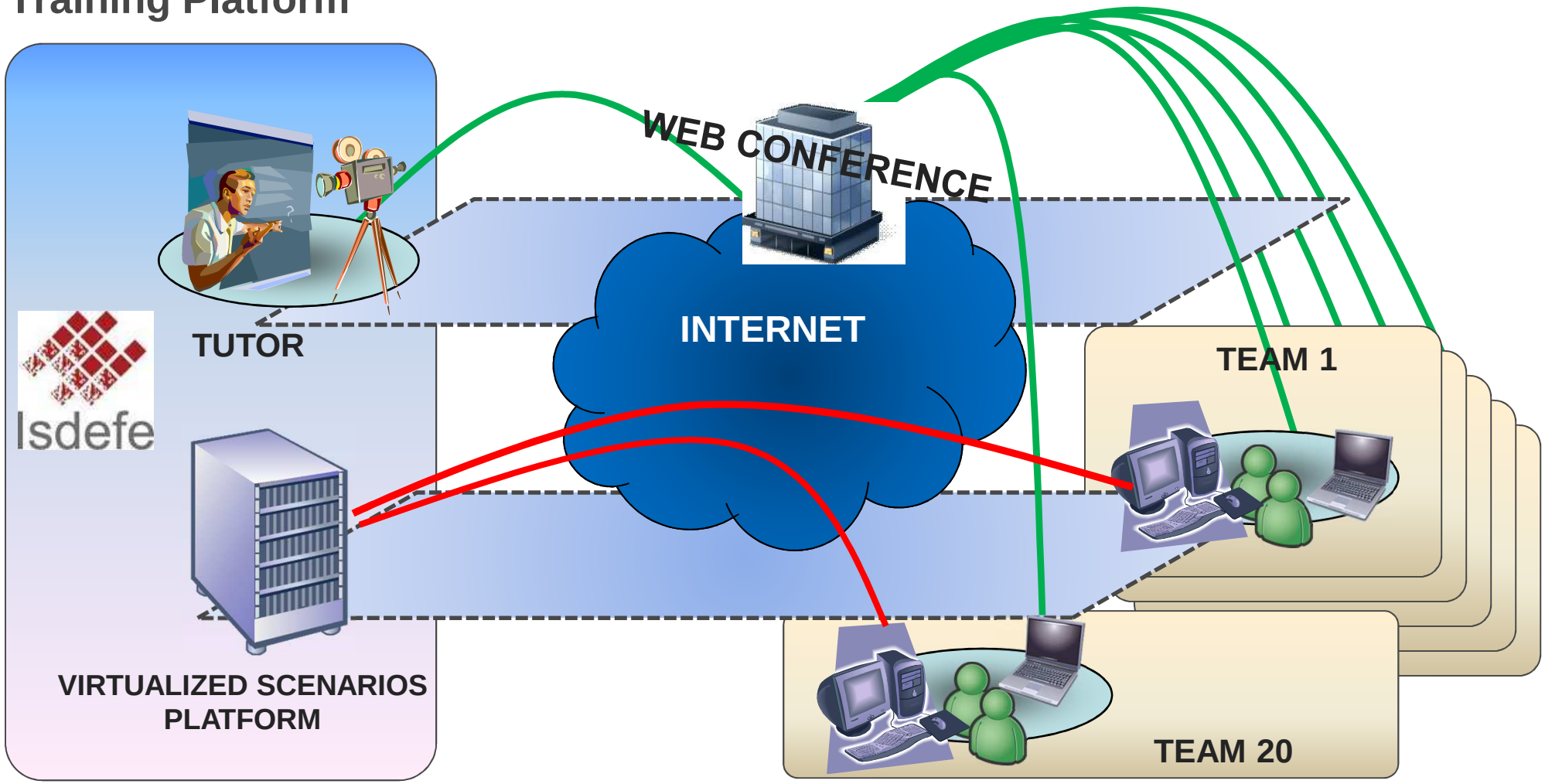
- **PILAR** for risk assessment and management.
- **Wiki** for recording incidents and sharing information.

Jornadas PSCIC

Content

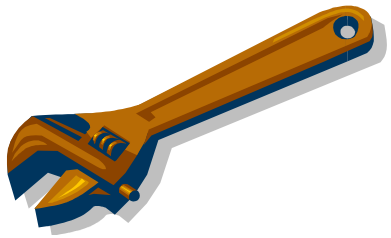
1. Background
2. Aim of the Workshop
3. Targeted Audience
4. Workshop Scheme
5. Training Platform
6. Results and Conclusion

Training Platform



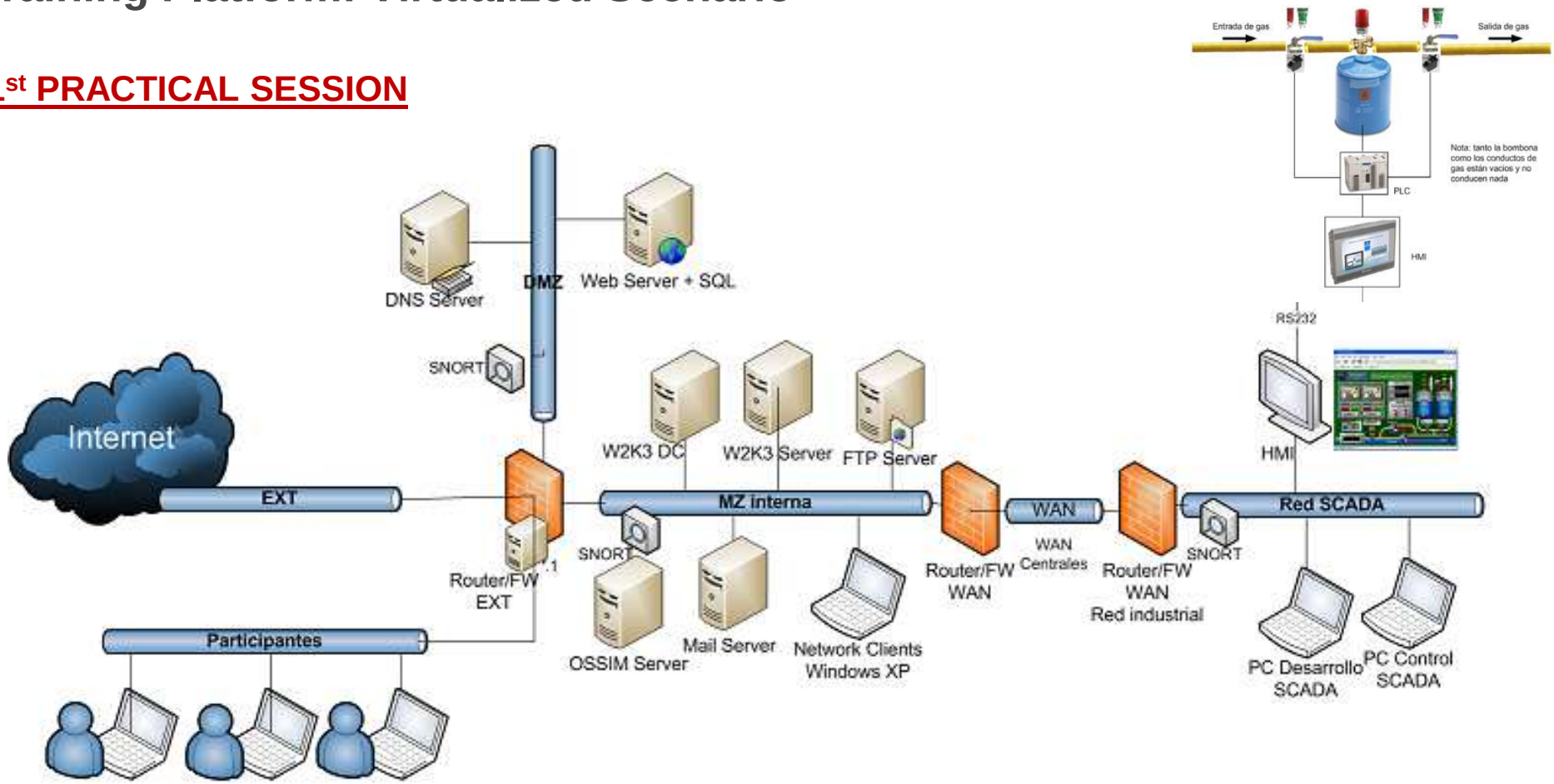
Training Platform

- Making practice remotely from each of the facilities of the participants.
- The tools were provided in a self-bootable DVD.
- Secure communications through a VPN with the platform of practice.
- Strong authentication with USB tokens.
- For participating only needed 1 PC and 1 Internet connection.



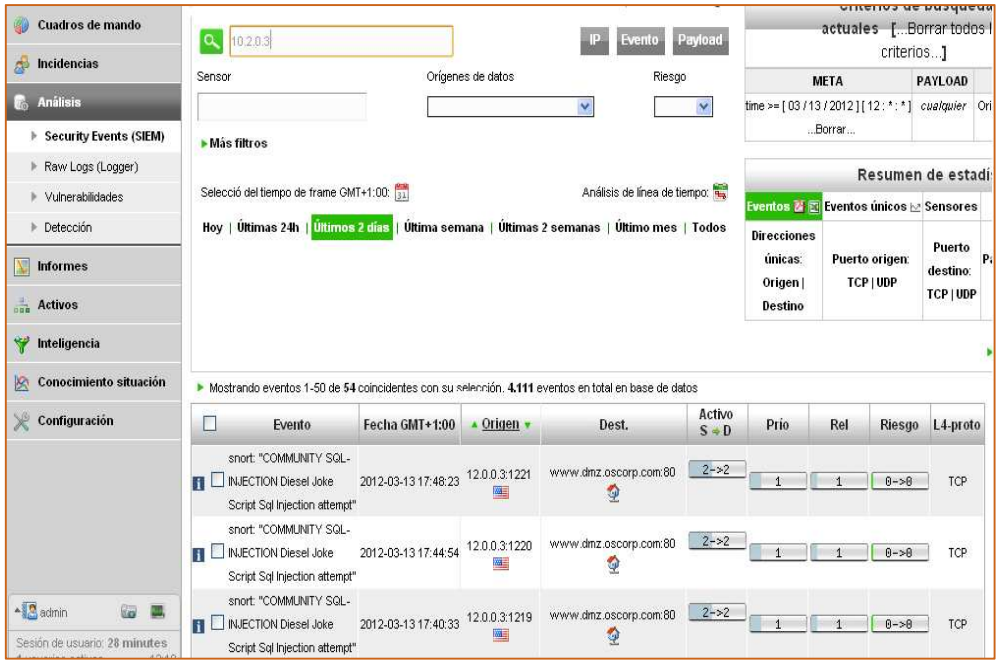
Training Platform: Virtualized Scenario

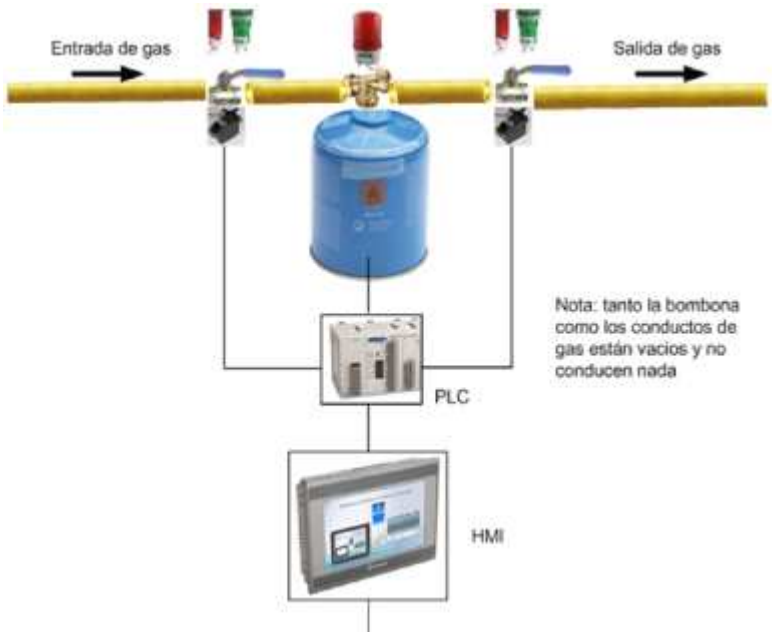
1st PRACTICAL SESSION



Training Platform: Tools and SCADA

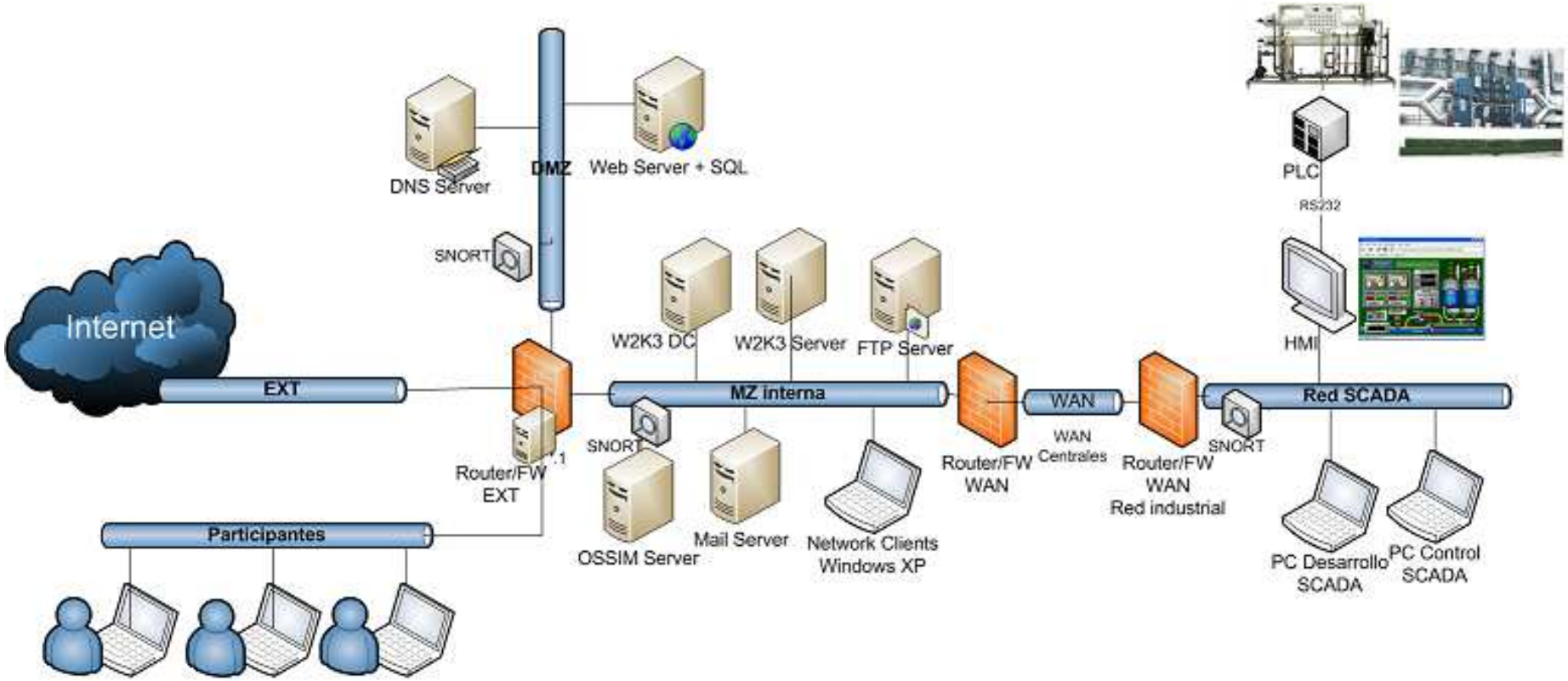
1st PRACTICAL SESSION





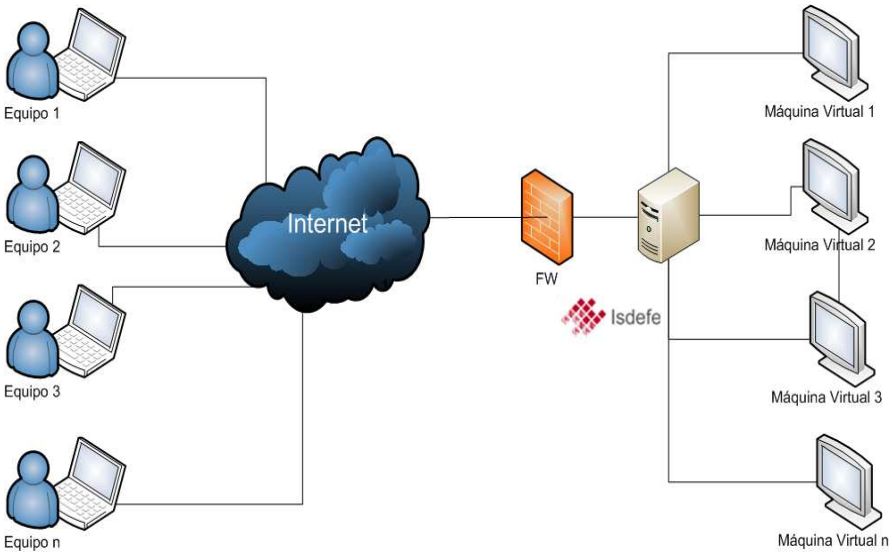
Training Platform: Virtualized Scenario

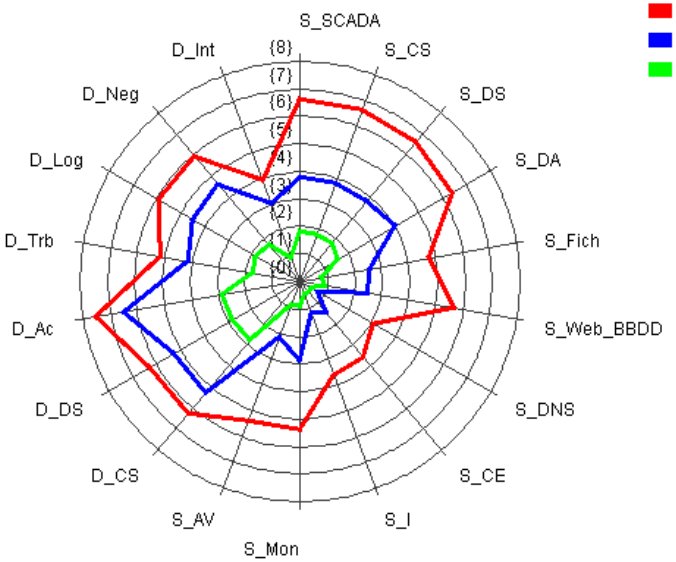
2nd PRACTICAL SESSION



Training Platform: Tools

2nd PRACTICAL SESSION





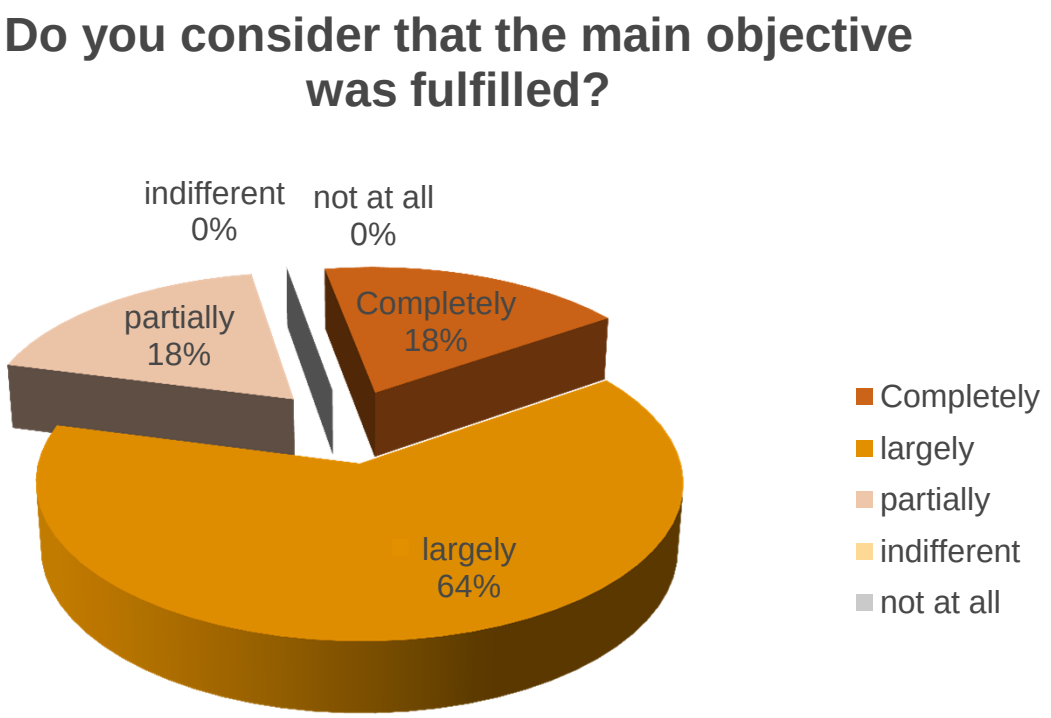
AARR_IJPSCIC: riesgo acumulado - [edu] I Jornadas PSCIC

activo	amenaza	dimensión	V	VA	D	I	F	riesgo
[SW.SW PC.SW_PC] Software gener...	[A.8] Difusión de software dañino	[D]		[9]	100%	[9]	100	{8,0}
[D_Ac] Datos de Acceso	[A.11] Acceso no autorizado	[C]	[9]	[9]	50%	[8]	100	{7,5}
[SW.SW SRV.SW_SRV] Software ge...	[A.8] Difusión de software dañino	[C]		[9]	100%	[9]	10	{7,1}
[SW.SW PC.SW_DE] Software de De...	[A.8] Difusión de software dañino	[D]		[9]	100%	[9]	10	{7,1}
[SW.SW SRV.SW_SD] Software de S...	[A.8] Difusión de software dañino	[C]		[9]	100%	[9]	10	{7,1}
[D_Ac] Datos de Acceso	[A.19] Revelación de información	[C]	[9]	[9]	100%	[9]	10	{7,1}
[SW.SW_PLC] Software PLC	[A.8] Difusión de software dañino	[D]		[9]	100%	[9]	10	{7,1}

Content

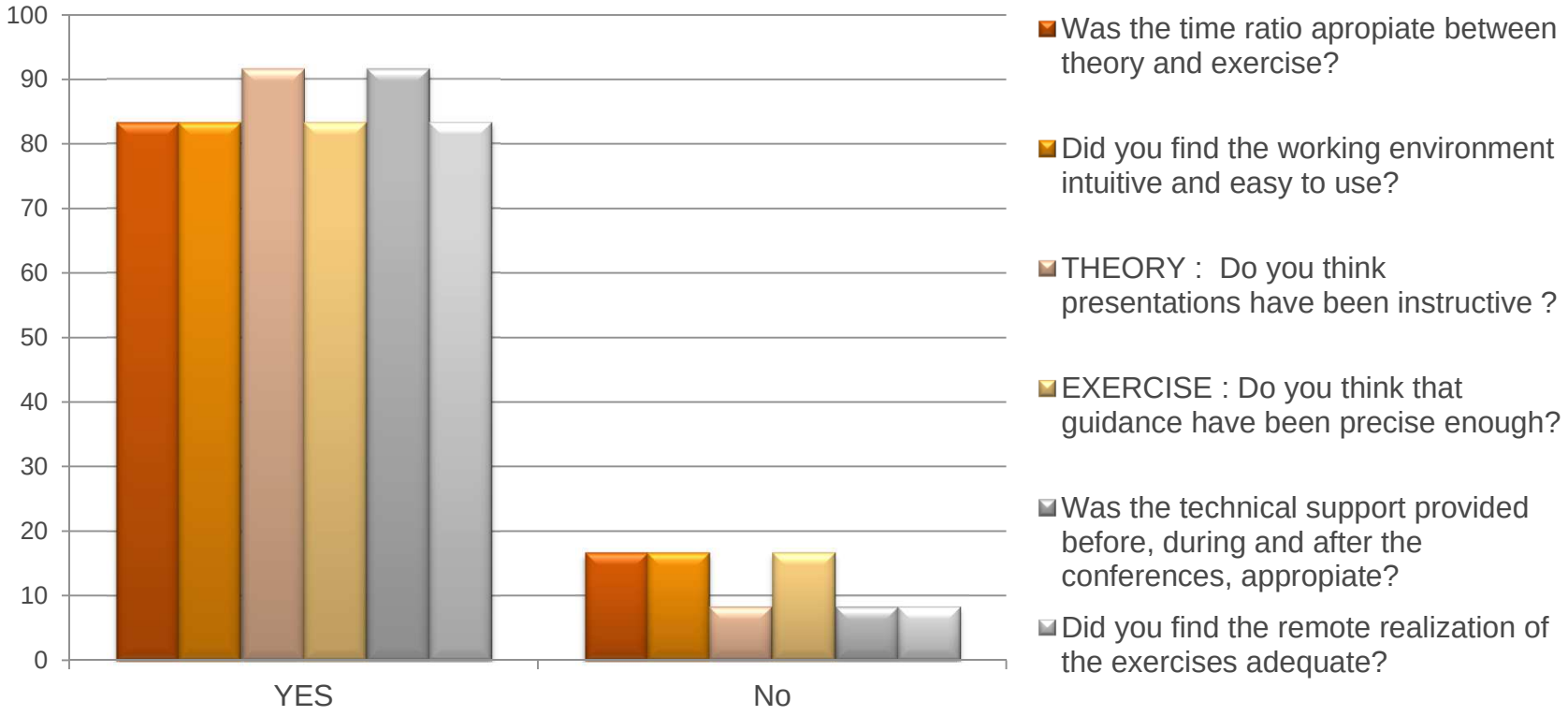
Results and Conclusion: Participants Assessment

Objectives



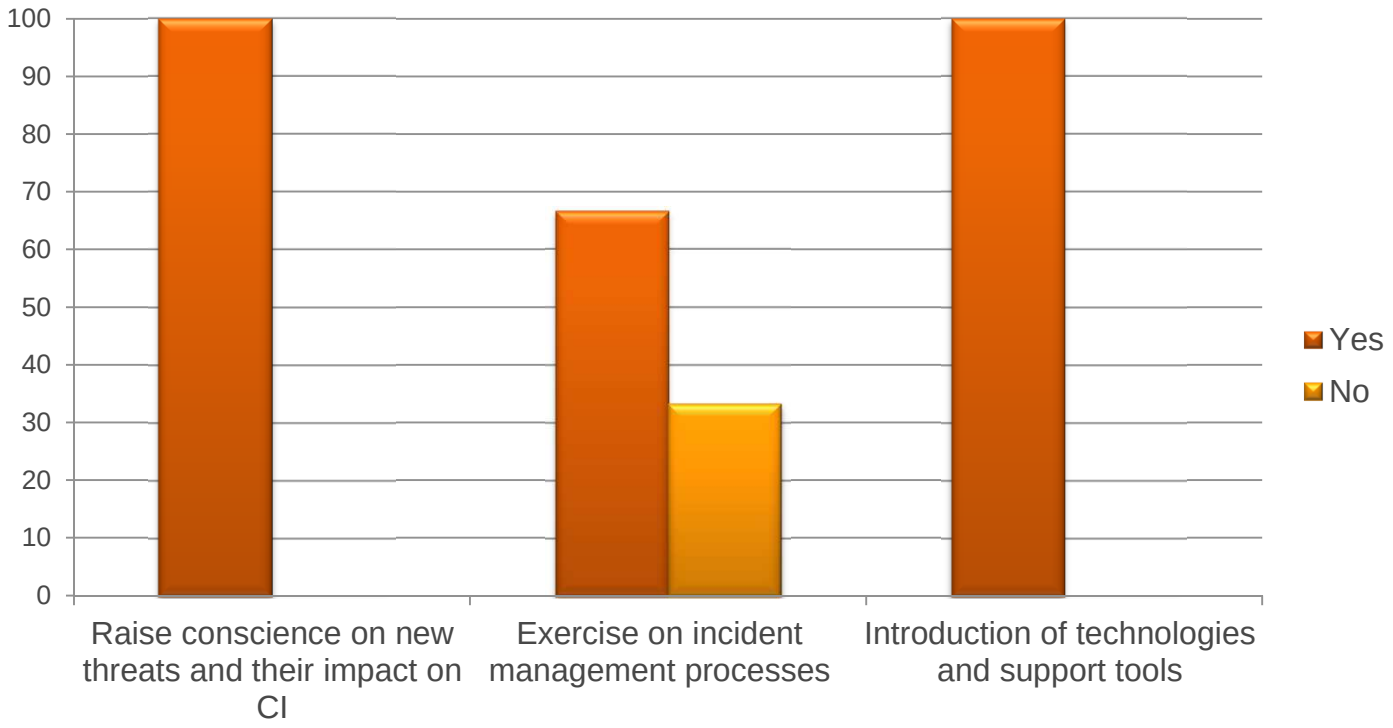
Results and Conclusion: Participants Assessment

Organization



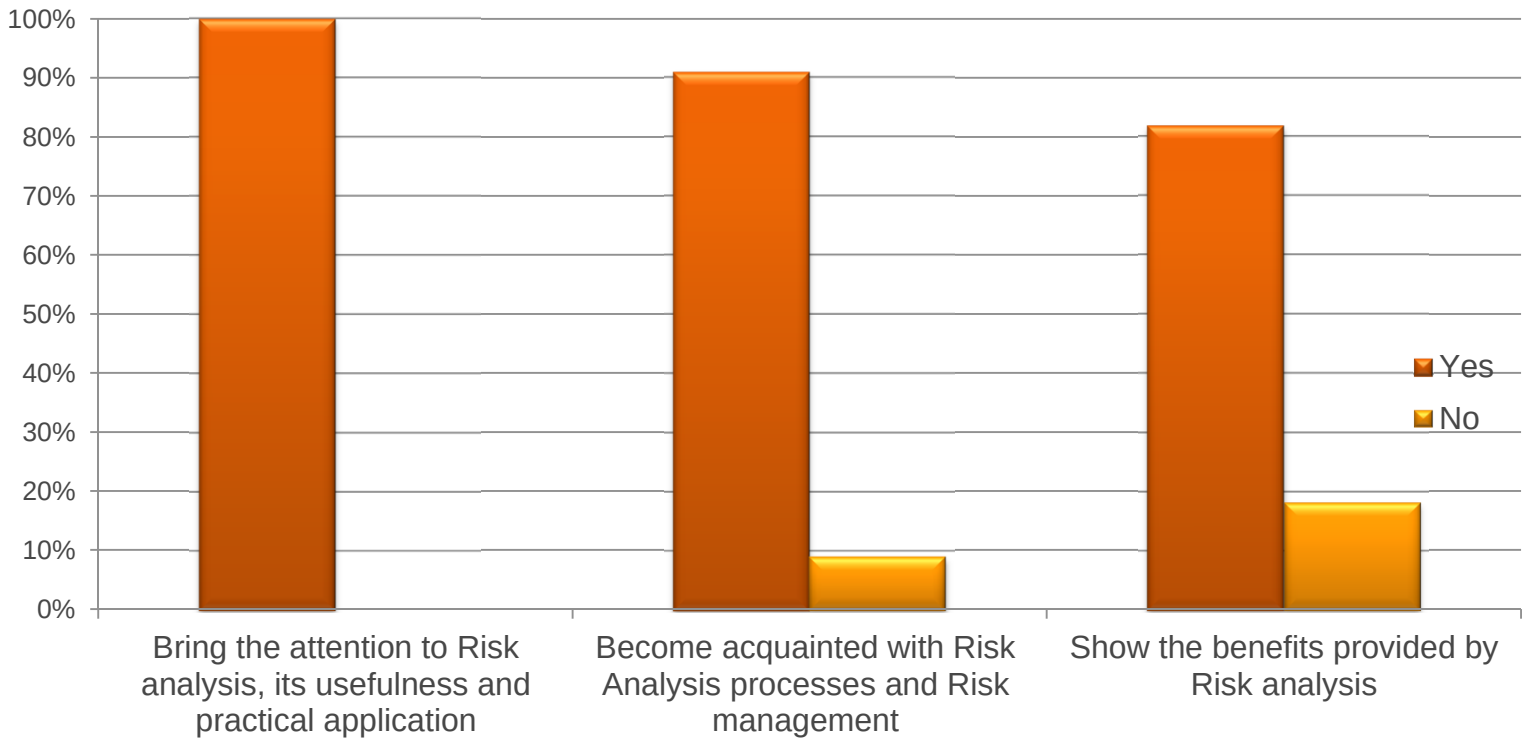
Results and Conclusion: Participants Assessment

Theme of 1st Practical Session



Results and Conclusion: Participants Assessment

Theme of 2nd Practical Session



Results and Conclusion: Lessons Learned

- Diversity in the number of participants per team, from 2 to 20 people / team.
- Different levels of technical knowledge among participants.
- Widespread use and positive Wiki as facilitator of information exchange.

Results and Conclusion: Lessons Learned

- **1st Practical Session: Security Incident Management**
  - Adaptation of the scenario to the expectations.
  - Disparity of expertise between the various participants.
  - Learning SIEM tools to be able to detect complex attacks.
  - Improvements were noted in the management of incidents by users during the course of the day.

Results and Conclusion: Lessons Learned

- **2nd Practical Session: Risk Assessment and Management**
  - Greater homogeneity in the level of knowledge of the participants in this field.
  - Greater complexity of this practice session for the participants.
  - High interest in expanding knowledge in the area of Risk Assessment.

Conclusion

- High acceptance of the event.
- Very satisfactory level of participation.
- According to assessment of participants, successful theme and organization.
- High degree of interest from the teams participating in the Practical Sessions.
- Achieved the objectives set out above.

Questions?

Diego Fernández Vázquez
dfvazquez@isdefe.es

Miguel Ángel Abad Arranz
cnpic-ciber@ses.mir.es

Isdefe

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS