Universidade do Minho
Serviços de Comunicações

3ª Reunião - Rede Académica de CSIRTs

Game of Hats @ CSIRT.UMINHO

Marco Teixeira (marco@csirt.uminho.pt)

2018-04-13

Agenda

1 – Introdução

2 – Motivação

3 – Desafios

4 – Game of Hats

5 – Questões

Introdução

Serviços de Comunicações da Universidade do Minho (SCOM)

(art. 32º do Regulamento Orgânico das Unidades de Serviços da Universidade do Minho)

1. Os Serviços de Comunicações da Universidade, adiante designados por SCOM, fornecem serviços e infraestrutura de comunicações à Universidade.

2. Compete aos SCOM a conceção, implementação e exploração de infraestruturas e serviços de comunicação basilares, nomeadamente o fornecimento dos recursos necessários ao desenvolvimento e manutenção da infraestrutura de comunicações e serviços básicos de apoio aos projetos a Universidade, designadamente:

Introdução

Serviços de Comunicações da Universidade do Minho (SCOM)

a) A gestão técnica das infraestrutura de voz e dados na Universidade;
b) A administração dos serviços básicos de comunicações de voz e dados;
c) A gestão das comunicações;
d) Os serviços de segurança na área das comunicações;
e) Gestão técnica e apoio às salas de access grid existentes nos campi da Universidade;
f) Assegurar o estabelecimento e monitorização de acordos de nível de serviço com os utentes, garantindo o atendimento e apoio técnico associado à configuração de portáteis e outros equipamentos, gestão de incidentes, pedidos de alterações de configurações, associados à componente de comunicações.

Introdução

Serviços de Comunicações da Universidade do Minho (SCOM)

Mais informações em:

http://www.scom.uminho.pt

Onde podem encontrar, entre outros:

- Catálogo de Serviços
- Relatórios de Atividades
- Dados sobre a infra-estrutura gerida

Introdução

CSIRT.UMINHO

O CSIRT.UMINHO (Computer Security Incident Response Team da Universidade do Minho) é um serviço na área da segurança prestado pelos Serviços de Comunicações da Universidade do Minho (SCOM) à sua Comunidade Académica.

CSIRT.UMINHO

Universidade do Minho Computer Security Incident Response Team

CSIRT.UMINHO - Missão

O CSIRT.UMINHO tem como missão contribuir para o esforço de cibersegurança da comunidade académica ligada à rede da UMinho, através de ações preventivas e reativas, bem como na promoção de uma cultura de segurança.

Nesse sentido:

- Coordena a resposta a incidentes de segurança informática no contexto da comunidade académica da UMinho;
- Presta apoio a utilizadores de sistemas informáticos da UMinho na resolução de incidentes de segurança, aconselhando procedimentos, analisando artefactos e coordenando ações com todas as entidades envolvidas;
- Reúne e dissemina informação relacionada com vulnerabilidades de segurança e produz recomendações referentes a potenciais riscos e atividades maliciosas em curso, no sentido de formar uma consciência de segurança junto dos utilizadores de sistemas informáticos;

Motivação

Porquê o CSIRT.UMINHO ?

- O CSIRT.UMINHO pretende contribuir para o esforço de cibersegurança da comunidade académica e nacional.

- Pretende-se efetuar uma **abordagem formal** a uma série de atividades que têm vindo a ser levadas a cabo no domínio da segurança informática.

Desafios

Descrevendo os desafios através do RFC2350

Domínio, website, e-mail, telefone

1.3. Acesso a este documento

A versão atualizada deste documento está disponível em
https://csirt.uminho.pt/pt/rfc2350-pt
A versão em língua inglesa está disponível em https://csirt.uminho.pt/en/rfc2350-en

2.7. Endereços de correio eletrónico

Correio eletrónico para notificação de incidentes de cibersegurança:
report@csirt.uminho.pt
Correio eletrónico para outros assuntos relacionados com os serviços CSIRT.UMINHO:
info@csirt.uminho.pt

Descrevendo os desafios através do RFC2350

Domínio, website, e-mail, telefone

2.4. Telefone

+351 253601020

2.5. Fax

+351 253601029

Descrevendo os desafios através do RFC2350

PGP Crash Course

2.8. Chaves públicas e informação de cifra

Correio eletrónico: report@csirt.uminho.pt
User ID: CSIRT.UMINHO (CSIRT University of Minho) <report@csirt.uminho.pt>
Key ID: A16201AF
Key type: RSA
Key size: 4096
Expires: never
Fingerprint: 4BAC4F98422D913461169F83FA631760A16201AF
A chave está disponível em: http://pgp.mit.edu

Descrevendo os desafios através do RFC2350

Endereçamento IP

3.2. Comunidade servida

O CSIRT.UMINHO responde a incidentes de segurança informática no contexto da comunidade académica da UMinho. As gamas de endereços IP abrangidos no âmbito da sua atuação são:

192.68.209.0/24	192.88.252.0/24	193.136.16.0/22	193.137.74.0/24
192.82.127.0/24	192.88.253.0/24	193.136.20.0/23	193.137.75.0/26
192.86.138.0/24	192.88.254.0/24	193.136.22.0/24	193.137.88.0/22
192.88.17.0/24	192.92.142.0/24	193.137.8.0/21	193.137.92.0/24
192.88.250.0/24	192.135.187.0/24	193.137.16.0/22	2001:690:2280::/64
192.88.251.0/24	193.136.8.0/21	193.137.72.0/23	

Descrevendo os desafios através do RFC2350

4.1. Tipos de incidente e nível de suporte

O CSIRT.UMINHO responde a todos os tipos de incidente de cibersegurança que ocorram no âmbito da sua comunidade académica, nomeadamente aqueles que resultam numa violação de segurança dos seguintes tipos:

Código Malicioso

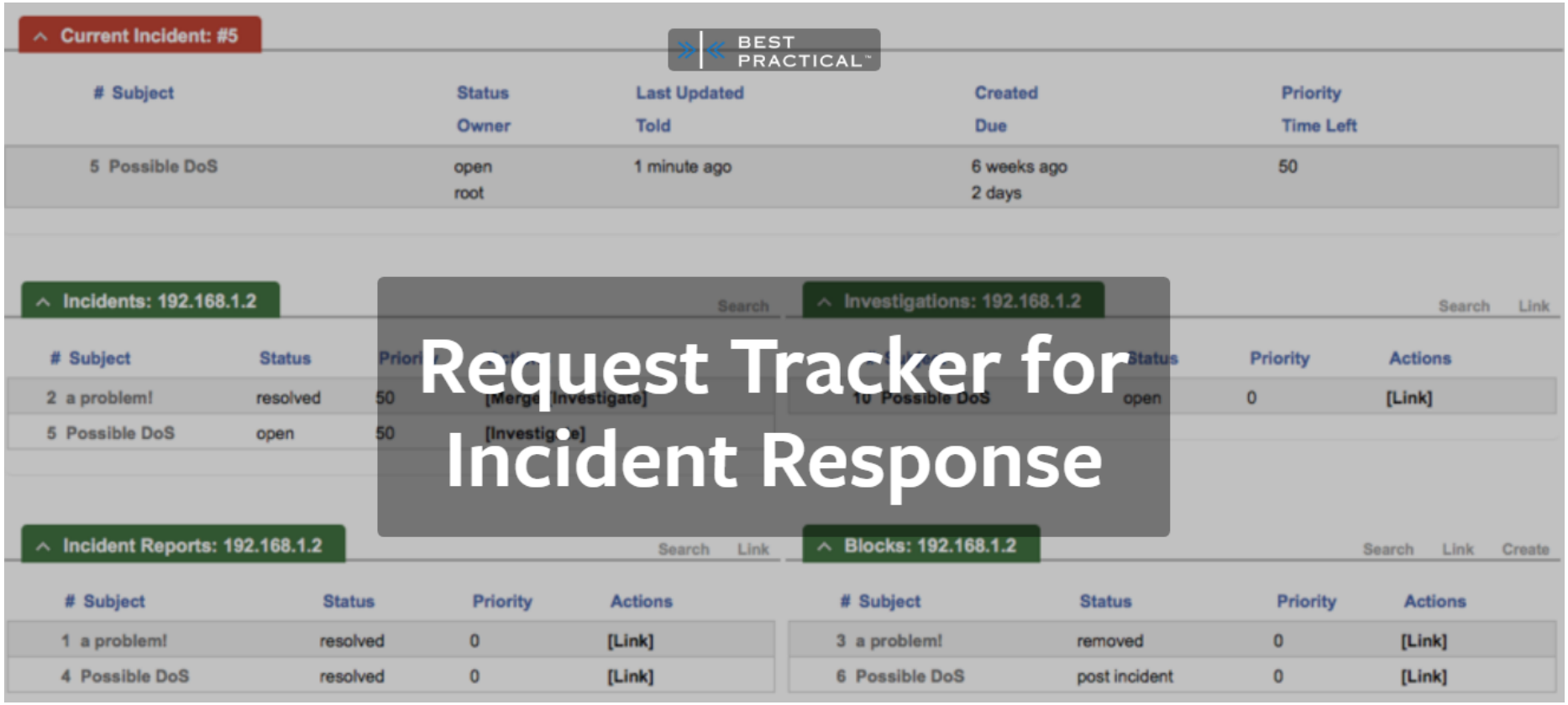
(...)

Outros

O nível de suporte dado pelo CSIRT.UMINHO varia consoante o tipo, gravidade e âmbito dos incidentes em curso e os **recursos disponíveis** para o seu tratamento.

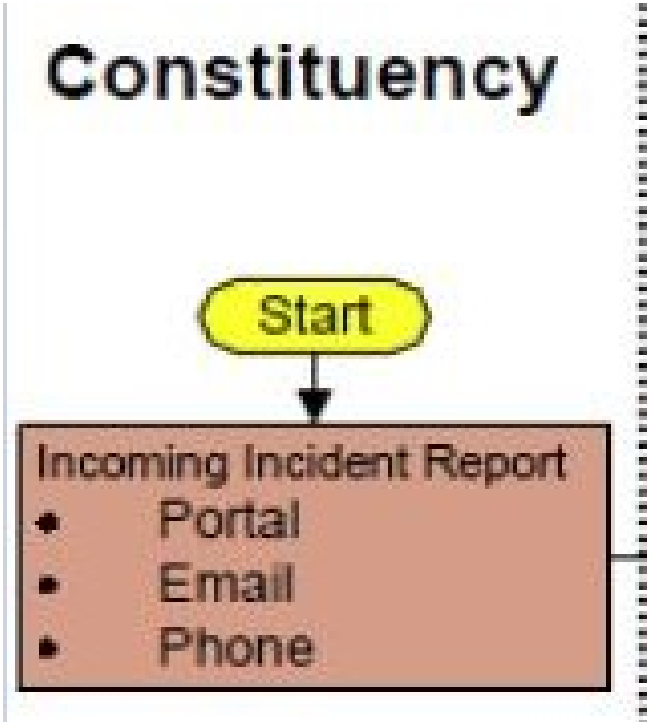
Game of Hats

Quantos chapéus é preciso num CSIRT?



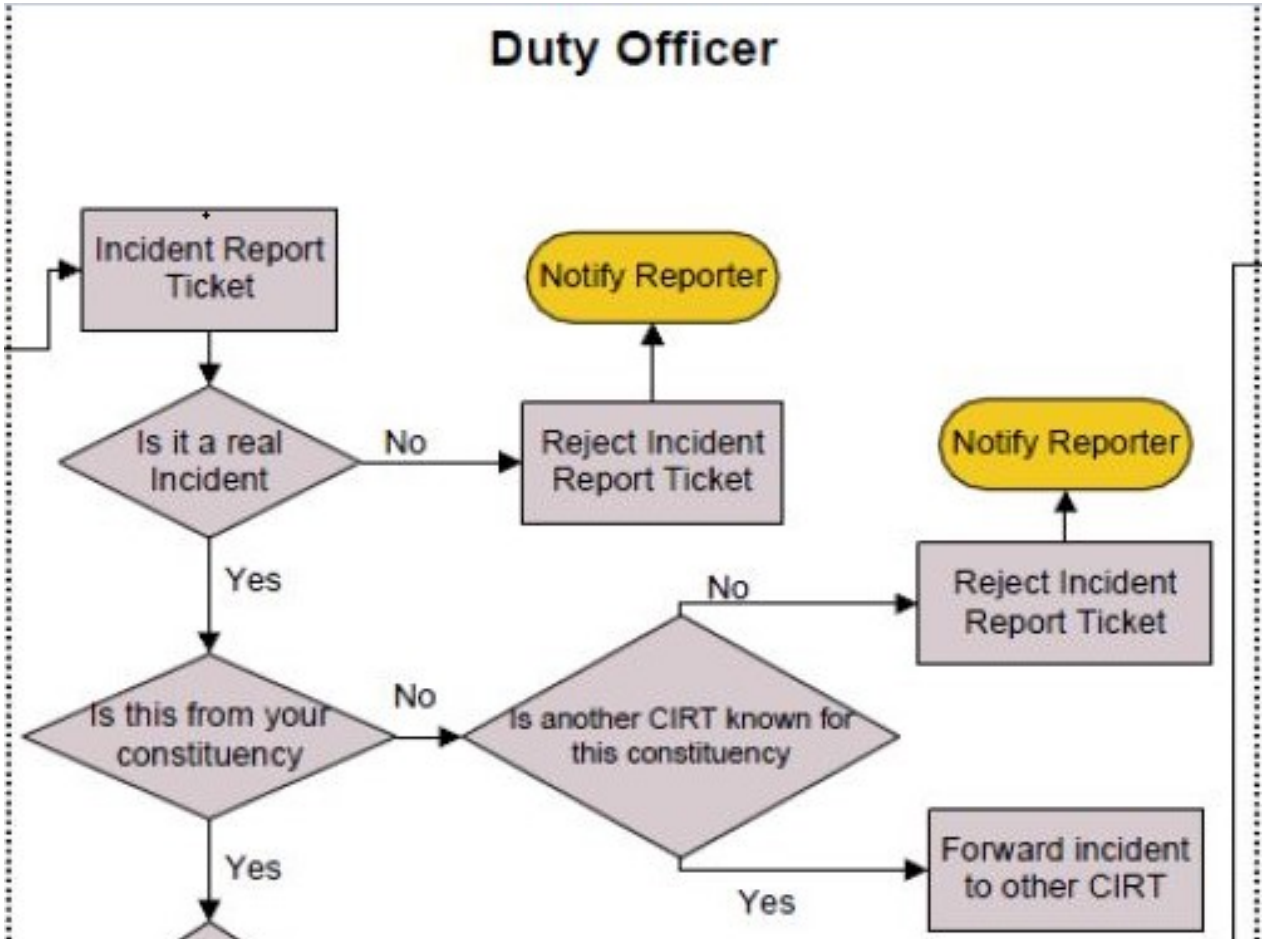
Game of Hats

Quantos chapéus é preciso num CSIRT?



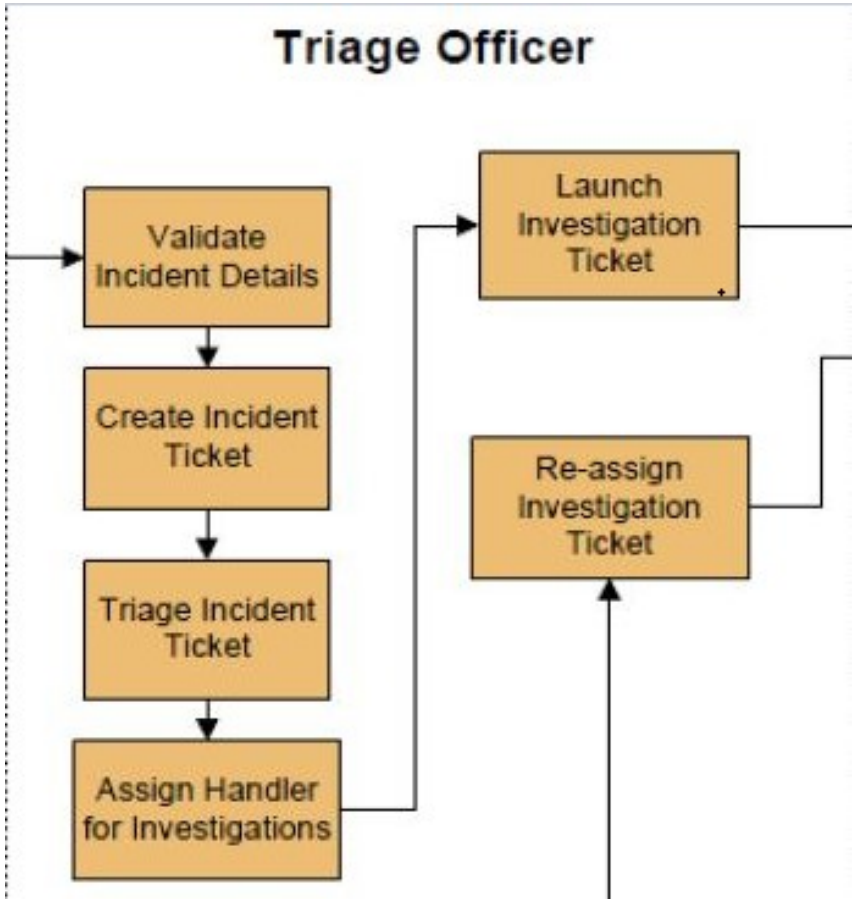
Game of Hats

Quantos chapéus é preciso num CSIRT?



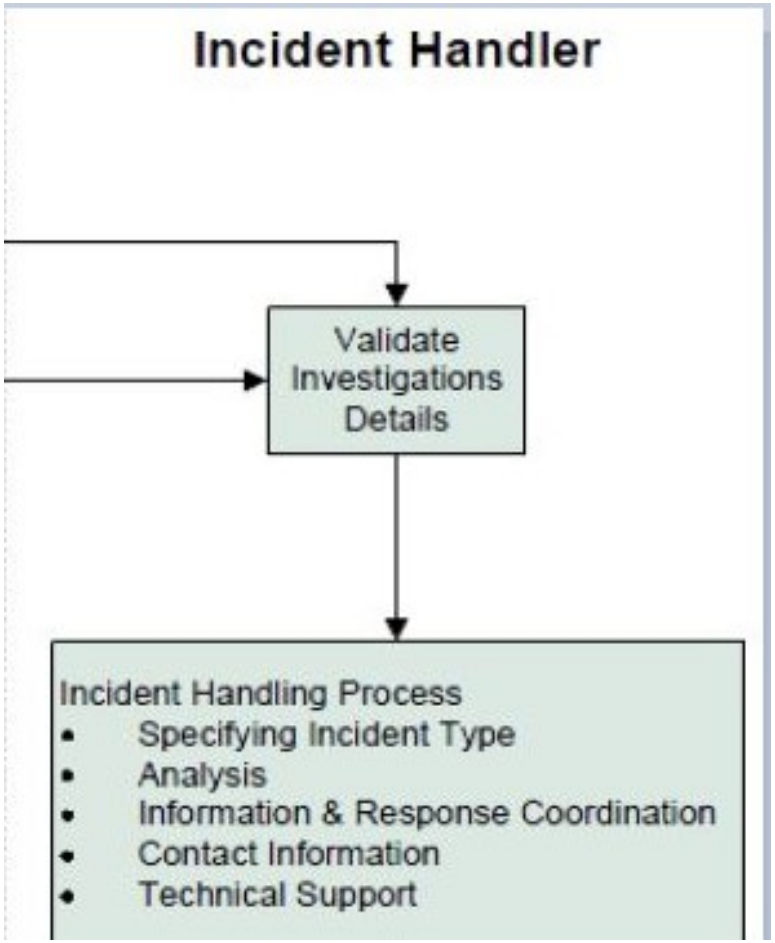
Game of Hats

Quantos chapéus é preciso num CSIRT?

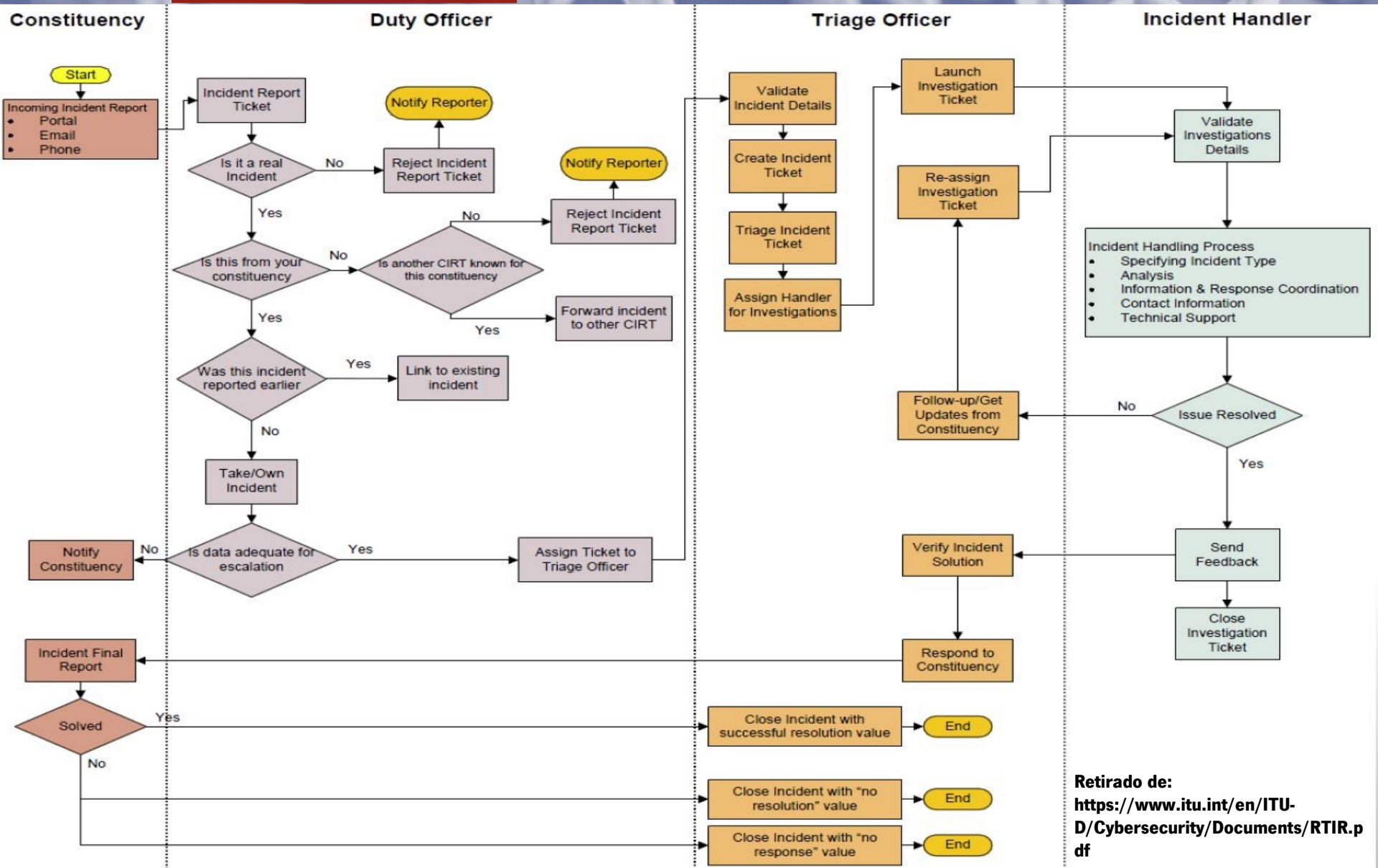


Game of Hats

Quantos chapéus é preciso num CSIRT?



Game of Hats



Retirado de: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RTIR.pdf

Game of Hats

É (relativamente) fácil ter um CSIRT

Basta usar chapéus!

Questões

UXVIc3TDtWVzPw==

marco@csirt.uminho.pt
www.csirt.uminho.pt

marco@scom.uminho.pt
www.scom.uminho.pt