

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

Computação
Científica Nacional

RESPOSTA A INCIDENTES I

Fábio Mestre



Agenda

- Resposta a incidentes
- Notificação
- Triagem
- Resolução
- Análise posterior
- Duvidas e questões



RESPOSTA A INCIDENTES

Resposta a incidentes



NIST Incident Response Cycle



Resposta a incidentes

SANS 504-B Incident Response Cycle: Cheat-Sheet

v1.0, 11.5.2016 – kf / USCW

Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)



Incidente de Segurança

O que é?

- Um incidente de segurança é o resultado de uma ação ou conjunto de ações que podem dar origem à perda de:
 - Confidencialidade
 - Integridade
 - Disponibilidade



Incidentes de Segurança

Origem



Denúncias de atividades maliciosas



Deteção de atividades suspeitas



Anomalias face aos padrões de funcionamento da infraestrutura, aplicações ou equipamento

NOTIFICAÇÃO

Notificação

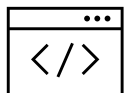
Canais de comunicação



Telefone



E-mail



Plataforma Web



Outros

Notificação Registo

- Um incidente de segurança deve ser sempre registado, de forma a manter um histórico de ocorrências.
- Deve ser utilizada um sistema ou ferramenta de gestão de incidentes centralizado.
- Automatização quando e onde for possível e adequado



Notificação

Ferramentas

- Algumas ferramentas de gestão de incidentes:
 - RTIR (Request Tracker Incident Response)
 - BMC Helix ITSM (Remedy)
 - Jira ITSM
 - STORM OTRS
 - osTicket
 - Outros...



⚡ Jira Service Management

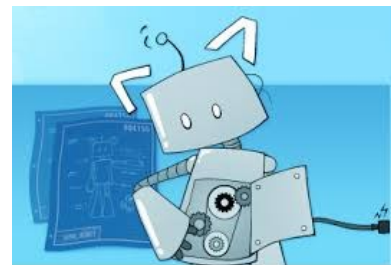


Notificação

Ferramentas – RTBOT & Dispatcher

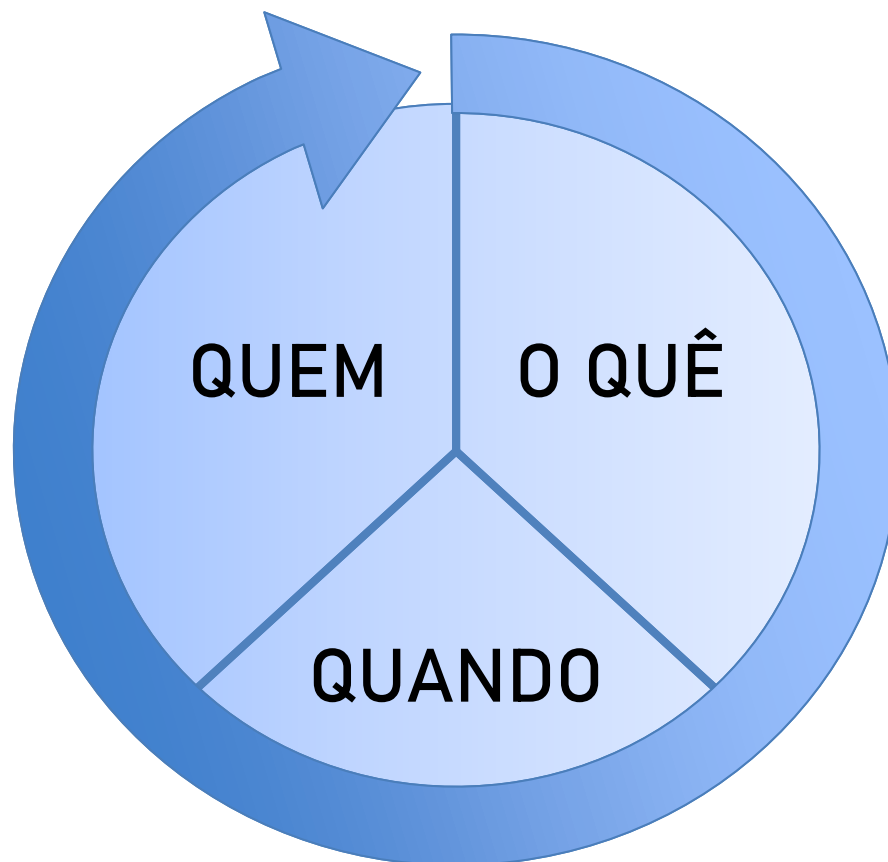


Dispatcher, 911 what is your emergency?



TRIAGEM

Triagem de incidentes



Triagem de incidentes

Como efetuar a triagem?

- É mesmo um incidente de segurança?
- Quem reportou o incidente?
- Faz parte do nosso âmbito?
- Qual o impacto e a criticidade?
- Que recursos necessitamos para o tratamento?
- Quem deve tratar do incidente?



Triagem de incidentes

Verificação



- Incidente recebido ✓



- Como será processado?



- O que pode ser esperado?



- O que se pode fazer entretanto?

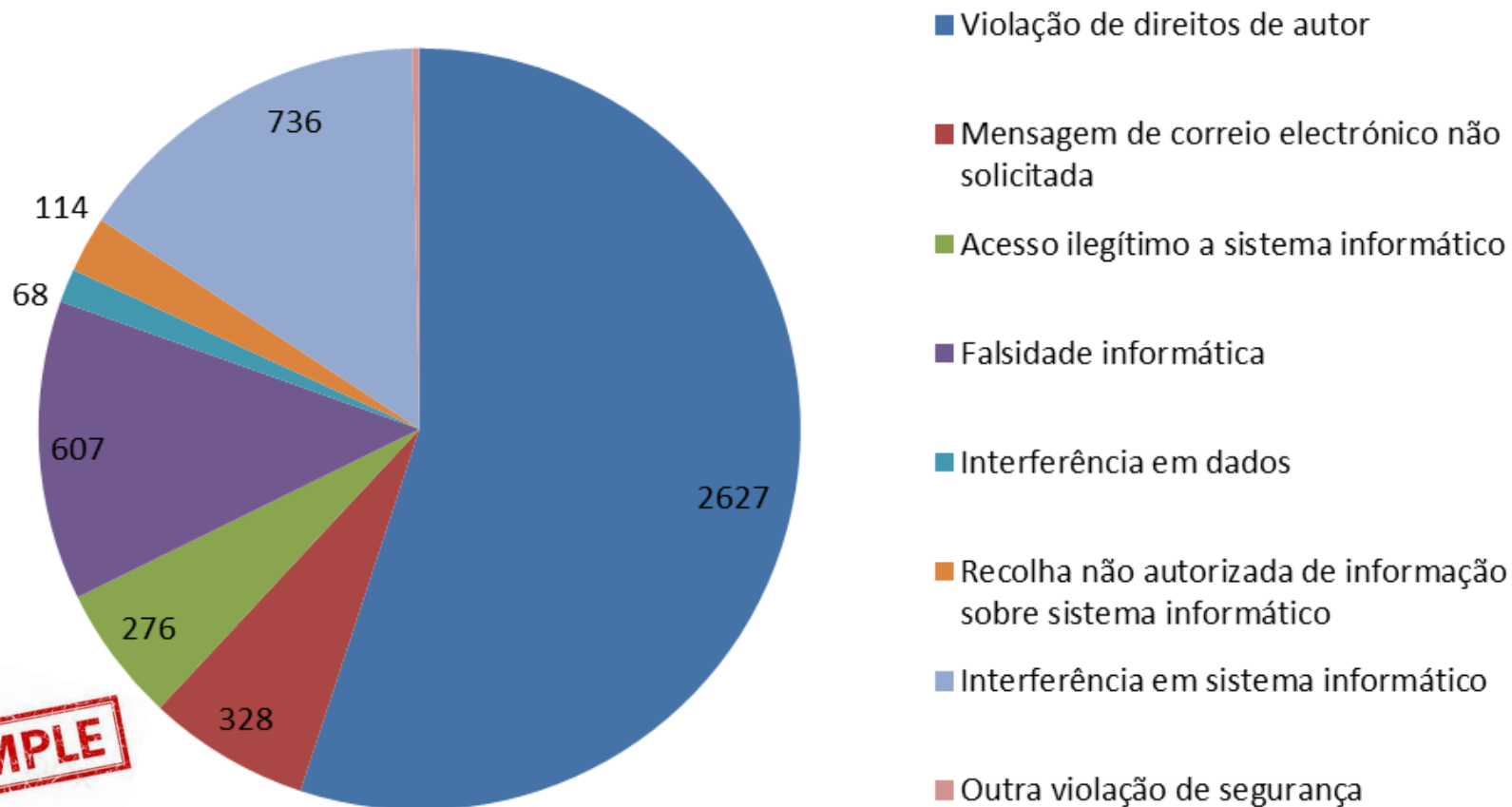
Triagem de incidentes

Classificação

- Taxonomias mais populares nos CSIRT:
 - Common language for incident response
 - By Carnegie Mellon University
 - Taxonomia eCSIRT.net
 - Desenvolvida durante o projeto eCSIRT.net
 - Taxonomia própria
 - Baseada em experiência
- Taxonomia usada na RCTS (e RNCSIRT):
 - https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf

Triagem de incidentes

Classificação



Triagem de incidentes

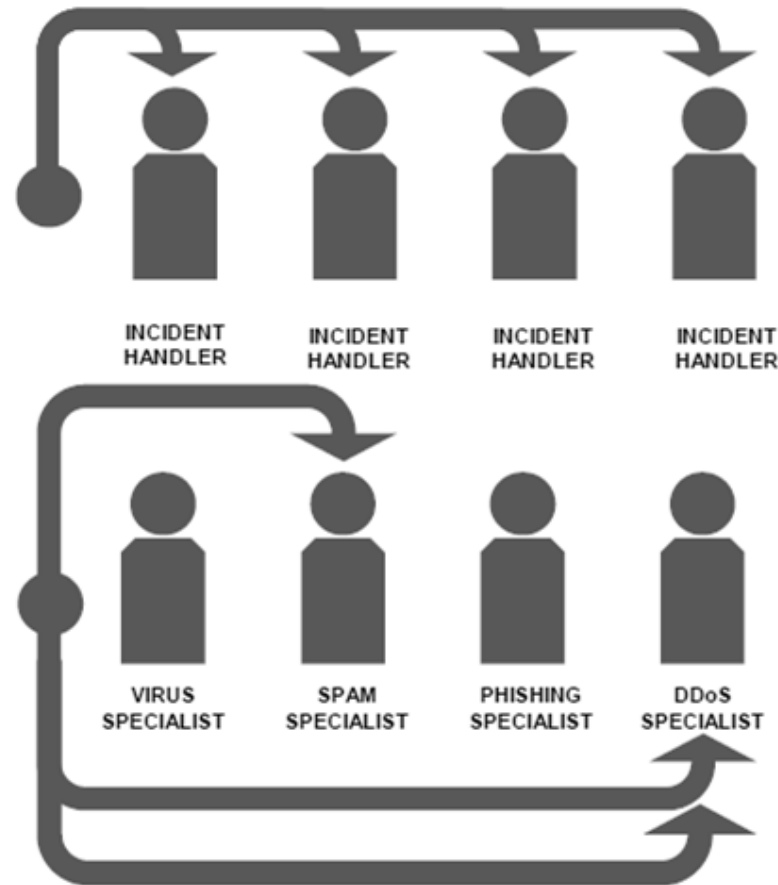
Classificação

- Classificar incidentes dá-nos a capacidade de:
 - Reconhecer tendências
 - Extrair estatísticas
 - Comparar dados
 - Ver parte do panorama de ameaças
- Desafios:
 - Ambiguidades
 - Perda de tempo com “sobre-classificações” (demasiados tipos de classificação)



Triagem de incidentes

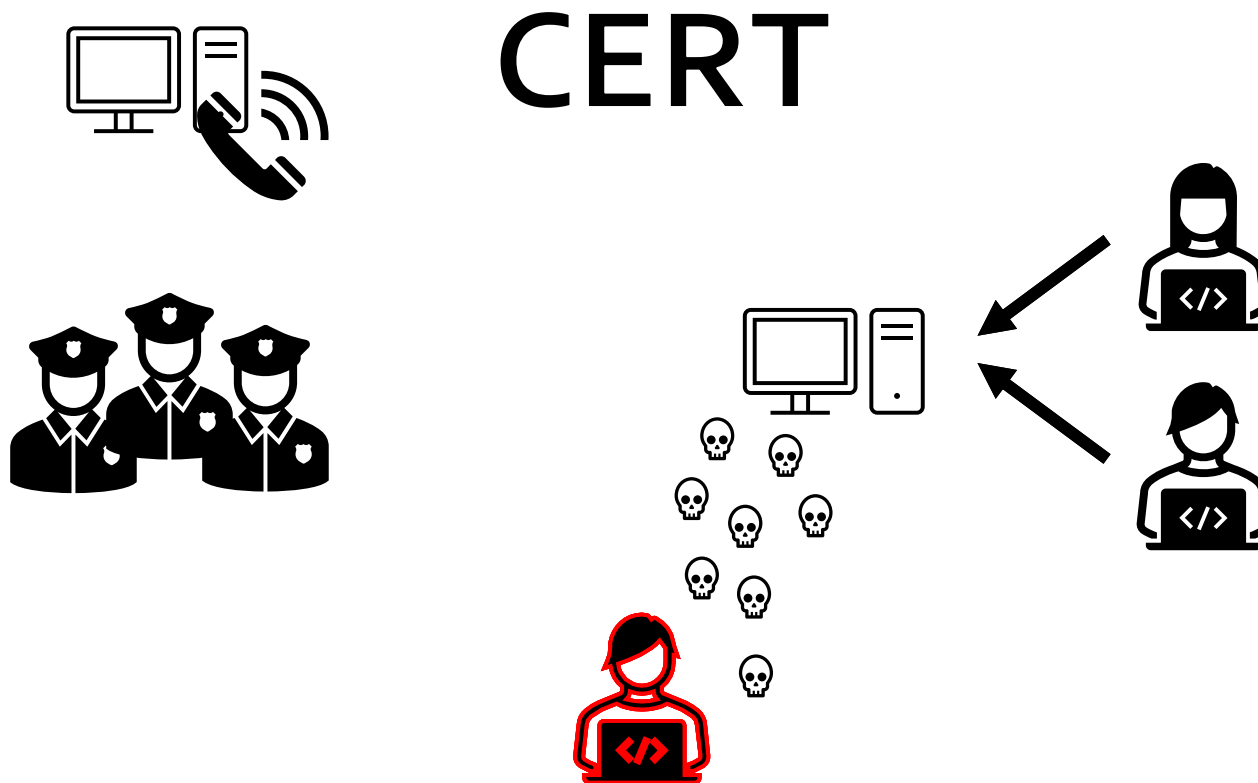
Atribuição



RESOLUÇÃO

Resolução de incidentes

Cooperação



Resolução de incidentes

Análise

- Devem ser analisadas e discutidas as observações e conclusões da resolução do incidente.
- Sessões de “brainstorming” são úteis para casos complexos e sofisticados.
- Devem ser selecionados os dados que contêm a informação mais importante ou de fontes de maior confiança.



Resolução de incidentes

Medidas

- As medidas propostas podem ser diferentes para diferentes intervenientes
- Podem-se propor medidas de remediação na fonte.
- A influência sobre terceiros é limitada, pelo que as medidas propostas também podem ser, consoante o interveniente.



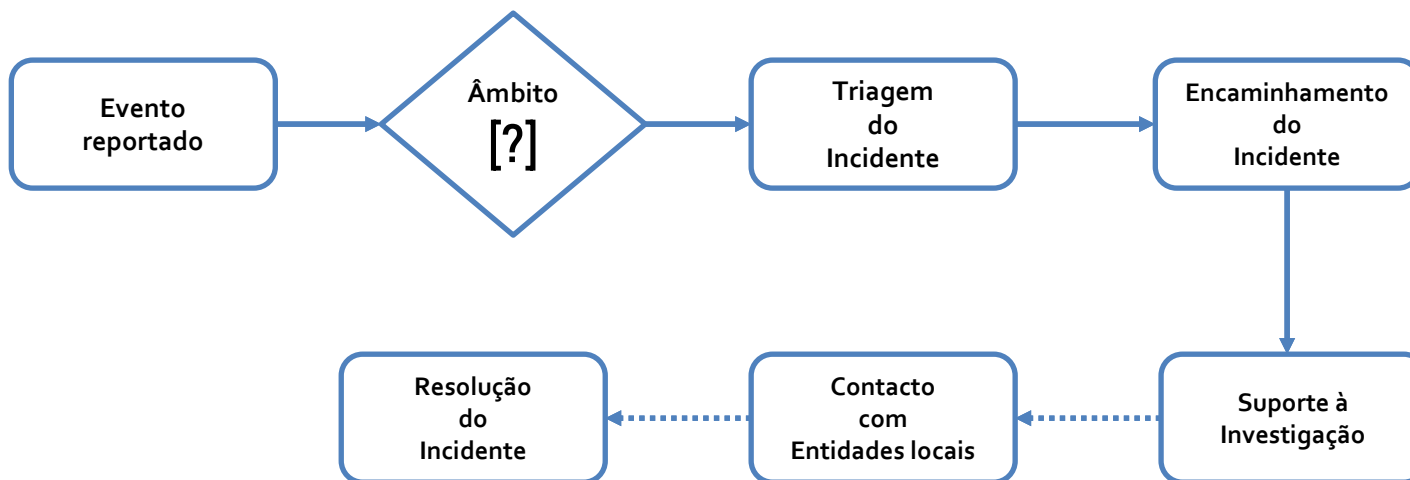
Resolução de incidentes

Recomendações

- É necessário analisar a anatomia do ataque para aprender como o evitar no futuro
- Deve-se tirar partido da informação sobre fragilidades, obtida através do incidente e usá-la para efetuar melhorias
- Deve ser partilhada informação relevante frequentemente com a comunidade de CSIRTS

Gestão de incidentes

Resumo - Workflow



ANÁLISE POSTERIOR

Análise posterior

Exemplo de agenda para uma reunião pós-incidente:

- a) Informação estatística das últimas n semanas
- b) Curta apresentação sobre os n incidentes mais interessantes
- c) Análise detalhada de um determinado incidente
- d) Discussão:
 - Lições extraídas
 - Fragilidades conhecidas
 - Propostas de melhoria



Em Resumo



A resposta a incidentes é um fluxo processual composto por várias fases importantes.



A utilização de uma ferramenta de gestão de incidentes é essencial.



Cada incidente deve ter uma conclusão e um rescaldo, permitindo a aprendizagem contínua.



Obrigado