FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Novo Portfólio de Serviços do RCTS CERT

Carlos Friaças
ASA / SEG
20-Nov-2018

História

- CERT.PT inicia operação na FCCN em 2002

- Marca CERT.PT migra para o CNCS em Out/2014

- O CERT da FCCN é rebaptizado como RCTS CERT

História

- Fundador da Rede Nacional CSIRT
- Membro do FIRST desde 2011
- Membro certificado do TI desde 2015

- O RCTS CERT faz mais do que resposta a incidentes
- RCTS CERT … RCTS SOC

Para além da Reacção

- A resposta a incidentes é puramente reativa
- Há muito por fazer no campo da prevenção que diminuirá a necessidade de capacidade de reacção
- Estrutura de segurança adaptativa

Créditos: Kaspersky

Portfólio Oficial - Hoje

- https://www.cert.rcts.pt/pt/sobre/servicos/

- Resposta a Incidentes
- Auditorias
- Serviços pró-activos / Detecção
- Operação da Hotline do Centro Internet Segura

- Em 2017 foi efetuado um inquérito…

Conclusões do inquérito

- Todos os serviços são úteis
- i.e. Expansão do portfólio
- (a dimensão da equipa dificultou este desígnio)

Equipa, Reforçada

- O RCTS CERT tem agora cinco elementos



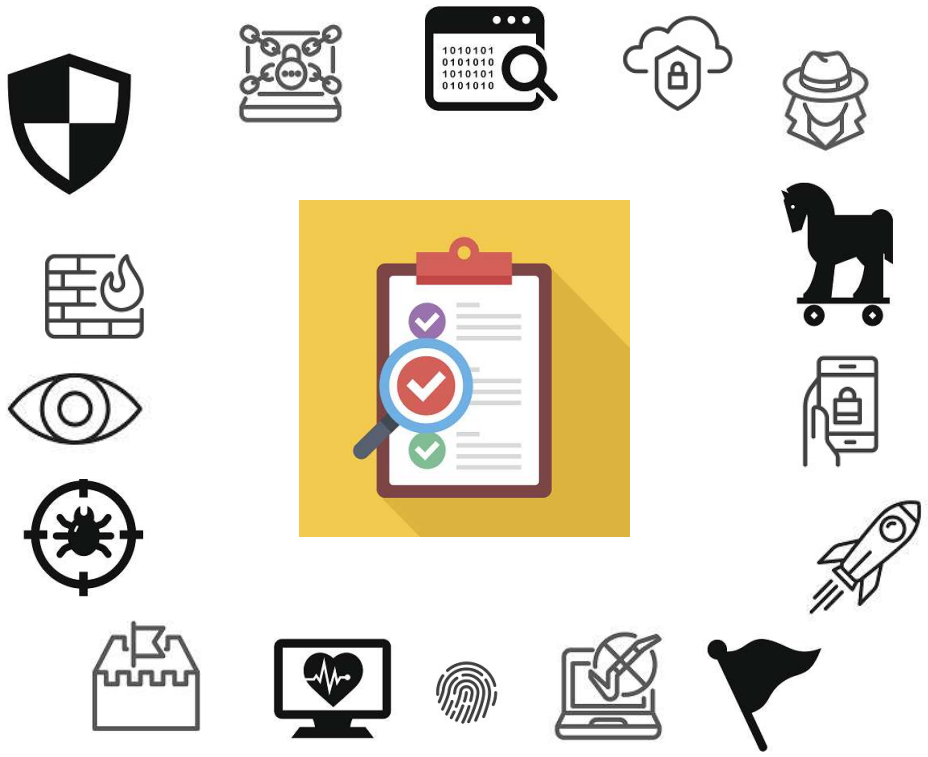


- A Linha Alerta passará a ser operada por outra entidade em 2019

Linha Alerta
internet segura.pt

- Entretanto alguns serviços foram lançados em regime «piloto»
  - E com pouca divulgação

Por onde começar?



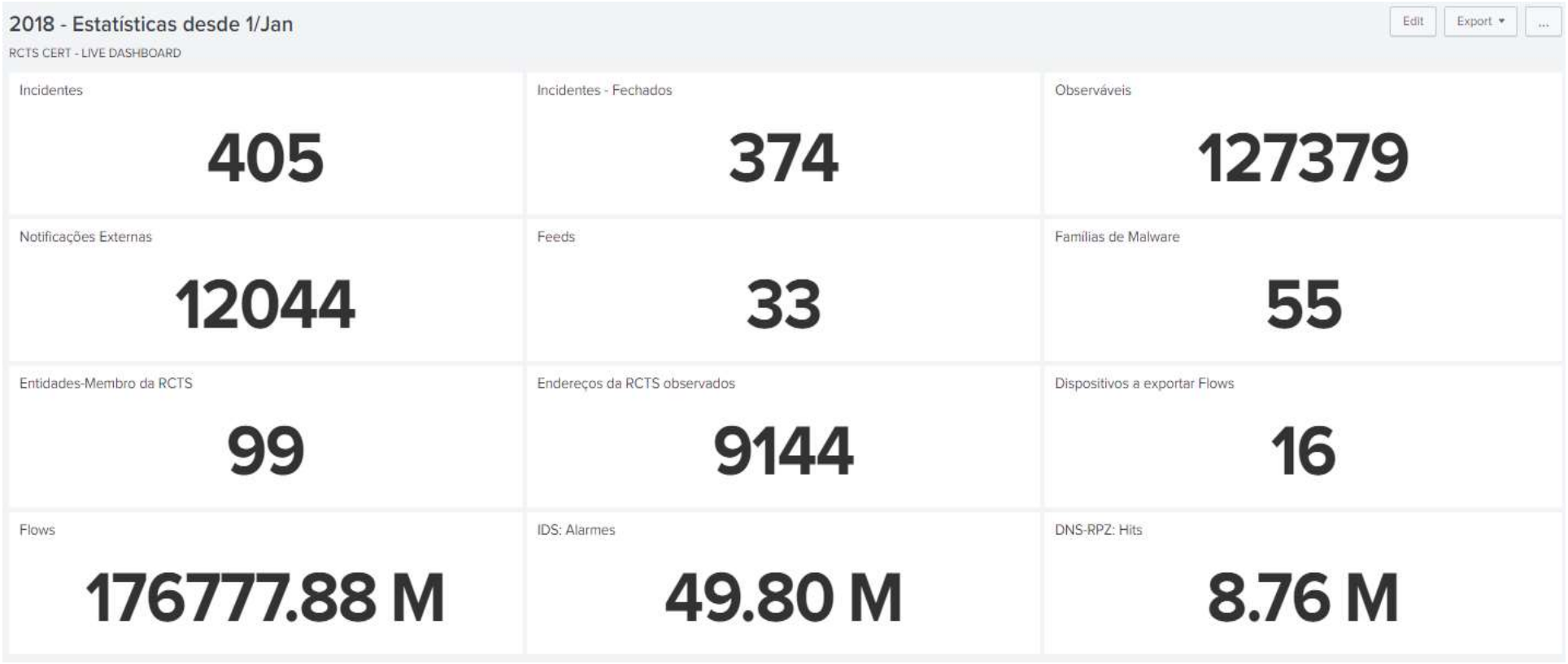
«Novos» Serviços

Serviço	Estado	Target	Como obter?
Análise de Malware	Produção	Membros RCTS	info@cert.rcts.pt, a pedido
Anti-DDoS	Produção	Membros RCTS	noc@fccn.pt, quando DDoS ocorre
Auditorias	Produção	Membros RCTS	info@cert.rcts.pt, a pedido
DNS Firewall	Beta	Membros RCTS	dnsfw@fccn.pt, pedido de adesão
Exercícios de Phishing	Beta	Membros RCTS	info@cert.rcts.pt, a pedido
Geração de Queixas	Beta	Outros CSIRTs	Automático
Gestão de Vulnerabilidades	Beta	Membros RCTS	info@cert.rcts.pt, indicar websites
Honeypots	Alpha	Datacenter FCCN	N/A. Replicável nos Membros RCTS
IDSaaS	Conceptual	Membros RCTS	info@cert.rcts.pt, pedido de adesão
Passive DNS	Beta	Membros RCTS	info@cert.rcts.pt, contribuição com resultados DNS
WebMon	Beta	Membros RCTS	info@cert.rcts.pt, indicar websites

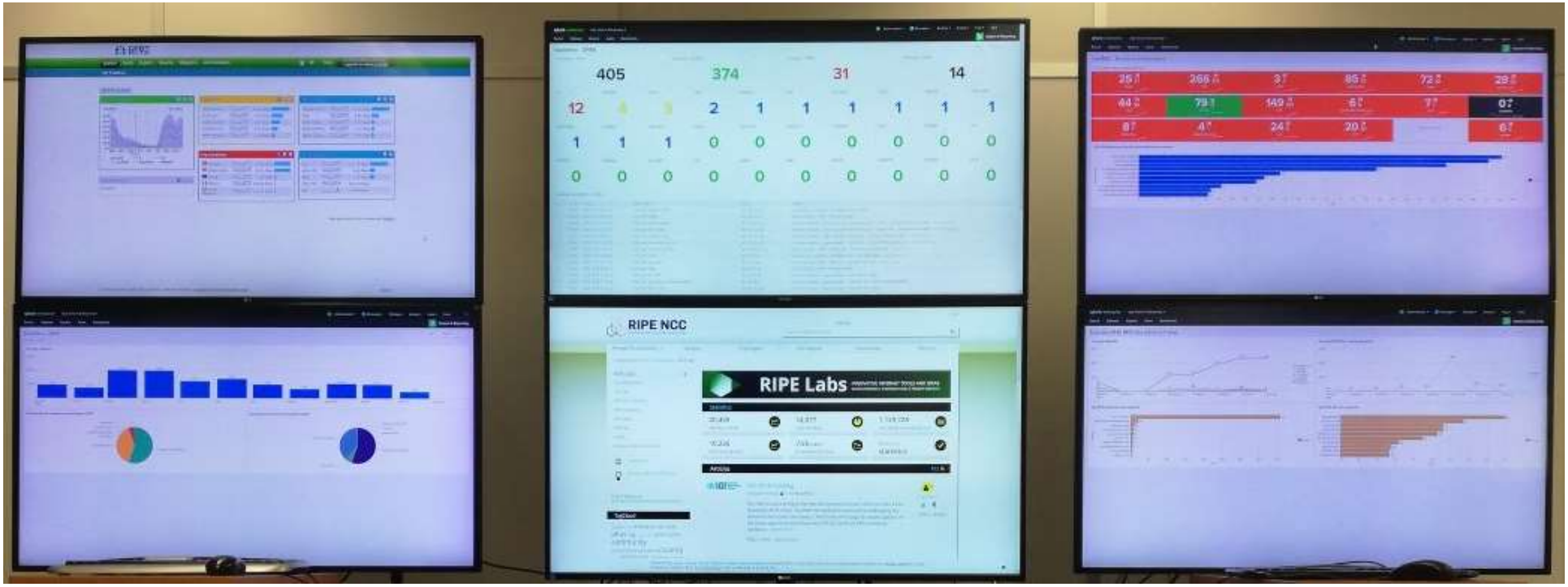
Outros Serviços

Serviço	Estado	Target	Como obter?
Análise Forense	Produção	Membros RCTS	info@cert.rcts.pt, a pedido
Capacitação (CSIRT-in-a-Box, etc…)	Produção	Membros RCTS	Inscrição gratuita, 1x/ano
Correlação de Eventos	Produção	Interno	N/A
Emissão de Alertas/Recomendações	Produção	Membros RCTS	Depende de contactos actualizados
Gestão da Rede Académica CSIRTs	Produção	Membros RCTS	Participação Livre, 2x/ano
Gestão de Consola Anti-Vírus	Produção	Interno FCCN	N/A
Local Internet Registry	Produção	Membros RCTS	lir@fccn.pt ou noc@fccn.pt
Relatórios semanais de vulnerabilidades	Produção	Membros RCTS	Automático (caso existam vulnerabilidades)

Mais informação em tempo real



Mais informação em tempo real



Que outros serviços serão úteis?

Questões

FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Obrigado pela atenção!

info@cert.rcts.pt