Questões Endereçadas para Incidentes de Segurança

Existe algum tipo de prevenção para este incidente? Se sim, qual(is)?
Os sistemas envolvidos tinham visibilidade suficiente? Se sim, qual(is)?
Este risco era conhecido?
Quando o incidente aconteceu? (timestamp)
Quando o incidente foi detectado? (timestamp)
Quem detectou o incidente?
Como o incidente foi detectado? (evidências)
Foi possível identificar o autor? Se sim, como? (evidências)
Identificação do autor?
Classificação do autor?
Quais sistemas foram envolvidos?
Quais sistemas/artefatos foram comprometidos?
Classificação do Incidente?
Descrição do incidente?
Classificação da causa raiz do incidente?
Qual foi a causa raiz do incidente?
Quando o incidente foi contido? (timestamp)
Quem trabalhou na contenção do incidente?
Como o incidente foi contido? (evidências)
Foi possível identificar todo o impacto causado pelo incidente?
Qual foi o impacto técnico do incidente? (evidências)
Qual foi o impacto ao negócio?
O incidente foi devidamente priorizado?
O que deve ser feito para que este tipo de incidente não aconteça novamente?
O que deve ser feito para melhorar a tratativa deste tipo de incidente?
Na sua opinião, o que poderia ser melhor na próxima resposta a incidente?