# Monitorando o progresso dos incidentes usando medições de SLA

O Archer Cyber Incident & Breach Response inclui métricas e relatórios integrados que fornecem às organizações de SOC percepções sobre onde as equipes estão gastando mais tempo no processo do incidente.

Nesta página

* [Acompanhar o tempo total](#Acompanharotempototal)
* [Status do incidente](#Statusdoincidente)

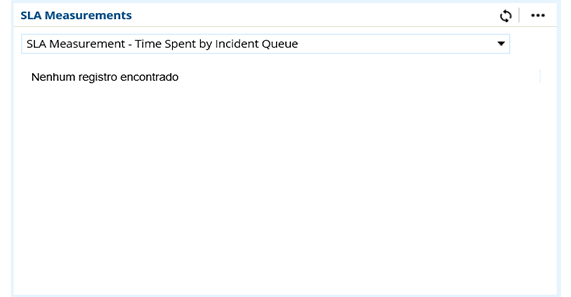
## Acompanhar o tempo total

O Archer usa cálculos para rastrear o tempo total gasto por manipuladores L1 e L2, bem como o tempo gasto por status (ou o tempo em que um registro de incidente permanece em cada fase do workflow avançado do incidente de segurança).

Se um manipulador N2 atribuir o registro do incidente ao manipulador N1, o Archer rastreará quanto tempo cada usuário gastou nessa fase específica.

Por exemplo, se um manipulador L2 gastou 10 minutos em um registro de incidente com status Em andamento antes da reatribuição a um manipulador L1 que, em seguida, gastou 30 minutos no registro (enquanto ele mantinha o estado Em andamento), o tempo total por status deve aparecer da seguinte forma:

o Tempo na fila L1 e L2 é calculado com base no tempo total gasto nas respectivas filas dos incidentes menos o tempo em que o registro manteve o status Correção.



## Status do incidente

A tabela a seguir descreve como o cálculo de tempo gasto por status é baseado nas atualizações de status.

| Status do incidente | Descrição |
| --- | --- |
| Novos | Status padrão na criação de um registro. |
| Atribuído | O incidente foi atribuído a um manipulador de incidentes N1, mas ele ainda não começou a trabalhar no incidente. |
| Em andamento | O manipulador de incidentes N1 começou a trabalhar no incidente. |
| Escalado | O manipulador de incidentes N1 escalou o incidente para um manipulador de incidentes N2.  Um registro de incidente permanece no status Escalado até que o processo de escalonamento do incidente seja concluído. Quando o Archer calcula o tempo gasto sob o status Escalado, o sistema obtém o tempo geral total gasto sob o status Escalado, que inclui o tempo gasto em cada uma das seguintes fases do escalonamento:   * Status de escalonamento: Novo * Status de escalonamento: Atribuído * Status de escalonamento: Análise jurídica em andamento * Status de escalonamento: Análise jurídica concluída |
| Retornado para o nível 1 | O manipulador de incidentes L2 analisou o incidente e descobriu que o escalonamento não é válido. Por exemplo, o manipulador de incidentes N1 pode ter deixado de fazer verificações antes de escalar o incidente. |
| Remediação necessária | O manipulador de incidentes N2 concluiu suas análises e encontrou itens que exigem remediação. |
| Remediação concluída | A remediação necessária foi concluída. |
| Inválido | Após a análise, as informações no incidente não indicam comprometimento de segurança ou atividade mal-intencionada. |
| Fechado | Todas as tarefas foram resolvidas e o incidente não está vinculado a nenhuma investigação ou violação aberta. |