Tarefa – Linha do tempo para a restauração da operação

Momento	24h	48h	72h	120h

1. Identificação e isolamento imediato dos sistemas afetados para conter o vazamento de dados.
2. Notificação das equipes de segurança, jurídica e de relações públicas sobre o incidente.
3. Início das investigações preliminares para determinar a extensão e origem do ataque.

1. Implementação de centralização dos alertas de segurança em um ponto único (SIEM).
2. Correção e otimização das configurações de alerta para garantir respostas rápidas a novas ameaças.
3. Início do processo de atualização dos contatos dos responsáveis por cada sistema para garantir comunicação eficiente.

1. Continuação da análise forense para identificar e eliminar quaisquer backdoors ou malwares remanescentes.
2. Reforço das medidas de segurança em todos os sistemas, incluindo patching e atualizações necessárias.
3. Revisão e atualização da documentação dos sistemas para refletir as mudanças e melhorias implementadas.

1. Configuração de isolamento/desconexão automática (SOAR) para prevenir a propagação do incidente.
2. Comunicação aos clientes afetados informando sobre o vazamento e medidas de mitigação.
3. Atualização das configurações de alerta para detectar qualquer atividade suspeita relacionada ao vazamento.

1

1. Orientação aos clientes sobre práticas seguras de armazenamento de dados e medidas preventivas.
2. Oferecimento de serviços adicionais de Cyber Security para aumentar a proteção dos dados dos clientes.
3. Desenvolvimento e implementação de indicadores de perda financeira para monitorar e avaliar futuros incidentes.

2 semanas	4 semanas	1 mês	2 meses	3 meses

1. Estabelecimento de uma operação 24/7 para monitoramento contínuo e resposta a incidentes.
2. Finalização da atualização e centralização das documentações dos sistemas.
3. Treinamento adicional das equipes internas e externas para garantir a eficácia das novas medidas de segurança.

1. Realização de auditorias regulares para garantir que todas as medidas de segurança estão sendo seguidas.
2. Monitoramento contínuo dos sistemas para identificar e mitigar novas ameaças proativamente.
3. Avaliação e ajuste das medidas de segurança baseadas em feedback e resultados das auditorias.

1. Consolidação das lições aprendidas com o incidente e documentação das melhores práticas.
2. Fortalecimento das parcerias com empresas de segurança cibernética para apoio contínuo.
3. Planejamento e execução de exercícios de simulação de incidentes para testar a prontidão da equipe.

Etapa 5 → **Etapa 6** → **Etapa 7** → **Etapa 8** → **Etapa 9**

1. Revisão completa das políticas de segurança e conformidade para prevenir futuros vazamentos.
2. Testes rigorosos dos sistemas de segurança implementados para assegurar sua eficácia.
3. Implementação de uma campanha de conscientização de segurança entre os colaboradores e clientes.

2

1. Revisão e atualização das políticas de segurança corporativa com base nas lições aprendidas.
2. Expansão das capacidades de segurança com novas tecnologias e estratégias.
3. Continuidade na educação e treinamento de segurança para todos os colaboradores.