CyberLab

CYBERSECURITY INNOVATION **LAB** FOR PUBLIC ADMINISTRATION

Bruno Pereira e **Sara Andrade** | CSIRT.UPORTO

Consórcio CyberLab

universidade de aveiro

U.PORTO

utad UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO

Cofinanciado por:

COMPETE 2020
PROGRAMA OPERACIONAL COMPETITIVIDADE E INTERNACIONALIZAÇÃO

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Motivação

- Cada vez maior digitalização na Administração Pública e Ensino Superior
- Necessidade de capacitar as equipas que gerem serviços essenciais face ao número crescente de ciberataques e ciber-incidentes
- Treino e avaliação destas equipas quanto à sua capacidade de resposta e resiliência face a incidentes

"(...) the rise of innovation hubs in the Public Sector have achieved considerable results and added extraordinary social and economic value to their host or parent organizations"

- *The Rise of the Innovation Lab in the Public Sector*, J. BARNES

INCIDENTES POR SETOR E ÁREA GOVERNATIVA REGISTADOS PELO CERT.PT, 2021 E 2022 - TOP 15*

2021				2022				Ordenação	
RK	Setor e Área Governativa[8]	Nº	%	RK	Setor e Área Governativa	Nº	%	Variação %	Lugar RK
1º	Outros	1220	39	1º	Outros	1055	37	-14	=
2º	Banca	411	13	2º	Banca	542	19	+32	=
3º	Presidência do Conselho de Ministros	270	9	3º	Infraestruturas Digitais	205	7	-23	+
4º	Infraestruturas Digitais	266	8	4º	Educação e Ciência, Tecnologia e Ensino Superior	202	7	+85	+
5º	Prestadores de Serviços de Internet	187	6	5º	Prestadores de Serviços de Internet	148	5	-21	=
6º	Administração Interna	181	6	6º	Presidência do Conselho de Ministros	131	5	-51	-
7º	Transportes	133	4	7º	Administração Local	129	5	+8	+
8º	Administração Local	120	4	8º	Transportes	93	3	-30	-
9º	Educação e Ciência, Tecnologia e Ensino Superior	109	3	9º	Saúde	83	3	+32	+
10º	Saúde	63	2	10º	Finanças	55	2	+175	+
11º	Energia	31	1	11º	Energia	34	1	+10	=
12º	Cultura e Turismo	26	1	12º	Administração Regional	29	1	+107	+
13º	Finanças	20	1	13º	Justiça	27	1	+80	+
14º	Defesa Nacional	19	1	14º	Trabalho, Solidariedade e Segurança Social	26	1	+44	+
15º	Negócios Estrangeiros	18	1	15º	Administração Interna	25	1	-86	-

Fonte: CERT.PT

* O total de incidentes por setor e área governativa é superior ao nº total de incidentes devido ao facto de em alguns casos um incidente poder ser contabilizado simultaneamente em mais do que um setor e área governativa. As áreas governativas identificadas dizem respeito a todas as entidades sob o domínio administrativo das mesmas.

In *Relatório de Cibersegurança em Portugal: Riscos e Conflitos*, CNCS (junho 2023)

Desafio

- Desenvolvimento ou aquisição de uma plataforma que permita capacitar e treinar equipas para resposta a ciberataques
- Prever, avaliar e mitigar riscos e perdas perante um ciberataque
- Testar a resiliência de IES, Administração Pública (AP) e empresas do setor privado
- Criação de parcerias entre instituições públicas e privadas para realização de exercícios de preparação para resposta a ciberataques

Objetivos do CyberLab

- **Laboratório de ciberexercícios** adaptados aos vários contextos da AP e recolha de indicadores
- **Formação** e capacitação de profissionais nas áreas de TI e Cibersegurança
- Realização de **exercícios e competições** (de tipo CyberRange) em conjunto **com outras institutições e partilha inter-institucional de conhecimento**
- Solução em concordância com os melhores **padrões e normas de segurança** (ISO 27001, NIST, NIS, etc.)

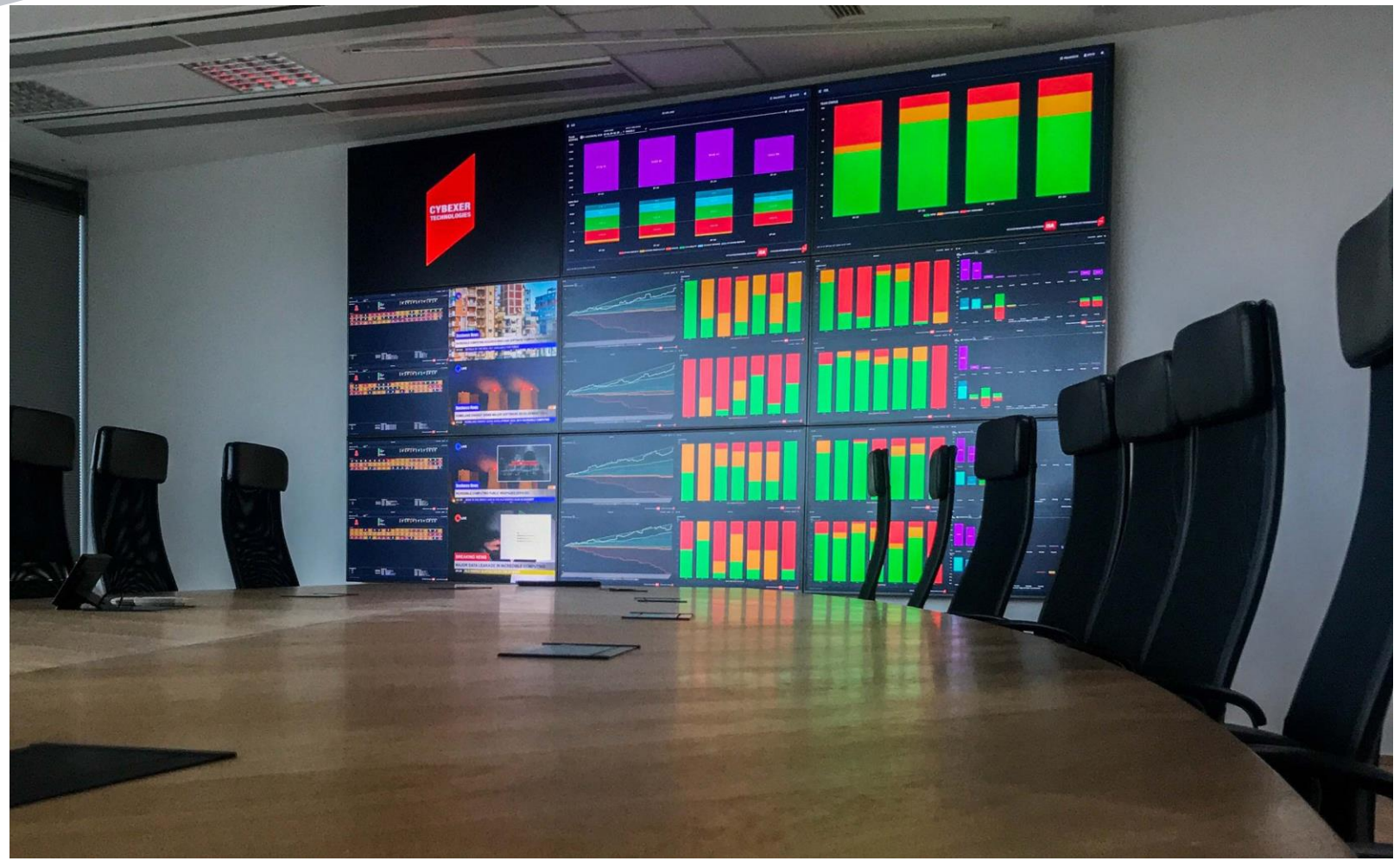
Cenários

1. Staff
2. Gestão de topo
3. Docentes
4. Investigadores
5. Estudantes

Plataforma a ser utilizada

- Solução da **Cybexer**
  - Resultado de um consulta pública internacional
  - Plataforma de topo utilizada por várias forças armadas, NATO, e organizações públicas e privadas a nível mundial. Em Portugal é regularmente utilizada no CiberPerseu.
  - Solução de elevada capacidade (até 1000 VM's ativas num cenário)


COMPACT VIEW
TEAM
BT-04
CAMPAIGN LIVE
PERIOD 2
DMZ SERVERS 10 TARGETS
R1.IC04.JC.CRP
R2.IC04.IC.CRP
FW1.SC04.JC.CRP
INT SEGMENT SERVERS AND WORKSTATIONS 27 TARGETS
DC1.INT.IC04.JC.CRP
DC2.INT.IC04.IC.CRP
FILES.INT.IC04.IC.CRP
WS2-2.INT.IC04.JC.C...
WS2-3.INT.IC04.JC.C...
WS2-4.INT.IC04.JC.C...
SECURITY TOOLS AND SERVERS 6 TARGETS
NESSUS.SEC.IC04.JC....
MOLOCH.SEC.IC04.JC...
OSSEC.SEC.IC04.JC.C...


CYBEXER
TECHNOLOGIES

Jornadas FCCN 2023

Como operacionalizar um laboratório de cibersegurança para corresponder às necessidades das IES?

Necessidade das IES

- Materiais de estudo (indicadores, biblotecas de vulnerabilidades, boas práticas).
- Biblioteca ampla e variada de cenários e exercícios para treino.

- Maior capacitação e resilência da IES face a ciberataques reais.
- Melhor preparação dos estudantes face à realidade logo para o mercado de trabalho.

Fases de um ciberexercício

Planeamento	Execução	Avaliação
- Definir objetivos, local, e data e tipo do exercício; - Definir equipas, participantes, monitores, etc. - Definir *Injects* e enredo do exercício - Preparar documentação	- Monitorizar os exercício e os participantes - Treinar as capacidades de acordo com o exercício	- Avaliação do trabalho realizado pelos participantes - Lançamento de documentação do exercício - Aplicação de *lessons-learned* na organização dos diferentes participantes

Planeamento

Infraestrutura

- Intra ou inter organização? Há organizações que cooperam entre si?

Modelo

- Tabletop ou Live Play?

Localização

- Verificar condições, salas, ventilação, alimentação, etc.

Recursos Humanos

- Participantes, Monitores, e Observadores

Objetivo

- Fazer o quê, em quê, e em que contexto?

Duração

- Poucas horas ou alguns dias?

Eq. Desenvolvimento

- Planear os cenários e injects
- Agir de acordo com o calendário de reuniões
- Planear o papel dos moderadores
- Planear a metedologia de avaliação
- Regras

Próximos passos…

- Está em curso a instalação da solução (hardware e software) da CyberExer (na Universidade de Aveiro).
- Mais novidades em breve ;-)

Patrocinadores

Platina

EBSCO

ELSEVIER

Microsoft

warpcom

cisco

FORTINET

axians

officelan

SECURNET

CHECK POINT

SYSCRUM

PAESSLER
THE MONITORING EXPERTS

ORACLE

NVIDIA.

paloalto NETWORKS

software one

Ouro

ACS Publications
Most Trusted. Most Cited. Most Read.

Clarivate™

CAMBRIDGE UNIVERSITY PRESS

DE G DE GRUYTER

HUAWEI

DIVULTEC

LOGICALIS
Architects of Change

Sage

SPRINGER NATURE

tp-link

wavecom

Bravantic

itcenter

reallife
technologies

Prata

ROYAL SOCIETY OF CHEMISTRY

IOP Publishing

MEO EMPRESAS

aws

emerald PUBLISHING

IEEE

Logiser

Organização

fct Fundação para a Ciência e a Tecnologia

FCCN

ESCOLA NAVAL