ManageEngine
Log360

Como o SIEM ajuda as empresas a cumprir o PCI DSS

www.manageengine.com/br/log-management/

Introdução

O Payment Card Industry (PCI) Security Standards Council foi fundado por cinco marcas globais de pagamento: American Express, Discover Financial Services, JCB International, MasterCard e Visa. Essas cinco marcas de pagamento tinham uma visão comum de fortalecer as políticas de segurança em todo o setor para evitar violações de dados para empresas que aceitam e processam cartões de pagamento. Juntas, elas elaboraram e lançaram a primeira versão do Padrão de Segurança de Dados PCI (PCI DSS 1.0) em 15 de dezembro de 2004. O PCI DSS 3.0 foi lançado em novembro de 2013 e a versão atual (PCI DSS 3.2.1) em maio de 2018.

O PCI DSS é um regulamento com doze requisitos que servem como linha de base de segurança para proteger os dados de cartões de pagamento. Essa norma enfatiza que a conformidade é um processo contínuo que envolve avaliações, reparos e relatórios, e que também precisa ser mantida entre as avaliações do PCI DSS. A obtenção da conformidade com o PCI DSS envolve a implementação de vários controles de segurança, incluindo a implantação de várias soluções específicas para este uso. Este guia detalha os requisitos 10 e 11.5 e como a solução SIEM da ManageEngine, o Log360, pode os atender.

Requisitos 10 e 11.5

O PCI DSS afirma que o objetivo dos requisitos 10 e 11.5 é monitorar e testar regularmente as redes. As descrições a seguir foram extraídas diretamente dele:

Requisito 10: rastreie e monitore todo o acesso aos recursos da rede e aos dados do titular do cartão

Os mecanismos de log e a capacidade de rastrear as atividades dos usuários são essenciais para prevenir, detectar ou minimizar o impacto de um comprometimento de dados. A presença de logs em todos os ambientes permite o rastreamento, o alerta e a análise completos quando algo dá errado. Determinar a causa de um comprometimento é muito difícil, se não impossível, sem os registros de atividade do sistema.

Requisito 11.5

Implante um mecanismo de detecção de mudanças (por exemplo, ferramentas de monitoramento de integridade de arquivos) para alertar a equipe sobre modificações não autorizadas (incluindo mudanças, adições e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo. Configure o software para realizar comparações de arquivos críticos pelo menos uma vez por semana. Implemente um processo para responder a todos os alertas gerados pela solução de detecção de mudanças.

A função do SIEM na conformidade do PCI DSS

Os Requisitos 10 e 11.5 tratam da implementação do monitoramento regular de redes e de mecanismos de detecção de mudanças, respectivamente. O motivo pelo qual o PCI DSS enfatiza muito esses dois aspectos é que os registros do sistema são a única maneira de investigar e responder a incidentes de segurança, como violações de dados.

Depois que a auditoria de segurança é ativada nos sistemas necessários, uma solução de gerenciamento de eventos e informações de segurança (SIEM) pode monitorar continuamente as redes, o que é essencial para atender aos requisitos do PCI DSS. Uma solução SIEM pode gerar os relatórios necessários para revisar periodicamente as informações de auditoria e também disparar alertas para atividades suspeitas que representem uma ameaça à segurança dos dados.

Recursos do Log360 que ajudam na conformidade do PCI DSS

O Log360 é uma solução SIEM abrangente que pode monitorar em tempo real os eventos de segurança que ocorrem em uma rede. Ele oferece recursos de monitoramento de segurança, incluindo relatórios incorporados e perfis de alerta necessários para os requisitos 10 e 11.5 do PCI DSS. Veja a seguir os recursos do produto que ajudam na conformidade com o PCI DSS:

Coleta centralizada de logs

As equipes de segurança devem primeiro identificar os diferentes sistemas em seu ambiente que armazenam ou processam os dados do titular do cartão e, em seguida, configurar o log neles. O log deve ser ativado para todos os sistemas e dispositivos de rede que se enquadram no escopo do PCI DSS. Isso permite que os profissionais de segurança de TI rastreiem os acessos e outras atividades nos recursos de rede que lidam com os dados do titular do cartão. Por exemplo, para rastrear os acessos a arquivos, a auditoria de acesso a objetos deve ser ativada nos servidores em questão. O Log360 pode então coletar registros de todos os diferentes sistemas que armazenam ou processam os dados do titular do cartão. A solução agrega dados de logs de servidores, bancos de dados, dispositivos de rede e outros sistemas para uma análise eficaz das informações de auditoria.

Revisão e geração de relatórios contínuos de logs

O Log360 transforma os dados brutos de logs coletados em informações acionáveis. As informações de auditoria são apresentadas em gráficos e painéis intuitivos. As equipes de segurança também podem programar relatórios para analisar os eventos de segurança diariamente. Os relatórios para os requisitos 10 e 11.5 estão disponíveis prontos para uso, o que significa que são gerados automaticamente assim que as fontes de log são adicionadas para monitoramento. Os relatórios listam as seções do PCI DSS de forma sistemática e são mapeados para suas subseções relevantes.

O sofisticado mecanismo de pesquisa de logs da solução permite que a equipe de segurança selecione e analise eventos de interesse durante a investigação de um incidente de segurança. O recurso de pesquisa do Log360 inclui funcionalidades básicas, como o uso de frases e operadores booleanos, bem como recursos avançados, como a correlação de vários eventos e atributos.

Retenção de logs

O PCI DSS exige que os dados de logs coletados sejam armazenados por pelo menos um ano. Os dados armazenados devem ser facilmente acessíveis, se necessário, para investigação forense. O Log360 pode ser configurado para os reter por qualquer período de retenção desejado. Se for necessário realizar uma investigação forense, eles podem ser facilmente recarregados no banco de dados e as operações de pesquisa podem ser realizadas neles.

Proteção de logs

Os agentes maliciosos geralmente tentam modificar os registros de auditoria para que suas atividades passem despercebidas. É por isso que o PCI DSS espera que os dados de registro sejam protegidos e invioláveis. O Log360 criptografa os arquivos de registro arquivados para garantir a segurança. Além disso, ele emprega técnicas como hashing e registro de data e hora para garantir que os logs arquivados não sejam adulterados.

Monitoramento da integridade do arquivo

O PCI DSS declara explicitamente que uma ferramenta de rastreamento de mudanças, como uma ferramenta de monitoramento de integridade de arquivos (FIM), deve ser implantada para alertar as equipes de segurança sobre modificações não autorizadas de arquivos críticos do sistema. Com os recursos de FIM do Log360, os profissionais de segurança podem rastrear centralmente as mudanças feitas em arquivos e pastas confidenciais, como arquivos e pastas criados, acessados, visualizados, excluídos, modificados e renomeados.

O Log360 fornece respostas para os quatro Qs vitais; as equipes de segurança saberão quem acessou um objeto, qual objeto foi acessado, quando a operação foi realizada e qual é o novo valor de um objeto. Isso garante que os acessos e as modificações feitas nos dados sejam autorizados e que a integridade dos dados do titular do cartão seja mantida.

Alertas em tempo real

O Log360 pode gerar alertas sobre a ocorrência de eventos críticos que podem comprometer a segurança dos sistemas que armazenam ou processam dados de cartões de pagamento. Os alertas pré-embalados do PCI DSS da solução podem ser ativados e os perfis de alerta podem ser personalizados com base em limites e outras condições. As equipes de segurança podem receber esses alertas por email ou SMS. Além disso, a solução permite que elas executem um script personalizado quando um alerta é acionado, a fim de automatizar a resposta às ameaças.

Monitoramento da atividade do usuário

O monitoramento da atividade do usuário é essencial para manter as ameaças internas sob controle. O Log360 monitora os usuários em tempo real e fornece uma trilha de auditoria completa de todas as atividades com seus relatórios. Ele também se concentra no rastreamento das ações dos usuários privilegiados, incluindo as mudanças críticas que eles fazem nos sistemas. A solução também vai além com seu módulo de análise do comportamento do usuário (UBA), que pode analisar o comportamento do usuário e identificar anomalias usando aprendizado de máquina não supervisionado e análise estatística. Isso permite que as equipes de segurança detectem instantaneamente atividades suspeitas de login e acesso a arquivos.

Requisitos do PCI DSS atendidos pelo Log360

A tabela abaixo fornece detalhes sobre os requisitos do PCI DSS que o Log360 pode atender.

Requisitos	Descrição dos requisitos	Como o Log360 ajuda
10.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema para reconstruir os seguintes eventos: (De 10.2.1 a 10.2.7)	Os componentes integrados do Log360 automatizam o processo de gerenciamento de logs e fornecem às equipes de segurança a trilha de auditoria completa necessária para obter visibilidade total da rede nas plataformas locais e na nuvem.
10.2.1	Todos os acessos de usuários individuais aos dados do titular do cartão.	O Log360 audita continuamente os acessos e as modificações feitas nos arquivos e bancos de dados que armazenam os dados do titular do cartão, bem como os arquivos de logs. A solução rastreia o acesso de cada usuário individual aos dados do titular. O relatório a seguir fornece os detalhes necessários: • Ação individual do usuário
10.2.2	Todas as ações realizadas por qualquer indivíduo com privilégios de root ou administrativos.	O Log360 monitora a atividade de usuários privilegiados e rastreia as várias ações executadas por eles em tempo real. Os relatórios de auditoria detalhados fornecem uma visão completa da atividade do administrador, e os alertas são acionados para atividades de login suspeitas e outras ameaças à segurança. O relatório a seguir fornece os detalhes necessários: • Ações administrativas do usuário

10.2.3	Acesso a todas as trilhas de auditoria.	O monitoramento da integridade dos arquivos pode ser ativado para os arquivos que armazenam dados de logs para rastrear os acessos às trilhas de auditoria. Os relatórios a seguir ajudam a rastrear as alterações de política: • Mudanças na política do usuário • Mudanças na política de domínio • Rastreamento da sessão do usuário • Mudanças na política de auditoria
10.2.4	Tentativas de acesso lógico inválidas.	O Log360 rastreia de forma abrangente a atividade de login nos sistemas, incluindo logins bem-sucedidos e tentativas fracassadas. O mecanismo de correlação de eventos pode detectar atividades de login suspeitas, inclusive ataques de força bruta. Os relatórios a seguir fornecem os detalhes de logon necessários: • Falhas de logon • Falhas de logon com base no usuário • Falhas de logon com base no DC
10.2.5	Uso e mudanças nos mecanismos de identificação e autenticação - incluindo, entre outros, a criação de novas contas e a elevação de privilégios - e todas as mudanças, adições ou exclusões de contas com privilégios de raiz ou administrativos.	O Log360 pode rastrear mudanças críticas, como a elevação de privilégios. Podem ser gerados relatórios sobre criações, exclusões e alterações de contas de usuários. O Log360 monitora as mudanças de associação de grupos de segurança no Active Directory em tempo real e dispara alertas quando os usuários são adicionados a grupos com privilégios elevados, como o grupo Administradores do Domínio. Relatórios de servidores individuais para outros servidores também estão disponíveis prontos para uso. Os relatórios a seguir fornecem os detalhes das mudanças necessárias: • Usuários criados recentemente • Usuários excluídos recentemente • Usuários modificados recentemente • Grupos criados recentemente • Grupos excluídos recentemente • Grupos de administradores modificados

10.2.6	Inicialização, interrupção ou pausa dos registros de auditoria.	O Log360 gera alertas se alguém desativar o registro ou limpar os registros de auditoria. Os relatórios a seguir fornecem as informações de registro necessárias: • Registros do sistema • Limpeza dos registros de auditoria
10.2.7	Criação e exclusão de objetos em nível de sistema.	O Log360 monitora objetos no nível do sistema, como executáveis de aplicações, arquivos de configuração, arquivos de configuração do sistema e executáveis do sistema com os seguintes relatórios prontos para uso: • Objeto acessado • Objeto criado • Objeto excluído • Objeto manipulado
10.3	Registre pelo menos as seguintes entradas de trilha de auditoria para todos os componentes do sistema em cada evento (de 10.3.1 a 10.3.6).	O Log360 registra todas as entradas críticas da trilha de auditoria de servidores, bancos de dados, arquivos/pastas, dispositivos de rede e muito mais.
10.3.1	Identificação do usuário	O Log360 ajuda a verificar a identificação do usuário incluída nas entradas de registro com seus relatórios detalhados de logon/logoff. As categorias de relatório a seguir fornecem os detalhes necessários da identificação do usuário: • Logon do usuário • Logon-logoff local • Auditoria do ADFS
10.3.2	Tipo de evento	O Log360 categoriza o tipo de evento na entrada de registro com base em sua gravidade, como erro, aviso, informação e outros. Os relatórios a seguir fornecem os detalhes necessários do evento: • Eventos de falha • Eventos de sucesso • Eventos de aviso • Eventos de informação • Eventos de erro • Visão geral dos eventos críticos

10.3.3	Data e horário	O Log360 analisa os dados delogs de data e horário nas entradas de logs para garantir relatórios e alertas precisos.
10.3.4	Indicação de sucesso ou falha	O Log360 analisa as informações de sucesso ou falha de um evento e relata os detalhes nos relatórios a seguir: • Eventos de sucesso • Eventos de falha
10.3.5	Origem do evento	O Log360 ajuda a verificar a origem de um evento analisando informações relevantes - como host, IP ou aplicação - das entradas de logs.
10.3.6	Identidade ou nome dos dados, componente do sistema ou recurso afetado.	A correlação avançada, a análise do comportamento do usuário e o mecanismo de alerta do Log360 ajudam as equipes de segurança a identificar instantaneamente os dados e sistemas afetados
10.5	Proteja as trilhas de auditoria para que não possam ser alteradas.	O Log360 protege as trilhas de auditoria contra modificações não autorizadas, arquivando, criptografando e marcando o tempo imediatamente dos registros coletados.
10.5.1	Limite a visualização das trilhas de auditoria àqueles que têm necessidade relacionada ao trabalho.	As configurações de acesso baseadas em funções do Log360 podem restringir a visualização de trilhas de auditoria àqueles que estão autorizados. As funções de administrador, convidado ou operador podem ser atribuídas aos técnicos.
10.5.2	Proteja os arquivos da trilha de auditoria contra modificações não autorizadas.	O monitoramento da integridade dos arquivos pode ser configurado para os arquivos de trilha de auditoria do Log360, que enviará alertas quando alguém tentar fazer modificações não autorizadas.
10.5.3	Faça imediatamente o backup dos arquivos da trilha de auditoria em um servidor de log centralizado ou em uma mídia que seja difícil de alterar.	O Log360 arquiva com segurança os dados de logs coletados em um local especificado. Os dados arquivados são protegidos ainda mais por mecanismos de hash e de registro de data e hora.

10.5.4	Grave logs de tecnologias voltadas para o exterior em um servidor de logs interno seguro e centralizado ou em um dispositivo de mídia..	O Log360 armazena dados de registro gerados por tecnologias voltadas para o exterior, como firewalls, DNS e servidores de e-mail, em um servidor interno seguro.
10.5.5	Use um software de monitoramento da integridade do arquivo ou de detecção de mudanças nos logs para garantir que os dados existentes não possam ser alterados sem gerar alertas (embora novos dados adicionados não devam causar um alerta).	O Log360 pode implementar o monitoramento da integridade do arquivo nos arquivos que armazenam dados de logs e gerar alertas quando os dados são acessados, excluídos ou modificados.
10.6	Analise os logs e os eventos de segurança de todos os componentes do sistema para identificar anomalias ou atividades suspeitas.	O Log360 pode ajudar as equipes de segurança a realizar análises diárias de registros para identificar atividades suspeitas e mitigar violações em um estágio inicial.
10.6.1	Revise os itens a seguir pelo menos diariamente: • Todos os eventos de segurança. • Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD. • Registros de todos os componentes críticos do sistema. • Registros de todos os servidores e componentes do sistema que executam funções de segurança (por exemplo, firewalls, sistemas de detecção de intrusão, sistemas de prevenção de intrusão (IDS/IPS), servidores de autenticação, servidores de redirecionamento de comércio eletrônico, etc.).	Os relatórios prontos para uso e personalizados, as regras de correlação, os perfis de alerta e o mecanismo de pesquisa de logs do Log360 permitem que as equipes de segurança analisem com eficiência os eventos de segurança necessários diariamente. Além disso, os relatórios de tendências fornecem insights profundos sobre as tendências de eventos históricos e sinalizam comportamentos anômalos.
10.6.2	Revise periodicamente os logs de todos os outros componentes do sistema com base nas políticas da organização e na estratégia de gerenciamento de riscos, conforme determinado pela avaliação anual de riscos da organização.	Além da ampla gama de dispositivos que o Log360 suporta prontos para uso, o analisador de logs personalizado e o recurso universal de análise e indexação de logs estendem seus recursos de auditoria a qualquer componente do sistema que gere logs em um formato legível por humanos.

10.6.3	Acompanhar as exceções e anomalias identificadas durante o processo de revisão.	O console de gerenciamento de incidentes integrado do Log360 cria um processo responsável para a resolução dos alertas acionados. Os alertas podem ser gerados automaticamente como tickets para o administrador designado, seja no produto ou por meio da integração com uma ferramenta de emissão de tickets.
10.7	Mantenha o histórico da trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponíveis para análise (por exemplo, on-line, arquivado ou restaurável a partir de backup).	O Log360 pode reter os logs por qualquer período personalizado. Os dados arquivados podem ser rapidamente recarregados no mecanismo de pesquisa para análise a qualquer momento.
11.5	Implantar um mecanismo de detecção de mudanças (por exemplo, ferramentas de monitoramento de integridade de arquivos) para alertar a equipe sobre modificações não autorizadas (incluindo mudanças, adições e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; e configure o software para realizar comparações de arquivos críticos pelo menos uma vez por semana..	O recurso de monitoramento de integridade de arquivos do Log360 audita os acessos e as modificações feitas em arquivos críticos em uma rede. Os relatórios semanais de monitoramento da integridade do arquivo podem ser programados e os alertas podem ser configurados para notificar a equipe de segurança sobre modificações não autorizadas. Os relatórios a seguir fornecem informações sobre eventos de arquivos e pastas:: • Todas as mudanças de arquivos ou pastas • Arquivo/pasta excluído • Arquivo/pasta renomeado • Arquivo/pasta movido • Arquivo/pasta modificado • Arquivo/pasta criado • Acesso de leitura do arquivo

Conclusão

A crescente sofisticação dos ataques cibernéticos e o número cada vez maior de violações de cartões de crédito tornaram a conformidade com o PCI DSS mais importante do que nunca. A importância de estar em conformidade com o PCI DSS foi destacada no relatório de conformidade com o PCI de 2015 da Verizon, que afirmou que, entre as empresas violadas que sua equipe forense investigou nos dez anos anteriores, nenhuma delas estava em conformidade no momento da violação.

A conformidade com o PCI DSS não deve ser vista como um exercício separado de segurança da informação. Em vez disso, ela deve estar entrelaçada com a estratégia geral de segurança de TI da organização. É importante que as organizações avaliem sua postura de segurança atual e tomem medidas para preencher as lacunas de segurança, o que normalmente envolve a implementação de políticas de segurança e a implantação de várias soluções.

Uma solução SIEM, como o Log360, pode desempenhar um papel fundamental em sua jornada rumo à conformidade contínua com o PCI DSS. Faça o download de uma avaliação gratuita e totalmente funcional de 30 dias do Log360 e comece a manter a conformidade hoje mesmo.

Sobre o autor

Siddharth Sharath Kumar é especialista em segurança e conformidade de TI na equipe de marketing de produtos da ManageEngine. Ele escreve artigos e e-books, organiza regularmente webinars sobre os principais tópicos de segurança de TI e faz apresentações nas conferências da ManageEngine e em outros eventos do setor em todo o mundo.