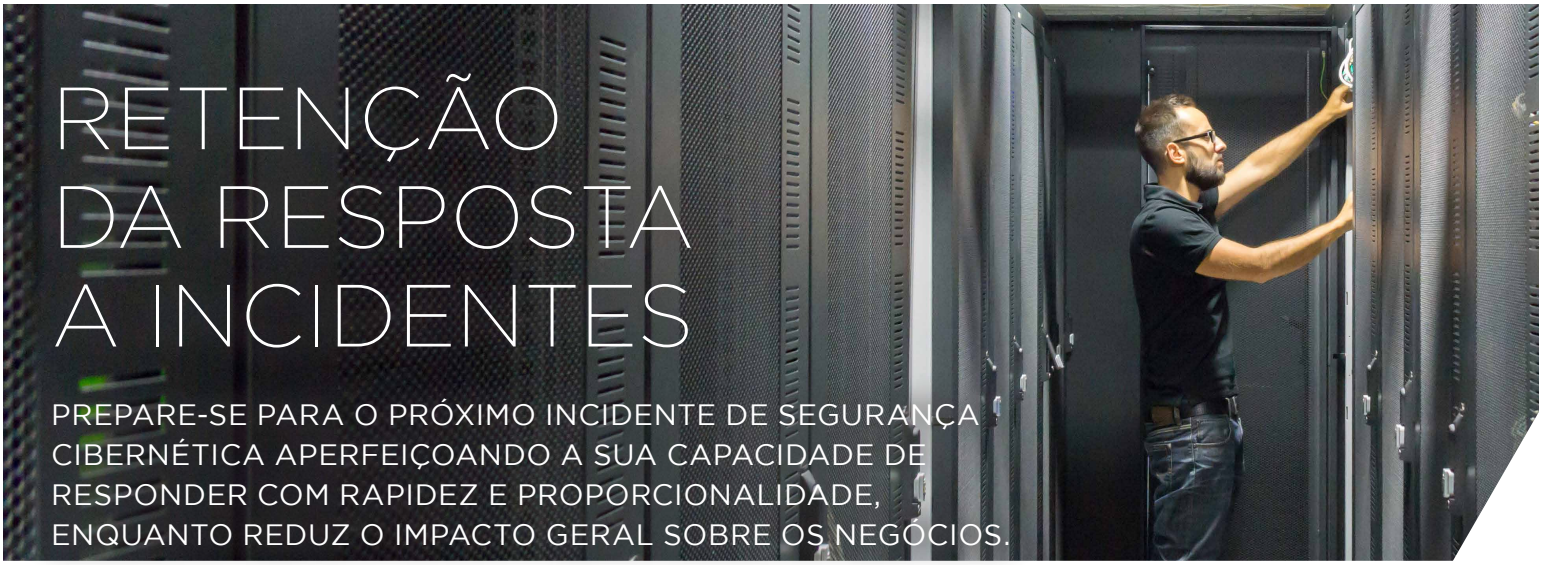

RETENÇÃO DA RESPOSTA A INCIDENTES

PREPARE-SE PARA O PRÓXIMO INCIDENTE DE SEGURANÇA CIBERNÉTICA APERFEIÇOANDO A SUA CAPACIDADE DE RESPONDER COM RAPIDEZ E PROPORCIONALIDADE, ENQUANTO REDUZ O IMPACTO GERAL SOBRE OS NEGÓCIOS.

VISÃO GERAL

Diferentemente de um crime físico como roubo, não existe instituição policial ou órgão governamental ao qual recorrer quando você descobre que foi vítima de um ataque cibernético. Nesse caso, as organizações precisam recorrer a empresas privadas de consultoria em segurança, especializadas em responder a ataques. No entanto, se você não tem um relacionamento estabelecido com um provedor de serviços, pode-se levar dias ou semanas para pesquisar empresas, obter as aprovações internas necessárias e finalizar um contrato. Isso toma um tempo precioso que os atacantes podem usar para percorrer a sua rede e roubar os seus dados antes que a investigação tenha início.

O que é uma retenção da resposta a incidentes?

Uma retenção da resposta a incidentes permite que uma empresa estabeleça os termos e condições para o fornecimento de serviços no caso de um incidente de segurança da informação suspeito ou confirmado. Com uma retenção implementada, a organização tem à disposição um parceiro confiável ao qual recorrer na eventualidade de uma violação de segurança. Essa abordagem proativa pode abreviar significativamente o tempo de resposta e reduzir o impacto de um incidente de segurança, incluindo o roubo de dados confidenciais.

Como avaliar empresas de resposta a incidentes?

Como em qualquer serviço, é difícil mensurar a qualidade até que se tenha a oportunidade de experimentar, em primeira mão, o serviço em questão. Se você ainda não teve um incidente, a melhor alternativa é perguntar a seus colegas a quem eles recorreram e como foi a experiência.

A maioria dos serviços de retenção oferece um tempo de resposta garantido. Além disso, você pode fazer algumas perguntas aos provedores de serviços para auferir suas capacidades e experiência, por exemplo:

- Vocês têm uma equipe de resposta a incidentes dedicada? Qual é a experiência dessa equipe?
- A quantos incidentes vocês responderam no ano passado? A que tipo de incidentes vocês responderam?
- Quais capacidades de análise de malware e recursos de inteligência vocês têm?
- Vocês têm experiência em trabalho conjunto com instituições policiais, caso isso seja necessário?
- Como vocês garantem que os atacantes foram realmente erradicados ao concluir uma investigação?
- Que tipo de níveis de serviço vocês oferecem quando há um incidente confirmado? Vocês podem oferecer suporte remoto imediato nas primeiras horas?

MANDIANT®
A FireEye® Company

DESTAQUES

- Saiba como as retenções podem reduzir o tempo de resposta a uma violação.
- Identifique perguntas fundamentais a fazer ao avaliar organizações.
- Determine como selecionar uma retenção que satisfaça suas necessidades em negócios.

FireEye®

Quais são os seus requisitos de segurança e de negócios?

Contratos de retenção podem ser elaborados de várias maneiras diferentes, conforme as suas necessidades. A maioria das pessoas desconhece que contratos de retenção da resposta a incidentes podem ser estabelecidos sem custo algum. Alguns provedores exigem que você compre um número pré-pago de horas para estabelecer um relacionamento, enquanto outros não exigem compromisso financeiro algum e se concentram em eliminar qualquer burocracia.

Veja a seguir alguns dos pontos mais importantes a serem considerados ao se decidir que tipo de retenção é apropriado para a sua organização:

- **Considerações orçamentárias:** o tipo mais comum de retenção estabelece uma taxa por hora, com um número determinado de horas pré-pagas. Durante uma investigação, você usa o bloco de horas pré-pago. Se mais horas forem necessárias, você paga a taxa por hora negociada previamente. Se você não quiser adquirir um bloco de horas, alguns provedores permitem que você assine um contrato estabelecendo termos e condições, incluindo uma taxa por hora, para que você possa pular o processo de contratação e compra no caso de uma violação de segurança.
- **Horas não utilizadas:** nem toda organização sofre uma violação grave. Se você escolher um contrato, uma consideração importante é o que acontece com quaisquer horas pré-pagas que não sejam utilizadas. Alguns contratos de retenção permitem que você use as horas em serviços proativos de resposta a incidentes, enquanto outros oferecem a flexibilidade de usar as suas horas em quaisquer serviços de segurança oferecidos pela empresa. Em alguns casos, as horas são perdidas quando o prazo do contrato se esgota.
- **Tempo de resposta:** a maioria dos contratos de retenção garante a presença de um consultor no local, no prazo de 24 a 48 horas. Algumas organizações são capazes de disponibilizar tecnologia antecipadamente para que possam iniciar a investigação imediatamente, mesmo antes que os consultores cheguem ao local.
- **Tempo de duração e condições de pagamento:** a maioria dos contratos de retenção cobre um período de 12 meses e requer pagamento adiantado.
- **Seguro cibernético:** o seguro cibernético está se tornando cada vez mais comum. A maioria dos provedores de seguros cibernéticos só reembolsa despesas com resposta a incidentes (RI) incorridas na resposta direta a um incidente. Muitos também oferecem prêmios menores para organizações que possam demonstrar uma forte abordagem proativa à segurança cibernética.

SOBRE OS SERVIÇOS DE RETENÇÃO DE RI DA MANDIANT

A Mandiant, uma empresa FireEye, oferece três níveis de retenção de resposta a incidentes.

O **nível 1** não exige compromisso financeiro. Ele estabelece os termos e condições básicos, incluindo a taxa por hora.

O **nível 2** corresponde a horas pré-pagas com um contrato de nível de serviço.

O **nível 3** é uma retenção com um contrato de nível de serviço agregado a serviços proativos pré-pagos. O nível 3 permite que os clientes se concentrem proativamente no fortalecimento de sua postura de segurança, com acesso à mais baixa taxa de resposta a incidentes por hora da Mandiant, caso ocorra um incidente. Isso é ideal para organizações que tenham ou estejam considerando adquirir um seguro cibernético.

COMPARAÇÃO DOS NÍVEIS DE RETENÇÃO DA RESPOSTA A INCIDENTES

RECURSO	NÍVEL 1	NÍVEL 2	NÍVEL 3
Termos e condições pré-negociados para serviços de RI	Sim	Sim	Sim
Hotline/e-mail para solicitação de serviços de RI 24 horas	Sim	Sim	Sim
Contrato de nível de serviço (SLA)	Melhor empenho	Sim	Sim
Horas de suporte da Mandiant descontadas	-	Pré-pagas + horas adicionais conforme a necessidade	Conforme a necessidade
Serviços proativos da Mandiant	-	Pode aplicar em serviços da Mandiant as horas de retenção não utilizadas	Aquisição agregada de serviços proativos a serem fornecidos durante o prazo da retenção
Serviço de prontidão para incidentes	-	Sim	Sim
Custo inicial	-	Com base na quantidade de horas de suporte selecionadas	Com base no serviço selecionado

Para obter mais informações sobre os serviços de consultoria da Mandiant, visite:
www.FireEye.com/services.html

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
+1 408.321.6300 / 877.FIREEYE (347.3393) / LATAM@FireEye.com

www.FireEye.com