# Respondendo a incidentes

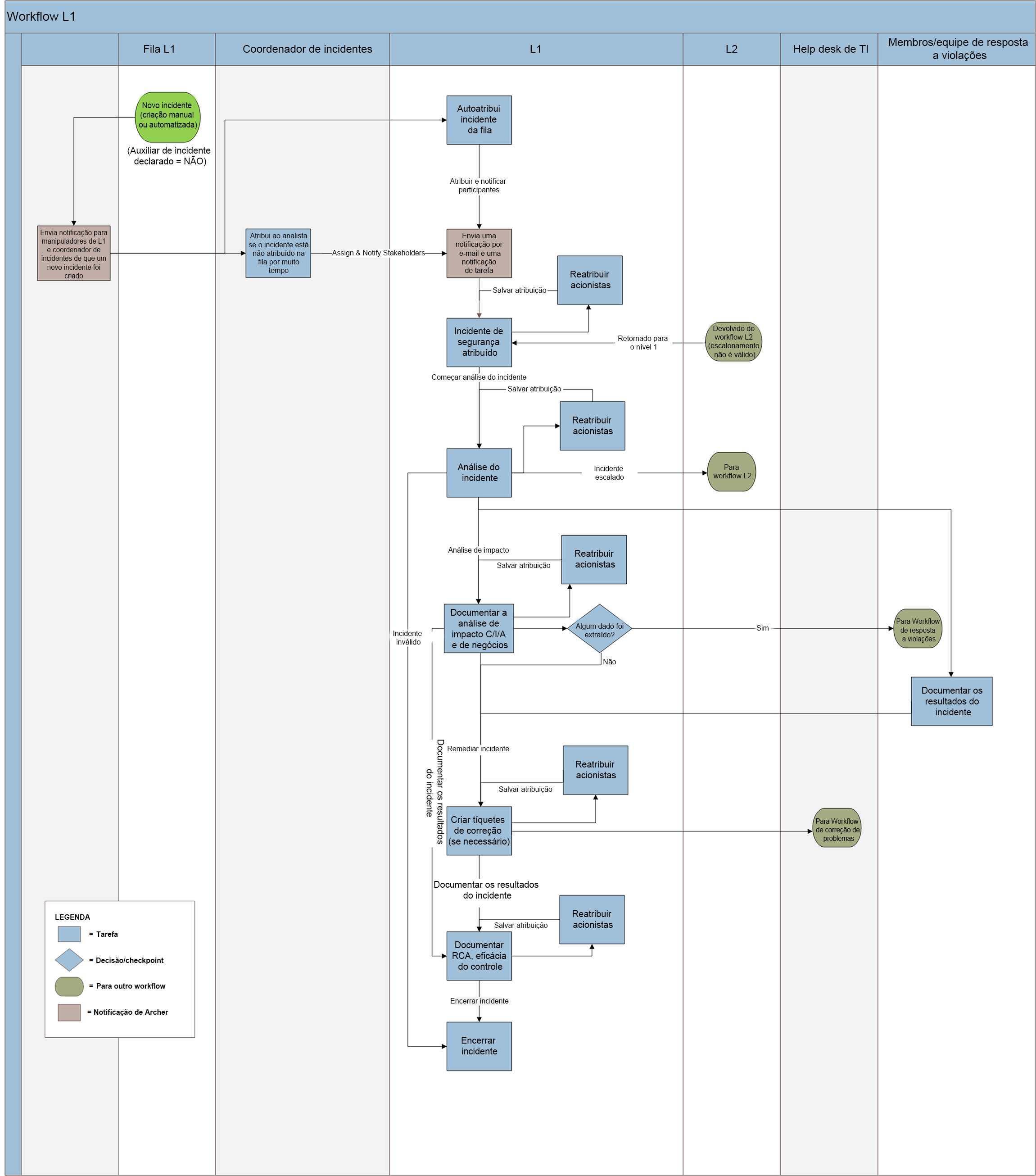
Nesta página

* [Workflow de resposta a incidentes – L1](#WorkflowderespostaaincidentesL1)
* [Workflow de resposta a incidentes – L2](#WorkflowderespostaaincidentesL2)
* [Alertas de segurança versus incidentes de segurança](#X3b191982d5d4014dd9ce8679725ddb10958c876)
* [Agregando vários alertas a um só incidente](#Xbaa5d6a648f86d5b9b92d73fadebc91722aa0fb)
* [Responder a incidentes](#Responderaincidentes)

## Workflow de resposta a incidentes – L1

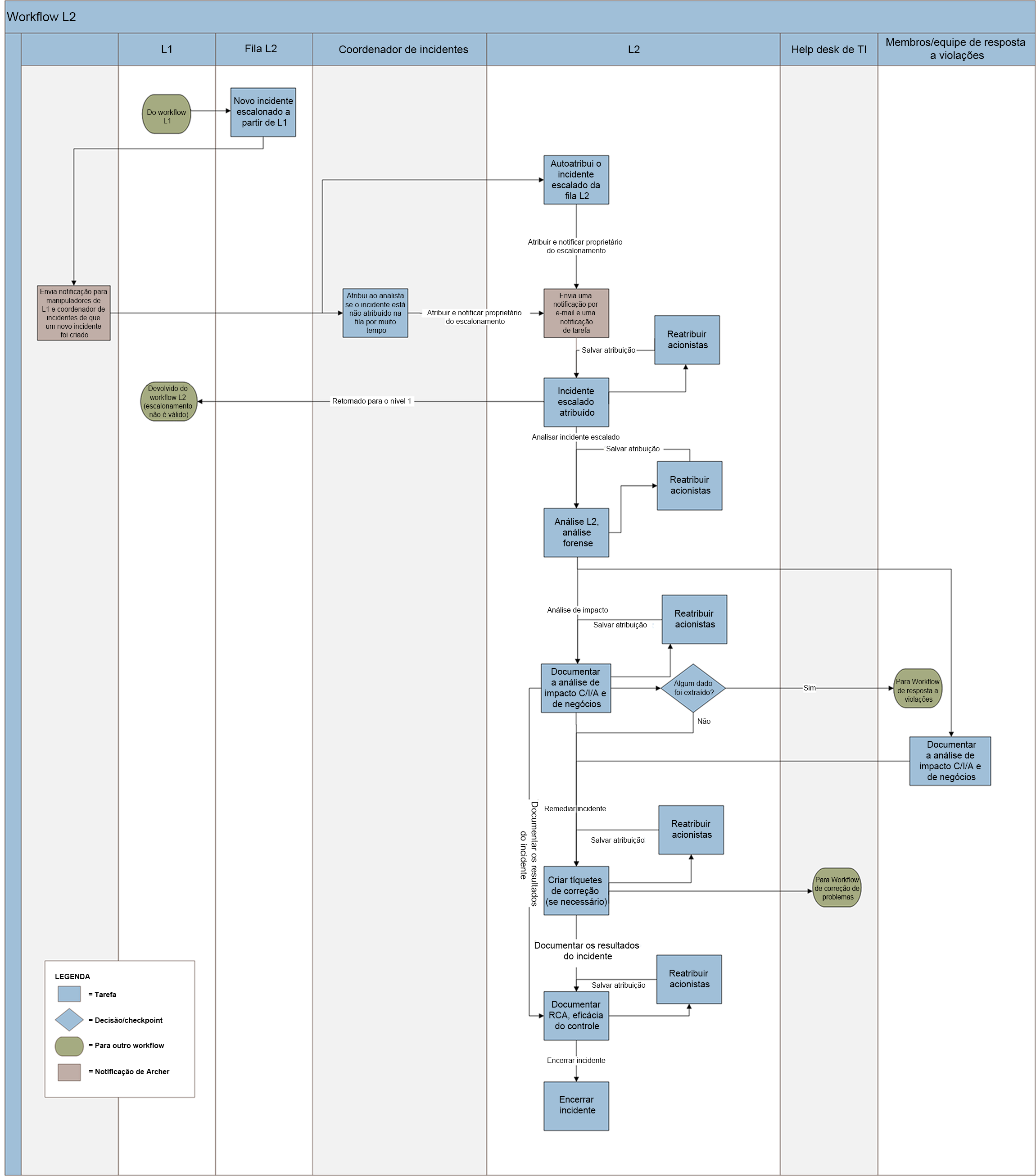
O caso de uso Cyber Incident & Breach Management foi desenvolvido para permitir os workflows de resposta a incidentes a seguir.

Faça download do arquivo de origem do diagrama aqui: [Diagrama de workflow de Cyber Incident & Breach Response L1](../../Resources/Images/Solutions/ITSecRisk/itsrm_cibr_incident_resp_wf_L1.vsd)



## Workflow de resposta a incidentes – L2

Faça download do arquivo de origem do diagrama aqui: [Diagrama de workflow de Cyber Incident & Breach Response L2](../../Resources/Images/Solutions/ITSecRisk/itsrm_cibr_incident_resp_wf_L2.vsd)



**Observação:** O workflow de gerenciamento de problemas só estará disponível se você tiver licenciado o Issues Management.

**Observação:** Os diagramas só incluem as notificações que são essenciais para os workflows. Para obter uma lista completa das notificações, consulte o *Dicionário de dados*.

## Alertas de segurança versus incidentes de segurança

Um alerta de segurança é um evento correlacionado com uma consequência negativa, como falhas no sistema, inundações de pacotes, uso não autorizado de privilégios do sistema, acesso não autorizado a dados confidenciais e execução de malware que destrói os dados ou uma combinação de 1 ou mais desses eventos.

Um incidente de segurança é um grupo distinto de alertas de segurança que envolvem invasores específicos, ataques, objetivos, locais e regulagem que resultam em uma violação ou ameaça iminente de violação de políticas de segurança de computador, políticas de uso aceitável ou práticas de segurança padrão.

O Cyber Incident & Breach Response pode coletar alertas de ferramentas SIEM e agregar alertas em incidentes, pode coletar incidentes do NetWitness ou permite criar um incidente manualmente. Dados de alerta são armazenados no aplicativo Alertas de segurança e os incidentes agregados são criados no aplicativo Incidentes de segurança

Um incidente de segurança pode ser composto por vários alertas de segurança, porém, só é possível vincular um alerta de segurança a um único incidente de segurança. É preciso vincular todos os alertas a um incidente.

## Agregando vários alertas a um só incidente

O NetWitness Respond coleta alertas de várias origens e permite configurar regras para agregar alertas em incidentes de modo que os manipuladores de incidentes possam investigar e remediar vários alertas no contexto de um só incidente.

Se você estiver usando uma ferramenta SIEM de terceiros como fonte de alerta, o UCF permitirá definir os critérios de agregação pelos quais os alertas serão agrupados em incidentes.

Em ambos os casos, a adição de alertas a um incidente continua de acordo com os critérios de agregação até que o incidente seja atribuído.

## Responder a incidentes

1. Crie um incidente e atribua as partes interessadas usando um dos seguintes métodos:
   * Automaticamente, usando o UCF (Unified Collector Framework) ou o NW IM Integration Service para agregar alertas de uma ferramenta SIEM a incidentes
   * Manualmente, no aplicativo Incidentes de segurança do Archer, ou pelo feed de dados.
2. Inicie a revisão do incidente analisando todas as informações que foram apresentadas até o momento e determina o coordenador do incidente apropriado e os membros adicionais da equipe.
3. Analise as informações no registro de incidente, incluindo todos os alertas e detalhes de alerta que correspondem ao incidente e quaisquer procedimentos e tarefas de resposta a incidentes gerados automaticamente. Além disso, as partes interessadas também podem adicionar manualmente procedimentos ou tarefas, conforme necessário, vincular o registro a incidentes relacionados e substituir a prioridade do incidente.
4. Atribua o registro do incidente ao proprietário do escalonamento.
5. Analise o incidente escalado.
   1. Analise o incidente escalado atribuído e determine se o escalonamento é válido. Dependendo da validade do escalonamento, prossiga para analisar o incidente, solicite informações adicionais ou reatribua as partes interessadas.
   2. Durante a análise do incidente escalado, conclua a análise de investigação do incidente, uma análise jurídica e também analise quaisquer procedimentos e tarefas de resposta ao incidente gerados automaticamente com base na categoria de ameaça. Se necessário, o manipulador L2 também pode adicionar outros procedimentos e tarefas de resposta ao incidente e documentar detalhes de investigação do incidente nas entradas do registro.
   3. Depois de confirmar um comprometimento da segurança, você precisa documentar o impacto do incidente. Você pode documentar o impacto do incidente sobre negócios, políticas corporativas, confidencialidade, integridade e disponibilidade. Se tiver sido identificada uma perda de dados, você também poderá reportar uma violação de dados.
6. Para cada problema que precisa de remediação, crie um registro de resultados na guia Remediação do registro de incidente de segurança. Descreva a ação a ser concluída, a relevância para o resultado, uma fila de destino e um tipo de tarefa de remediação.
7. Documenta a análise do incidente. Forneça os resultados do incidente, os atores e as técnicas que contribuíram para o incidente, os detalhes de destino do incidente e adicione os controles de segurança associados à descoberta do incidente.