Jak Safetica pomaga spełnić wymogi PCI-DSS

Payment Card Industry Data Security Standard (PCI-DSS) jest standardem opracowanym w celu ochrony poufnych danych związanych z kartami płatniczymi i tworzonych przy użyciu takich kart.

Sam standard zawiera dwanaście wymogów, które opisywane są przez konkretne wyznaczniki. Aby osiągnąć pełną zgodność z PCI-DSS, firma musi spełnić wszystkie wymagania określone w tych wyznacznikach.

Safetica z łatwością pomoże spełnić następujące wymogi:

Wymogi PCI-DSS	Jak pomaga Safetica
3. Ochrona przechowywanych danych właścicieli kart	
3.2.3 Nie należy przechowywać osobistego numeru identyfikacyjnego (PIN) ani zaszyfrowanego bloku PIN po autoryzacji.	Safetica DLP > Kategorie danych, Reguły DLP
3.4 Należy uniemożliwić odczytanie numeru PAN w każdym miejscu jego przechowywania (w tym na przenośnych nośnikach cyfrowych, nośnikach zapasowych i w logach).	Safetica > Dyski BitLocker
4. Szyfrowanie transmisji danych posiadaczy kart przez otwarte, publiczne sieci	
4.1 Wykorzystanie zaawansowanej kryptografii i protokołów bezpieczeństwa w celu ochrony poufnych danych posiadaczy kart podczas transmisji przez otwarte sieci publiczne z uwzględnieniem następujących zasad: - Akceptowane są tylko zaufane klucze i certyfikaty. - Używany protokół obsługuje tylko bezpieczne wersje lub konfiguracje. - Poziom szyfrowania jest odpowiedni do stosowanej metodologii szyfrowania.	Safetica DLP > Strefy, Kontrola urządzeń, Reguły DLP
4.2 Nigdy nie należy wysyłać niezabezpieczonych numerów PAN za pomocą technologii komunikacyjnych użytkownika końcowego (np. e-mail, komunikator, SMS, czat itp.).	Safetica DLP > Reguły DLP, Kategorie danych
7. Ograniczenie dostępu do danych posiadacza karty zgodnie z zasadą ograniczonego dostępu.	
7.1 Należy ograniczyć dostęp do składników systemu i danych posiadaczy kart tylko do tych osób, których praca wymaga takiego dostępu.	Safetica DLP > Reguły DLP, Szyfrowanie dysków
7.2 Należy ustanowić system(y) kontroli dostępu do komponentów systemu, który ogranicza dostęp według zasady ograniczonego dostępu i jest ustawiony na odmowę dostępu dla wszystkich, chyba że udzielono wyraźnego pozwolenia.	WebSafetica> Kontrola aplikacji, Kontrola stron internetowych Safetica DLP > Reguły DLP, Kontrola urządzeń, Strefy
7.3 Należy zapewnić, że zasady bezpieczeństwa i procedury operacyjne dotyczące ograniczania dostępu do danych posiadaczy kart są udokumentowane, stosowane i znane wszystkim zainteresowanym stronom.	Safetica DLP > Reguły DLP

9. Ograniczenie fizycznego dostępu do danych posiadaczy kart	
9.7 Należy zachować ścisłą kontrolę nad przechowywaniem i dostępnością nośników.	Safetica DLP > Kontrola urządzeń
10. Śledzenie i monitorowanie całego dostępu do zasobów sieciowych i danych posiadaczy kart	
10.1 Należy wprowadzić dzienniki inspekcji w celu powiązania wszystkich przypadków dostępu do elementów systemu z poszczególnymi użytkownikami.	Ustawienia i logi Safetica
10.2.1 Wszystkie przypadki uzyskania przez użytkowników dostępu do danych posiadacza karty	Safetica Discovery > Pliki Safetica DLP > Reguły DLP
10.2.2 Wszystkie działania podejmowane przez dowolną osobę z uprawnieniami administratora lub roota	
10.2.7 Tworzenie i usuwanie obiektów na poziomie systemu	
10.3 Dla każdego zdarzenia należy zarejestrować co najmniej następujące wpisy dziennika inspekcji dla wszystkich elementów systemu.	Logi Safetica
10.5 Zabezpieczenie dzienników inspekcji w taki sposób, aby nie można było ich zmienić.	Ustawienia > Zarządzanie dostępem
10.6 Przeglądanie logów i zdarzeń związanych z bezpieczeństwem wszystkich komponentów systemu w celu identyfikacji anomalii lub podejrzanej aktywności.	Logi, Alerty, Raporty Safetica
10.7 Przechowywanie historii dziennika inspekcji przez co najmniej jeden rok, przy czym przez co najmniej trzy miesiące musi być on bezpośrednio dostępny do analizy (np. online, zarchiwizowany lub odtworzony z kopii zapasowej).	Ustawienia > Zarządzanie bazą danych
11. Regularne testowanie systemów i procesów bezpieczeństwa.	
11.5 Wdrożenie mechanizmu wykrywania zmian (np. narzędzia do monitorowania integralności plików) w celu ostrzegania personelu o nieuprawnionych modyfikacjach (w tym zmianach, dodawaniu i usuwaniu) krytycznych plików systemowych, plików konfiguracyjnych lub plików zawartości; oraz skonfigurowanie oprogramowania do porównywania krytycznych plików co najmniej raz w tygodniu.	Safetica Discovery > Pliki
12. Posiadanie zasad bezpieczeństwa informacji odnoszących się do całego personelu.	
12.3 Opracowanie zasad użytkowania krytycznych technologii i określenie właściwego sposobu korzystania z nich.	Szeroka gama narzędzi Safetica. Najważniejsze: Safetica Discovery > Pliki, Strony internetowe, E-maile, Aplikacje, Drukowanie
12.3.1 Wyraźne zatwierdzenie przez upoważnione strony	
12.3.2 Uwierzytelnianie na potrzeby korzystania z technologii	
12.3.3 Wykaz wszystkich odpowiednich urządzeń i personelu mającego do nich dostęp	
12.3.5 Dopuszczalne sposoby korzystania z technologii	
12.3.7 Wykaz produktów zatwierdzonych przez firmę	WebSafetica > Kontrola aplikacji, Kontrola stron internetowych, Kontrola drukowania Safetica DLP > Szyfrowanie dysków, Kontrola urządzeń, Reguły DLP
12.6 Wdrożenie oficjalnego programu podnoszenia świadomości bezpieczeństwa w celu zapoznania całego personelu z zasadami i procedurami bezpieczeństwa danych posiadaczy kart.	Safetica > Powiadomienie

17-1018