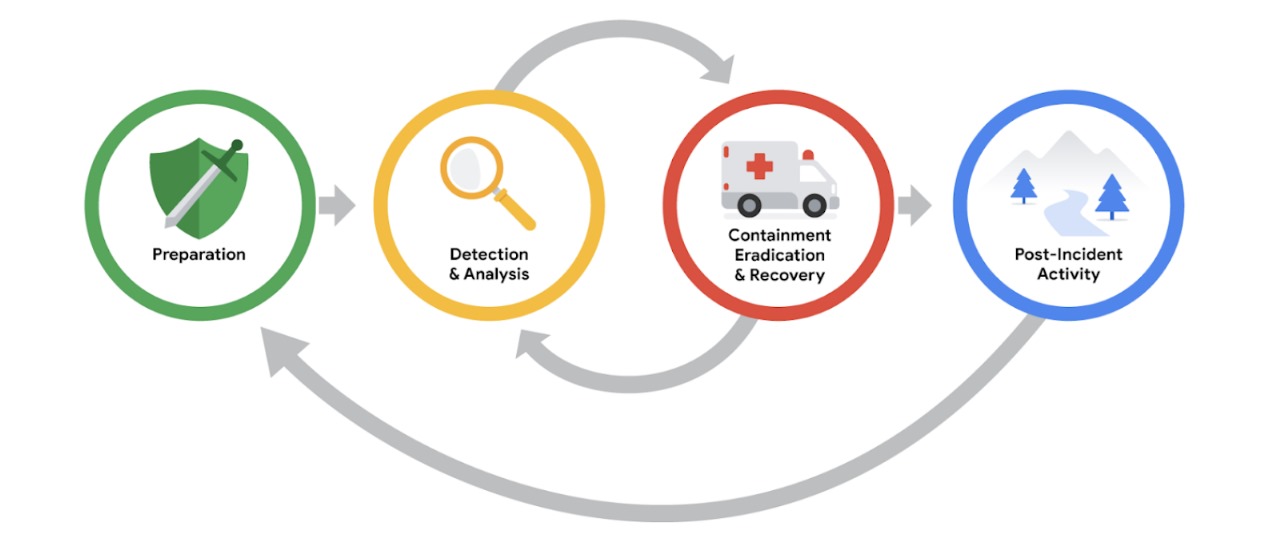
Revisão pós-incidente

Anteriormente, você explorou a fase de Contenção, Erradicação e Recuperação do Ciclo de Vida de Resposta a Incidentes da NIST. Esta leitura explora as atividades envolvidas na fase final do ciclo de vida: **Atividade pós-incidente**. Como analista de segurança, é importante se familiarizar com as atividades envolvidas nessa fase porque cada incidente de segurança lhe dará a oportunidade de aprender e melhorar suas respostas a futuros incidentes.

**Atividade pós-incidente**

A fase de atividade pós-incidente do ciclo de vida de resposta a incidentes do NIST é o processamento da revisão de um incidente para identificar áreas de melhoria durante o tratamento do incidente.



**Lições aprendidas**

Após uma organização ter conseguido conter, erradicar e se recuperar de um incidente, o incidente chega ao fim. Entretanto, isso não significa que o trabalho dos profissionais de segurança esteja concluído. Os incidentes oferecem às organizações e às suas Equipes de segurança uma oportunidade de aprender com o que aconteceu e priorizar maneiras de melhorar o processo de tratamento de incidentes.

Isso geralmente é feito por meio de uma **reunião de Lições aprendidas**, também conhecida como análise post-mortem. Uma reunião de Lições aprendidas inclui todas as partes envolvidas após um incidente grave. Dependências do escopo de um incidente, várias reuniões podem ser programadas para reunir dados suficientes. O objetivo dessa reunião é avaliar o incidente em sua totalidade, avaliar as ações de resposta e identificar quaisquer áreas de melhoria. Ela oferece uma oportunidade para que a organização e seu pessoal aprendam e melhorem, e não para atribuir culpa. Essa reunião deve ser agendada no máximo duas semanas após o incidente ter sido remediado com sucesso.

Nem todos os incidentes exigem sua própria reunião de Lições aprendidas; o tamanho e a gravidade de um incidente ditarão se a reunião é necessária. No entanto, os principais incidentes, como ataques de ransomware, devem ser analisados em uma reunião dedicada às Lições aprendidas. Essa reunião é composta por todas as partes que participaram de qualquer aspecto do processamento da resposta ao incidente. Aqui estão alguns exemplos de perguntas que são abordadas nessa reunião:

* O que aconteceu?
* A que horas aconteceu?
* Quem descobriu o incidente?
* Como foi feita a contenção?
* Quais foram as medidas tomadas para a recuperação?
* O que poderia ter sido feito de forma diferente?

Além de ter a oportunidade de aprender com o incidente, há outros Benefícios em realizar uma reunião de Lições aprendidas. Para grandes organizações, as reuniões de Lições aprendidas oferecem uma plataforma para que os Membros da equipe de todos os departamentos compartilhem informações e recomendações para prevenção futura.

**Dica profissional**: antes de uma equipe realizar uma reunião de Lições aprendidas, os organizadores devem certificar-se de que todos os participantes estejam preparados. Normalmente, os anfitriões da reunião desenvolvem e distribuem uma Agenda com antecedência, que contém os tópicos de discussão e garante que os participantes estejam informados e preparados. Além disso, as Funções da reunião devem ser designadas com antecedência, incluindo um moderador para liderar e facilitar a discussão e um escrevente para fazer as anotações da reunião.

**Recomendações**

As reuniões de Lições aprendidas oferecem oportunidades de crescimento e melhoria. Por exemplo, as Equipes de segurança podem identificar erros nas ações de resposta, lacunas nos processos e procedimentos ou Controles de segurança ineficazes. Uma reunião de Lições aprendidas deve resultar em uma lista de ações priorizadas ou recomendações acionáveis destinadas a melhorar os processos de processamento de incidentes e a postura geral de segurança de uma organização. Isso garante que as organizações estejam implementando as Lições aprendidas após um incidente para que não fiquem vulneráveis a sofrer o mesmo incidente no futuro. Exemplos de mudanças que podem ser implementadas incluem a atualização e o aprimoramento das instruções do manual ou a implementação de novas ferramentas e tecnologias de segurança.

**Relatório final**

Ao longo deste curso, você explorou a importância da documentação para o registro de detalhes durante o ciclo de vida da resposta a incidentes. No mínimo, a documentação de resposta a incidentes deve descrever o incidente, abrangendo os 5 Ws da investigação de incidentes: *quem*, *o quê*, *onde*, *por que* e *quando.* Os detalhes capturados durante a resposta ao incidente são importantes para o desenvolvimento de documentos adicionais durante o final do ciclo de vida.

Uma das formas mais essenciais de documentação criada durante o final de um incidente é o **relatório final**.O relatório final fornece uma análise abrangente de um incidente. Os relatórios finais não são padronizados e seus formatos podem variar entre as organizações. Dependências, vários relatórios finais podem ser criados, dependendo do público para o qual foram escritos. Aqui estão alguns exemplos de elementos comuns encontrados em um relatório final:

* **Resumo executivo**: um resumo de alto nível do relatório, incluindo as principais descobertas e fatos essenciais relacionados ao incidente
* **Linha do** tempo: uma linha do tempo cronológica detalhada do incidente que inclui registros de data e hora que datam a sequência de eventos que levaram ao incidente
* **Investigação**: Uma compilação das ações tomadas durante a detecção e análise do incidente. Por exemplo, a análise de um Artefato de rede, como uma captura de pacote, revela informações sobre as atividades que ocorrem em uma rede.
* **Recomendações**: Uma lista de ações sugeridas para prevenção futura

**Dica profissional**: ao escrever o relatório final, considere o público para o qual está escrevendo o relatório. Muitas vezes, executivos de negócios e outros profissionais que não são da área de segurança e que não têm o conhecimento necessário para entender detalhes técnicos lerão os relatórios finais pós-incidente. Considerar o público-alvo ao redigir um relatório final o ajudará a comunicar com eficácia os detalhes mais importantes.

**Principais conclusões**

As ações pós-incidente representam o fim do ciclo de vida da resposta a incidentes. Essa fase oferece a oportunidade para as equipes de segurança se reunirem, avaliarem as ações de resposta, fazerem recomendações de melhoria e desenvolverem o relatório final.

Marcar como concluído

Curtir

Não curtir

Relatar problema