

Coordenação e Colaboração

Filipa Macieira



Agenda

- Identificação
- Comunicação



IDENTIFICAÇÃO

Endereços IP

- Os incidentes estão associados quase sempre a endereços IP
- Como se associa um IP a uma entidade?
- É útil associar um IP a um país?
- Globalmente: Ecossistema de Regional Internet Registries (RIR)

WHOIS

- Protocolo WHOIS (WHO IS?)
 - Dono/Utilizador (de uma rede/domínio/...)
- Fontes autoritativas
 - whois.ripe.net
 - whois.arin.net
 - whois.apnic.net
 - whois.lacnic.net
 - whois.afrinic.net
- Cliente WHOIS ou via web



WHOIS

% Information related to '194.210.0.0 - 194.210.255.255'

% Abuse contact for '194.210.0.0 - 194.210.255.255' is 'report@cert.rcts.pt'

inetnum: 194.210.0.0 - 194.210.255.255
netname: PT-RCCN-951102
country: PT
org: **ORG-FpaC1-RIPE**
admin-c: JNF1-RIPE
tech-c: IF575-RIPE
status: ALLOCATED PA
mnt-by: RIPE-NCC-HM-MNT
mnt-by: AS1930-MNT
mnt-lower: AS1930-MNT
mnt-domains: AS1930-MNT
mnt-routes: AS1930-MNT
mnt-irt: IRT-RCTS-CERT
created: 1970-01-01T00:00:00Z
last-modified: 2016-07-20T13:38:30Z
source: RIPE



organisation: ORG-FpaC1-RIPE
org-name: Fundacao para a Ciencia e a Tecnologia, I.P.
org-type: LIR
address: Avenida do Brasil, 101
address: 1700-066
address: Lisboa
address: PORTUGAL
phone: +351218440100
fax-no: +351218472167

COMUNICAÇÃO

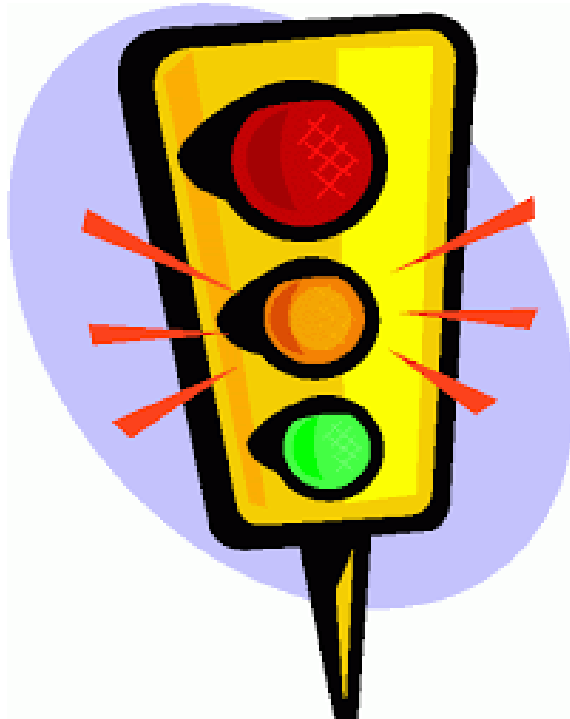
Eixos

- Respeito
- Humildade
- Entreajuda

Distribuição de Informação

- Tem que existir um conjunto de **regras**
- Com quem se pode **partilhar** determinada informação?
- Alicerce da **confiança** entre equipas e indivíduos

Traffic Light Protocol (TLP)



Traffic Light Protocol (TLP)

- **TLP:RED** = *Not for disclosure, restricted to participants only.*
 - Os destinatários não podem partilhar informação marcada como TLP:RED. No contexto de uma reunião, a informação TLP:RED é limitada ao conhecimento dos presentes na própria reunião.

Traffic Light Protocol (TLP)

- **TLP:AMBER** = *Limited disclosure, restricted to participants' organizations.*
 - Os remetentes poderão usar TLP:AMBER quando a informação requer ação por parte dos destinatários, podendo existir riscos para a privacidade, reputação ou operações se o conteúdo for partilhado com o exterior das organizações envolvidas. Os destinatários apenas podem partilhar informação TLP:AMBER com membros da própria organização e com clientes/parceiros que necessitam dela para se protegerem. **Os remetentes podem especificar limites adicionais para a partilha: o seu cumprimento pelos destinatários é obrigatório.**

Traffic Light Protocol (TLP)

- **TLP:GREEN** = *Limited disclosure, restricted to the community.*
 - A informação pode ser partilhada no interior de uma comunidade. Não devem ser usados canais de acesso público.

Traffic Light Protocol (TLP)

- **TLP:WHITE** = *Disclosure is not limited.*
 - Os remetentes podem usar TLP:WHITE quando a informação transporta um risco mínimo ou nenhum potencial de uso indevido. O conteúdo TLP:WHITE pode ser distribuído sem nenhuma restrição desde que observadas as regras de *copyright* aplicáveis.

Em Resumo



WHOIS é o protocolo que permite perceber a que operador (ou entidade) está associado um determinado endereço IP



O *Traffic Light Protocol* é o standard de-facto de classificação de informação usado na comunidade CSIRT



Obrigado