

## FICHA TÉCNICA

# Retenção da resposta a incidentes

## Reduza o tempo de resposta a incidentes e minimize o impacto dos incidentes de segurança



### VANTAGENS

- Especialistas da Mandiant conhecidos no mundo todo ao seu dispor
- Acesso à tecnologia da Mandiant, líder no setor
- Termos e condições negociados previamente que reduzem o tempo de resposta quando isso é mais importante
- SLA de rápida resposta que minimizam o impacto de uma violação
- Acesso ao serviço de prontidão para resposta a incidentes da Mandiant
- Tempos de resposta garantidos em caso de suspeita de incidente
- Flexibilidade para adaptar horas não utilizadas em vários serviços estratégicos e técnicos

### Por que contar com a FireEye Mandiant?

A FireEye Mandiant está na linha de frente da inteligência em segurança cibernética e ameaças cibernéticas desde 2004. Os responsáveis pela resposta a incidentes estiveram nas linhas de frente das violações mais complexas do mundo. Temos um profundo conhecimento dos agentes de ameaça existentes e emergentes, bem como de suas ferramentas, táticas e procedimentos (Tools, Tactics and Procedures, TTPs), sempre em constante mudança.

### Visão geral

A retenção de resposta a incidentes (Incident Response Retainer, RRI) da FireEye Mandiant permite que as organizações estabeleçam termos e condições para serviços de resposta a incidentes antes da suspeita de um incidente de segurança cibernética. Com uma IRR implementada, você tem um parceiro confiável à disposição. Essa abordagem proativa pode diminuir significativamente o tempo de resposta e, conseqüentemente, reduzir o impacto de uma violação.

A IRR oferece a flexibilidade para estruturar a retenção de que sua empresa precisa.

- **Retenção sem custo:** estabelece termos e condições entre sua organização e a Mandiant para serviços de resposta a incidentes. O contrato define taxas por hora para serviços relacionados e tarifas de tecnologia. Não há custo anual nem compromisso financeiro algum. Somente haverá cobrança, dependendo dos materiais e tempo, caso seja declarado um incidente.
- **Horas pré-pagas:** compre um bloco pré-pago de horas de resposta a incidentes por uma taxa por hora com desconto, com a flexibilidade de adaptar as horas não utilizadas. As horas pré-pagas podem ser usadas em vários serviços de consultoria estratégica e técnica.<sup>1</sup>

Além dos termos e condições preestabelecidos, adicione um Contrato de nível de serviço (Service Level Agreement, SLA) e fique tranquilo com os tempos de resposta garantidos. O SLA padrão da Mandiant tem duração máxima de quatro horas, com um SLA aprimorado de duas horas para reduzir ainda mais o impacto de incidentes.

<sup>1</sup> As horas devem ser adaptadas dentro do termo do contrato.

**Tabela 1.** Benefícios das horas pré-pagas.

Resposta inicial	Contrato de nível de serviço	Serviço de prontidão para resposta a incidentes
<ul style="list-style-type: none"> <li>• Problema de segurança na triagem</li> <li>• Forneça a avaliação inicial com base na experiência da Mandiant e inteligência da FireEye</li> <li>• Análise de resposta dos sistemas em tempo real para identificar atividade maliciosa</li> </ul>	<ul style="list-style-type: none"> <li>• Acesso a uma linha direta permanente para resposta a incidentes</li> <li>• Contato inicial (por e-mail ou telefone) em até quatro horas: O primeiro contato é com um responsável pela resposta a incidentes da Mandiant, que pode ajudar imediatamente com a triagem do incidente</li> <li>• SLA aprimorado de duas horas disponível</li> <li>• Um responsável por primeira resposta da Mandiant é designado para o seu caso em até 24 horas<sup>2</sup></li> </ul>	<ul style="list-style-type: none"> <li>• Exame das tecnologias existentes de monitoramento, registro e detecção</li> <li>• Capacidade garantida de conter um incidente</li> <li>• Exame da atual arquitetura de host e rede</li> <li>• Avaliação das capacidades de primeira resposta</li> <li>• Planejamento colaborativo para cenários de resposta típicos</li> <li>• Recomendações para as áreas a serem aprimoradas</li> </ul>

**Tabela 2.** Os serviços de consultoria disponíveis para adaptar as horas pré-pagas incluem:

Serviços técnicos	Serviços estratégicos	Serviços de educação
<ul style="list-style-type: none"> <li>• Avaliação de comprometimento</li> <li>• Avaliações Red Team</li> <li>• Testes de penetração</li> </ul>	<ul style="list-style-type: none"> <li>• Avaliação de prontidão de resposta</li> <li>• Avaliação de programa estratégico</li> <li>• Exercício de simulação de resposta a incidentes</li> <li>• Desenvolvimento de centros de defesa cibernética</li> </ul>	<ul style="list-style-type: none"> <li>• Resposta a incidentes e análise forense</li> <li>• Análise de malware</li> <li>• Inteligência e segurança cibernética</li> </ul>

<sup>2</sup> Mediante aceitação da declaração.

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

**FireEye, Inc.**

601 McCarthy Blvd. Milpitas, CA 95035 EUA  
 408.321.6300/877.FIREEYE (347.3393)  
 info@FireEye.com

© 2019 FireEye, Inc. Todos os direitos reservados. FireEye é uma marca registrada da FireEye, Inc. Todos os outros nomes de marcas, produtos e serviços são ou podem ser marcas comerciais ou marcas de serviços de seus respectivos proprietários. M-EXT-DS-US-EN-000038-04

**Sobre a FireEye, Inc.**

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos.

