# Archer Cyber Incident & Breach Response 2024.03

A Cyber Incident & Breach Response do Archer permite catalogar ativos organizacionais e de TI de forma centralizada, estabelecendo o contexto de negócios para impulsionar a priorização de incidentes e implementar processos projetados para escalonar, investigar e resolver incidentes declarados. O caso de uso foi projetado de forma que as equipes trabalhem de modo eficaz por meio de procedimentos definidos para triagem e resposta a incidentes, preparando-se contra uma possível violação de dados.

Nesta página

* [Benefícios do caso de uso Cyber Incident & Breach Response](#X2f92f3f6402c32c830cbd7d3c4e7192fcaabc00)
* [Como a Cyber Incident & Breach Response se enquadra em um programa de risco e conformidade](#Xb8c18cde06f332c29e209dd8e6009d7dfe0a495)
  + [Casos de uso de pré-requisito e seguintes](#Casosdeusodepr%C3%A9requisitoeseguintes)
  + [Casos de uso relacionados em outras áreas de solução](#X4c9f0ed4225641c1ff1d4f7f9a8426f7ce40e4b)
* [Introdução](#Introdu%C3%A7%C3%A3o)

## Benefícios do caso de uso Cyber Incident & Breach Response

Os workflows e relatórios integrados foram desenvolvidos para que os gerentes de segurança assumam o controle dos problemas mais urgentes e simplifiquem processos. Os problemas relacionados a investigações de incidentes declarados podem ser monitorados e gerenciados em um portal centralizado com visibilidade completa e geração de relatórios. Se um incidente se transformar em uma violação de dados, workflows e avaliações integrados já criados estarão disponíveis para ajudar a mais ampla equipe comercial da empresa a trabalhar com a equipe de segurança e reagir apropriadamente.

Com a Cyber Incident & Breach Response do Archer, os eventos de segurança e cibernéticos declarados podem ser escalonados com consistência e rapidez. O workflow avançado e a percepção sobre a velocidade dos incidentes de segurança e cibernéticos declarados permitem uma utilização mais eficiente dos recursos da equipe de segurança, resultando em mais rapidez nas taxas de análise, resposta e encerramento de incidentes de segurança críticos. Com processos e recursos aprimorados, a equipe de segurança pode aproveitar com mais eficiência a infraestrutura existente (como SIEMs, tecnologias para segurança de endpoint e ferramentas de captura de pacotes e registros) para se concentrar nos incidentes que causam mais impacto. Esses recursos melhoram o preparo da equipe de segurança em caso de incidentes graves que envolvam possíveis violações de dados, aumentando o retorno sobre os investimentos em infraestrutura, reduzindo também o risco de segurança geral.

Para obter os principais recursos e benefícios deste caso de uso, consulte o Data sheet na Archer Community: <https://www.archerirm.community/t5/solution-use-case-overviews/archer-solutions-amp-use-cases/ba-p/572564>

## Como a Cyber Incident & Breach Response se enquadra em um programa de risco e conformidade

A Cyber Incident & Breach Response é um caso de uso na área de solução Gerenciamento de riscos de TI e segurança. As seções a seguir descrevem os casos de uso exigidos pela Cyber Incident & Breach Response como pré-requisito, para os quais você pode fazer upgrade quando seu programa amadurecer e que podem ser integrados em outras áreas de soluções para a obtenção de outros contextos e funcionalidades de negócios.

### Casos de uso de pré-requisito e seguintes

A tabela a seguir mostra como este caso de uso se encaixa na área de solução geral Gerenciamento de riscos de TI e segurança.

| Pré-requisitos | O que você tem | O que vem depois |
| --- | --- | --- |
| Gerenciamento de problemas | Cyber Incident & Breach Response | *N/D* |
| * Estabelecer sua hierarquia de negócios * Consolidar e coordenar resultados e planos de remediação a partir de avaliações de risco, conformidade e auditorias, entre outras * Gerenciar exceções com aprovação/aceitação adequada de riscos | * Gerenciar contatos e equipe do SOC * Gerencie incidentes, inclusive a geração de relatórios, o escalonamento e a correção, usando um processo de workflow avançado. * Gerencie os incidentes declarados usando um processo simplificado de workflow avançado. * Gerenciar operações de segurança * Gerenciar as violações de dados |  |

### Casos de uso relacionados em outras áreas de solução

A tabela a seguir mostra os recursos adicionais que estarão disponíveis se você tiver os casos de uso específicos licenciados.

Para obter informações sobre estes casos de uso do Archer, consulte a [Ajuda das soluções Archer.](https://help.archerirm.cloud/archer_suite_help/en-us/Content/PortalHome/SolutionsHome/sol_home.htm)

| Nome do caso de uso | Nome do aplicativo | Principal finalidade da relação |
| --- | --- | --- |
| Gerenciamento de crises | Evento de crise | Usando o Gerenciamento de crises do Archer, você pode criar um registro de evento de crise para que sua equipe de eventos de crise o monitore e resolva. |
| Qualquer caso de uso que contenha o aplicativo Riscos | Riscos | É possível vincular seu registro de incidente aos riscos relacionados no aplicativo Riscos. |

## Introdução

* [Saiba mais sobre a arquitetura de casos de uso](itsrm_cibr_design.htm)
* [Saiba como funciona o caso de uso](itsrm_cibr_using_the_uc.htm)
* [Instalar e configurar o caso de uso](itsrm_cibr_install.htm)
* [O que há de novo nesta versão](ReleaseNotes/itsrm_cibr_2024_03_RN.htm)