SecureTrust
a Trustwave division

Descrição do Serviço

Serviço de Validação de Conformidade de Padrão de Segurança de Dados do Setor de Cartões de Pagamento

Sumário

SERVIÇO DE VALIDAÇÃO DE CONFORMIDADE PCI DSS

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

DESCRIÇÃO DO SERVIÇO

O Serviço de Validação de Conformidade (CVS – Compliance Validation Service) do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS – Payment Card Industry Data Security Standard) da SecureTrust (o "**Serviço**") inclui serviços profissionais para validar se os componentes do sistema incluídos ou conectados aos ambiente de dados do titular do cartão (CDE – cardholder data environment) estão em conformidade com o PCI DSS conforme estabelecido pelo Conselho de Padrões de Segurança de PCI (o "Padrão"). O Serviço também inclui acesso ao Portal SecureTrust, com aplicativos para gerenciar o processo de engajamento e gerenciar as varreduras de vulnerabilidades externas do PCI.

Os termos em maiúsculas usados nesta descrição de serviço, mas não definidos aqui, têm seus significados indicados no Contrato Principal de Serviços da Trustwave localizado 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

O Portal SecureTrust consiste, entre outros, nos seguintes aplicativos e funções principais:

Gerenciador de conformidade – O aplicativo para gerenciar o processo de engajamento, bem como coletar e armazenar com segurança evidências, documentação e produtos finais.

Gerenciador de PCI – O aplicativo para gerenciar as varreduras ilimitadas de vulnerabilidades externas do PCI com um scanner certificado como fornecedor de varreduras aprovado (ASV – Approved Scanning Vendor) e gerar relatórios de varreduras do PCI ASV.

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 recurso principal para a execução do Serviço, sendo responsável pela condução da validação, 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 atua como ponto final para a interpretação dos requisitos do PCI DSS 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 PCI DSS ou a revisão de um controle de compensação.

PCI DSS CVS – O Serviço valida se os componentes identificados do sistema do Cliente incluídos ou conectados ao CDE estão em conformidade com o Padrão. Se os sistemas em escopo do Cliente forem considerados em conformidade com o Padrão, a SecureTrust fornecerá ao Cliente um Relatório de conformidade (ROC – Report on Compliance) e um Atestado de conformidade (AOC - Attestation of Compliance) completo como declaração do status de conformidade do Cliente. Se os sistemas em escopo do Cliente forem considerados fora de conformidade com o Padrão, a SecureTrust fornecerá um ROC de não conformidade.

Garantia de qualidade da SecureTrust (QA – Quality Assurance) – A equipe de QA da SecureTrust avalia as descobertas do ROC e dos controles antes do envio formal, conforme solicitado pelo Conselho de Padrões e Segurança do PCI. Quando a avaliação do ROC estiver concluída, a QA da SecureTrust finalizará o ROC e o AOC para entrega ao cliente e/ou às entidades de relatório relevantes.

Reuniões de revisão da rotina de negócios – As reuniões de revisão da rotina de negócios são usadas ao longo do ano para monitorar e revisar a eficácia dos processos de controle de segurança do Cliente na manutenção da conformidade de PCI DSS de forma contínua. A SecureTrust fornecerá reuniões trimestrais de revisão da rotina de negócios ao Cliente.

Pontuações de maturidade de segurança – As pontuações de maturidade de segurança identificam a classificação de maturidade da organização do Cliente e ajudam a priorizar áreas que podem exigir correção para atingir conformidade com o nível de maturidade desejado para a implementação dos controles de PCI DSS do Cliente.

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 para coletar e analisar informações sobre os sistemas em escopo do Cliente.

As principais atividades de coleta de informações incluem:

- Coleta de documentação de escopo;
    - A documentação de escopo pode incluir, entre outras, políticas e procedimentos, inventários de ativos, diagramas de fluxo de dados, diagramas de rede e outras documentações que definem os sistemas em escopo do Cliente.
- Concordância sobre os sistemas em escopo iniciais.

- Identificação dos itens de ação iniciais ou da evidência em falta.

A SecureTrust executará uma Verificação de preparação do PCI para determinar a capacidade do Cliente para concluir o Serviço. Se a Verificação de preparação do PCI determinar que o Cliente não está pronto para concluir o Serviço, ou não está em conformidade com o Padrão, mas uma declaração de conformidade oficial for necessária, a SecureTrust fornecerá ao Cliente uma ROC de não conformidade.

Fase II: Testes

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 coletará evidências por meio de itens de ação no aplicativo Gerenciador de conformidade no Portal SecureTrust.

A SecureTrust determinará se os sistemas em escopo do Cliente são qualificados para amostragem. Se os sistemas em escopo do Cliente forem qualificados para amostragem, e conjuntos de amostras identificarem itens fora de conformidade, um segundo conjunto de amostras será coletado. Se o segundo conjunto de amostras identificar itens fora de conformidade, os sistemas em escopo do Cliente serão identificados como fora de conformidade.

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 PCI DSS ROC documentando as observações e recomendações a partir do Serviço.

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

A SecureTrust fornecerá ao Cliente um produto de relatório final, conforme definido abaixo:

- Se os sistemas em escopo do Cliente forem considerados em conformidade com o Padrão e, uma vez finalizado pela equipe de QA da SecureTrust, o ROC, junto a todas as documentações de suporte, será enviado ao ponto de contato do Cliente ou às entidades de relatório relevantes.
- Se os sistemas em escopo do Cliente forem considerados fora de conformidade com o Padrão, a SecureTrust fornecerá um ROC de não conformidade ao Cliente.

A SecureTrust conduzirá uma reunião de fechamento com o Cliente.

Reuniões de revisão da rotina de negócios

A SecureTrust conduzirá Reuniões de revisão da rotina de negócios trimestralmente ao longo da vigência do Serviço.

A SecureTrust concluirá e fornecerá uma planilha de “Revisão da rotina de negócios” ao ponto de contato do Cliente para cada Reunião de revisão da rotina de negócios.

Pontuações de maturidade de segurança

A SecureTrust conduzirá pontuações de Maturidade de segurança como parte do Serviço.

A SecureTrust fornecerá ao Cliente pontuações de Maturidade de segurança para a implementação de controles de PCI DSS e categorias de controle de segurança do 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, consistindo em etapas principais, estimativas de duração, produtos e requisitos de recursos.
- Agendar e conduzir reuniões de abertura, status periódico e fechamento.
- Executar a verificação de preparação do PCI.
- Validar o escopo do Serviço, incluindo segmentação, e discutir a metodologia de amostragem.
- Criar e responder a itens de ação no Gerente de conformidade no Portal SecureTrust.
- Determinar a qualificação para amostragem do Cliente.
- Executar validação de acordo com os procedimentos de teste do Padrão.
- Identificar para o Cliente quaisquer observações que exijam correção.
- Determinar o status de conformidade dos sistemas em escopo do Cliente, de acordo com o Padrão.
- Produzir um ROC de PCI DSS de conformidade ou não conformidade, dependendo do status dos sistemas em escopo do Cliente quando ocorrer o Serviço.
- Fornecer ao Cliente um relatório final, documentando observações e recomendações a partir do Serviço.
- Conduzir Reuniões de revisão da rotina de negócios.
- Conduzir pontuações de Maturidade de segurança.

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.
- Concordar com as datas de início e término do Serviço.

- Enviar todas as evidências e as atividades completas de correção a não menos de cinco (5) dias antes do final do Serviço.
- Aceites do cliente:
    - Todas as atualizações de segurança e recursos do Portal SecureTrust serão incluídos em atualizações de versões principais.
    - O Serviço pode consistir em atividades de avaliação remota e no local.
    - As datas de início e término do Serviço 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, ou para estabelecer se as informações fornecidas pelo Cliente são precisas.
    - 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.