FCT Fundação para a Ciência e a Tecnologia

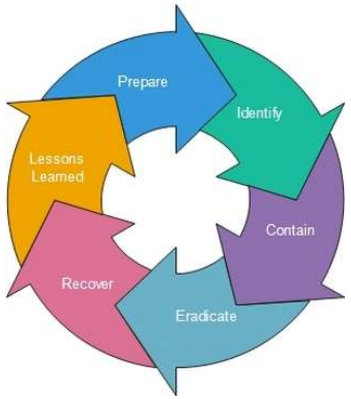
Computação Científica Nacional
FCCN

Formação @RAC

Carlos Friaças
ASA / SEG
20-Nov-2018

Novas equipas, novas capacidades

- A actividade central de um CSIRT é a resposta a incidentes



- É necessário um processo
- É necessário know-how para analisar cada incidente
- Formação contínua

CSIRT-in-a-Box

- Flexível em duração
- Organizado pelo RCTS CERT em 2015, 2016 e 2017
- Componente Hands-On

- Ideal para membros de equipas ou elementos «PPTO»

CSIRT-in-a-Box

CSIRT-in-a-Box

- Pacote CSIRT-in-a-Box
- Construção de um novo CSIRT
- Medidas de Controlo de Incidentes e Eventos na RCTS
- Resposta a Incidentes

- IntelMQ
- Splunk
- Ferramentas para Auditorias
- Netflow
- DDoS, Malware e outras Ameaças

Transits - GÉANT

- TRANSITS-I para novos recrutas

- TRANSITS-II para elementos com experiência
- Financiamento da ENISA

enisa European Union Agency for Network and Information Security

- CNCS promove estes cursos em Portugal

CERT.PT Centro Nacional de Cibersegurança PORTUGAL

IntelMQ 1-on-1

- Instalação de IntelMQ para CSIRTs da RAC
- Workshop “hands-on” de um dia na FCCN, por instituição
- Replicar o modelo de instalação dos IdP
- Partindo de uma VM pré-instalada

Capture The Flag

- Realizado nas Jornadas 2018, em Braga
- Poucos participantes
- 14 exercícios
- Plataforma disponível para eventos organizados por terceiros

Conteúdo para treinos internos

- Boas práticas
- Backups
- Anti-Vírus
- E-Mails, anexos
- BYOD
- Pause/Resume p2p
- Anti-Phishing
- Anti-Ransomware
- Lock Screen
- Passwords

Perguntas

FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Obrigado pela atenção!

info@cert.rcts.pt