

A Cyber Crucible possui um processo de resposta a incidentes e notificação de violações?

Resposta curta: Sim. Um processo documentado de resposta a violações de dados define as funções e as etapas para responder a um suspeito de furto, violação ou exposição de dados protegidos, incluindo a notificação ao cliente. Um prazo de notificação comprometido pode ser estabelecido por contrato para clientes regulados.

O processo de resposta

Um suspeito de incidente é reportado imediatamente por meio de canais internos monitorados pela função de Segurança da Informação. Após a identificação, o acesso ao recurso afetado é removido e é convocada uma equipe de resposta a incidentes presidida pela alta administração. Investigadores forenses e especialistas, disponibilizados por meio do seguro cibernético e tecnológico da Cyber Crucible, determinam como o incidente ocorreu, os dados envolvidos, as partes afetadas e a causa raiz. Um plano de comunicação é desenvolvido em conjunto com os departamentos Jurídico, de Comunicações e de Recursos Humanos para notificar a equipe, o público e as partes afetadas conforme apropriado — incluindo a notificação ao cliente por meio de um canal mutuamente acordado — seguido de uma revisão pós-incidente.

Resposta de suporte e notificação

Os incidentes voltados ao cliente são acompanhados de acordo com os níveis de gravidade publicados no SLA (SEV1 a SEV4), e um prazo de notificação de violação ou incidente pode ser comprometido contratualmente para clientes regulados.

Alinhamento com frameworks e o limite honesto

O processo está alinhado ao NIST SP 800-61 e à ISO/IEC 27001:2022 A.5.24–A.5.26. Nenhuma certificação é reivindicada. O procedimento completo de resposta a incidentes e notificação de violações é fornecido aos avaliadores mediante acordo de confidencialidade (NDA).

Revision #1

Created 2026-07-24 23:37:16 UTC by Dennis Underwood

Updated 2026-07-24 23:37:16 UTC by Dennis Underwood