SecureTrust
a Trustwave division

Descrição do Serviço

Avaliação de Lacunas do Padrão de Segurança de Dados do Setor de Cartões de Pagamento

Copyright © 2021 SecureTrust, Inc. Todos os direitos reservados.

Sumário

Copyright © 2021 SecureTrust, Inc. Todos os direitos reservados.

Avaliação de Lacunas do PCI DSS

A SecureTrust™ é uma divisão da Trustwave Holdings, Inc.

DESCRIÇÃO DO SERVIÇO

A Avaliação de Lacunas do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS – Payment Card Industry Data Security Standard) da SecureTrust (o "Serviço") foi desenvolvida para identificar as lacunas e priorizar áreas que podem necessitar de correção para obter conformidade com o PCI DSS, conforme estabelecido pelo Conselho de Padrões de Segurança do PCI (o "Padrão").

Os termos em maiúsculas usados nesta descrição de serviço, mas não definidos aqui, têm seus significados indicados no Contrato Principal de Serviços da Trustwave, disponível em https://www.trustwave.com/en-us/legal-documents/contract-documents/ ou em um contrato similar assinado entre a SecureTrust e o Cliente.

RECURSOS DO SERVIÇO BÁSICO

O Serviço inclui os seguintes recursos padrão:

Portal SecureTrust

Os recursos do Portal SecureTrust consistem, entre outros, em um aplicativo de Gerenciamento de conformidade para administrar o processo de engajamento, bem como para coletar e armazenar com segurança evidências, documentação e produtos finais.

Serviços Globais de Conformidade e Risco

A equipe de Serviços Globais de Conformidade e Risco (GCRS — Global Compliance and Risk Services) é composta, entre outras, pelas seguintes pessoas e funções de destaque:

Avaliador de segurança qualificado (QSA – Qualified Security Assessor) – Um QSA é o principal recurso para a execução do Serviço, sendo responsável pela condução da avaliação, determinação de conformidade e relatórios.

Consultor gerencial (MC – Managing Consultant) – Um MC fornece orientação, supervisão de projeto e garantia de qualidade de relatórios ao QSA, além de servir como ponto de contato secundário do Cliente para escalamentos e consultas.

Conselho de Revisão de Conformidade (CRB – Compliance Review Board) – O CRB serve como ponto final para a interpretação dos requisitos do Padrão ou para a solução de questões complicadas de conformidade, fornecendo consistência e continuidade ao longo das avaliações da SecureTrust. O CRB também é o ponto final de escalamento para a solução de problemas relativos a status de conformidade contra os requisitos do Padrão ou a revisão de um controle de compensação.

Avaliação de lacunas – A avaliação identifica as lacunas e prioriza áreas que podem necessitar de correção para obtenção de conformidade com o Padrão. A SecureTrust fornecerá ao Cliente orientação para o design de controles de PCI DSS e para a identificação de políticas, procedimentos e práticas

Copyright © 2021 SecureTrust, Inc. Todos os direitos reservados.

organizacionais de apoio relevantes ao Padrão. A SecureTrust fornecerá ao Cliente um relatório final detalhando os resultados do Serviço.

ENTREGA E iMPLEMENTAÇÃO

Início do projeto

A equipe de GCRS da SecureTrust facilita a entrega do Serviço, o que inclui o agendamento e a condução da reunião de abertura remota para definir e chegar a um acordo sobre um plano de projeto de alto nível que consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos, requisitos de recursos e procedimentos de escalamento.

Fase I: Coleta de informações

A SecureTrust e o Cliente trabalharão juntos para coletar e analisar informações sobre os sistemas em escopo do Cliente.

A SecureTrust trabalhará com o Cliente, onde aplicável, para:

- Determinar ativos críticos;
- Examinar processos de negócios;
- Identificar processos de gerenciamento de segurança e conformidade vigentes.
- Revisar a documentação anterior de conformidade com PCI DSS.

Fase II: Avaliação de lacunas do PCI DSS

A SecureTrust conduzirá revisões de documentação, entrevistas, discussões, revisões de evidências, inspeções de instalações, análises de controles e exames da arquitetura de segurança atual do Cliente.

A SecureTrust trabalhará com o Cliente, onde aplicável, para:

- Avaliar a adequação do conhecimento do Cliente sobre o Padrão e as responsabilidades de todas as partes envolvidas em demonstrar a conformidade como PCI DSS.
- Compreender o ambiente a fim de identificar lacunas cruciais entre o estado atual do Cliente e o Padrão.
- Entender postura de conformidade com PCI DSS do Cliente;
- Identificar lacunas na obtenção de conformidade com o Padrão.
- Priorizar os esforços corretivos necessários para obtenção de conformidade com o Padrão.

A SecureTrust analisará evidências de acordo com o Padrão e determinará o status de conformidade dos sistemas em escopo do Cliente.

Fase III: Relatórios

A SecureTrust desenvolverá um relatório documentando as observações e recomendações a partir do Serviço.

Um esboço do relatório será enviado ao Cliente para revisão. O Cliente poderá comentar e sugerir alterações no esboço do relatório antes que a equipe de QA da SecureTrust finalize o relatório. A SecureTrust mantém a autoridade final em relação ao conteúdo do relatório e ao tipo de produto final a ser desenvolvido.

A SecureTrust fornecerá ao Cliente um relatório final como o produto final.

Copyright © 2021 SecureTrust, Inc. Todos os direitos reservados.

A SecureTrust conduzirá uma reunião de fechamento com o Cliente.

RESPONSABILIDADES DA SECURETRUST

- Estabelecer contato e permanecer disponível para comunicações com o Cliente.
- Estabelecer comunicação e planos de escalamento.
- Criar uma conta do Cliente no Portal SecureTrust.
- Definir o plano de projeto de alto nível, o qual consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos e requisitos de recursos.
- Agendar e conduzir reuniões de abertura, status periódico e fechamento.
- Validar o escopo do Serviço, incluindo segmentação, e discutir a metodologia de amostragem.
- Criar e responder a itens de ação do Cliente no Portal do Gerenciador de conformidade.
- Entrevistar o pessoal apropriado da organização e coletar informações dessas pessoas.
- Realizar uma avaliação de lacunas nos procedimentos de testes do Padrão.
- Determinar os resultados do Serviço e de acordo com o Padrão.
- Produzir um relatório de esboço no momento em que a avaliação ocorrer.
- Fornecer ao Cliente um relatório final, documentando todas as observações e recomendações a partir da avaliação.

RESPONSABILIDADES E ACEITES DO CLIENTE

- Estabelecer contato e permanecer disponível para comunicações com a SecureTrust.
- Estabelecer comunicação e planos de escalamento.
- Concordar com o plano de projeto de alto nível, o qual consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos e requisitos de recursos.
- Fornecer com precisão todas as informações necessárias, incluindo principais partes interessadas, informações aplicáveis sobre o ambiente do Cliente e requisitos de configuração.
- Informar à SecureTrust sobre todas as atividades de manutenção do ambiente do Cliente e sobre mudanças que podem impactar o fornecimento do Serviço.
- Responder com precisão às solicitações das equipes da SecureTrust ao estabelecer contato e na coleta das informações necessárias.
- Fornecer detalhes completos e precisos sobre o ambiente relevante e outras informações sobre as operações de negócios.
- Disponibilizar recursos capazes de participar das atividades do Serviço.
- Participar de e compreender os materiais explicados durante as chamadas, reuniões, entrevistas, discussões, inspeções de instalações e análises de controles.
- Aceites do cliente:
    - Todas as atualizações de segurança e recursos do Portal SecureTrust serão incluídos em atualizações de versões principais.
    - O Serviço não substituirá uma avaliação de conformidade de PCI DSS e não resultará em um relatório sobre a conformidade ou em um atestado de conformidade.
    - O Serviço pode consistir em atividades de avaliação remota e no local.
    - As datas de início e término do projeto serão determinadas durante a chamada de abertura.
    - A SecureTrust poderá solicitar evidências dos sistemas e processos do Cliente conforme necessário para comprovar a conformidade com quaisquer requisitos específicos. O Cliente concorda em fornecer todas essas evidências o mais breve possível.
    - A SecureTrust não é responsável por definir sistemas em escopo nem pela exatidão das informações fornecidas pelo Cliente.

Copyright © 2021 SecureTrust, Inc. Todos os direitos reservados.

- A SecureTrust reserva-se o direito de rejeitar ou aceitar comentários do Cliente baseados nos fatos e circunstâncias do Serviço.
- A SecureTrust desempenhará o Serviço no idioma inglês.
- A SecureTrust não criará ou modificará documentação do Cliente como parte do Serviço.
- A SecureTrust não fornecerá serviços corretivos como parte do Serviço.
- A SecureTrust não oferecerá nenhuma orientação ou aconselhamento legal.
- A qualidade e a precisão do Serviço dependem do fornecimento pelo Cliente de informações precisas e acesso aos sistemas e recursos do Cliente para a SecureTrust.

Copyright © 2021 SecureTrust, Inc. Todos os direitos reservados.