

CASE STUDY: Reflectiz convalida le capacità della propria piattaforma PCI DSS con Integrity360

Il cliente

Reflectiz offre una piattaforma agentless per la gestione dell'esposizione web che aiuta le organizzazioni a identificare e gestire script, componenti di terze parti e catene di fornitura digitali presenti sui loro siti web.

La sua piattaforma dedicata PCI DSS supporta le organizzazioni e-commerce nel monitoraggio, nell'autorizzazione e nella raccolta delle evidenze richieste dai requisiti PCI DSS v4.0.1 6.4.3 e 11.6.1.

La piattaforma monitora da remoto le pagine di pagamento senza richiedere modifiche al codice, installazione di software o l'inserimento di tag di monitoraggio.

Criteri di selezione

Reflectiz necessitava di un valutatore in grado di:

- Fornire competenze specialistiche PCI DSS
- Valutare le capacità tecniche e procedurali della piattaforma
- Verificare l'allineamento ai requisiti 6.4.3 e 11.6.1
- Esaminare i processi di monitoraggio, approvazione e reporting
- Fornire una valutazione indipendente e credibile
- Comprendere le aspettative relative alle evidenze richieste durante una valutazione QSA

Integrity360 Europe è una PCI Qualified Security Assessor Company e membro della Global Executive Assessor Roundtable del PCI Security Standards Council.

reflectiz



Settore

Conformità nei pagamenti



Sfida

Reflectiz desiderava una valutazione indipendente dell'allineamento della propria piattaforma PCI DSS ai requisiti PCI DSS v4.0.1 6.4.3 e 11.6.1.

La valutazione doveva verificare se la piattaforma fosse in grado di supportare efficacemente:

- Inventario e autorizzazione degli script nelle pagine di pagamento
- Verifica dell'integrità degli script
- Giustificazioni aziendali e tecniche documentate
- Rilevamento di manomissioni delle pagine di pagamento e degli header HTTP
- Monitoraggio e avvisi continui
- Raccolta delle evidenze per gli assessment PCI DSS

L'incarico consisteva in una revisione delle capacità della piattaforma e non in una certificazione o valutazione di conformità relativa a uno specifico ambiente cliente.

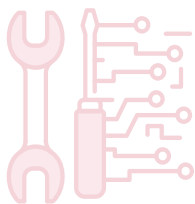
Soluzione

Integrity360 ha esaminato l'architettura, le capacità di monitoraggio e i processi di compliance della piattaforma PCI DSS di Reflectiz.

La valutazione ha analizzato come Reflectiz:

- Identifica gli script di prima, terza e quarta parte
- Monitora il comportamento degli script all'interno del browser
- Rileva modifiche alle pagine di pagamento e agli header HTTP
- Mantiene inventari degli script e giustificazioni documentate
- Registra le approvazioni tramite audit trail con marcatura temporale
- Genera avvisi ed evidenze pronte per le valutazioni

Integrity360 ha inoltre valutato il modello di implementazione agentless della piattaforma, la frequenza di monitoraggio configurabile, le funzionalità Smart Approval e le integrazioni con piattaforme di sicurezza e workflow.



Valutazione di Integrity360

Integrity360 ha rilevato che la piattaforma PCI DSS di Reflectiz è ben posizionata per aiutare le organizzazioni a soddisfare i requisiti PCI DSS v4.0.1 6.4.3 e 11.6.1.

L'inventario automatico degli script, l'analisi comportamentale dell'integrità, il workflow strutturato di approvazione, il monitoraggio continuo degli header HTTP e le funzionalità di reporting e audit supportano direttamente gli obiettivi di controllo pertinenti. Inoltre, l'architettura agentless consente alle organizzazioni di rafforzare il monitoraggio delle pagine di pagamento senza modifiche significative al codice né un elevato impatto operativo.



I team che si occupano di compliance hanno tutte le ragioni per essere prudenti nei confronti delle dichiarazioni dei fornitori. Il fatto che Integrity360 Europe, una Qualified Security Assessor Company indipendente, abbia esaminato come la nostra piattaforma si allinea ai requisiti PCI DSS 6.4.3 e 11.6.1 trasforma le nostre affermazioni in qualcosa che un merchant può valutare sulla base di elementi concreti. È proprio questa indipendenza a rendere la valutazione così preziosa”

Idan Cohen
Co-Fondatore e CEO di Reflectiz



Benefici

- Convalida indipendente da parte di una PCI Qualified Security Assessor Company
- Chiaro allineamento con gli obiettivi chiave di controllo PCI DSS
- Maggiore fiducia per clienti e valutatori
- Supporto comprovato per l'inventario e l'autorizzazione degli script
- Monitoraggio basato sul comportamento oltre i tradizionali hash statici dei file
- Monitoraggio continuo delle pagine di pagamento e degli header HTTP
- Riduzione del lavoro di preparazione delle evidenze per gli assessment QSA
- Riconoscimento di un valore più ampio in termini di sicurezza della supply chain

Se correttamente configurata e integrata in un più ampio programma di governance, rischio e compliance, Reflectiz può rappresentare un'alternativa più efficiente e sostenibile rispetto alle revisioni manuali degli script e agli approcci di monitoraggio statico.

Prospettive future

La valutazione indipendente fornisce a Reflectiz una base solida per dimostrare come la propria piattaforma possa supportare le organizzazioni nel soddisfare i requisiti PCI DSS relativi alla sicurezza delle pagine di pagamento.

La piattaforma può inoltre offrire un valore aggiunto più ampio migliorando la visibilità sulle catene di fornitura digitali, identificando minacce lato client e supportando programmi più estesi di governance, privacy e conformità normativa.

Per i merchant SAQ A idonei, una corretta implementazione può contribuire a dimostrare che le pagine di pagamento non sono vulnerabili ad attacchi basati su script. L'idoneità e i risultati di conformità dipendono comunque dall'ambiente e dai controlli specifici di ciascun merchant.



Informazioni su Integrity360

Integrity360 è uno dei principali specialisti indipendenti in cybersecurity e PCI operanti nell'area EMEA e in Nord America, con uffici nel Regno Unito e in Irlanda, Bulgaria, Italia, Svezia, Spagna, Germania, Svizzera, Francia, Belgio, Lituania, Ucraina, Africa, Caraibi e Canada. L'azienda gestisce Security Operations Center (SOC) a Dublino, Madrid, Sofia, Stoccolma, Roma e Città del Capo, garantendo monitoraggio e risposta continui attraverso molteplici fusi orari.

Con oltre 700 dipendenti, tra cui più di 580 professionisti dedicati alla cybersecurity, Integrity360 offre una gamma completa di servizi professionali, di supporto e di sicurezza gestita che coprono l'intero ciclo di vita del rischio cyber, dall'identificazione e dalla prevenzione fino al rilevamento, alla risposta e al ripristino.



Gartner

Integrity360 è citata in sei guide di mercato di Gartner relative ai fornitori di servizi di sicurezza gestiti, ai servizi SIEM gestiti, ai servizi di rilevamento e risposta gestiti, ai servizi di sicurezza in co-gestione, alla risposta agli incidenti e all'analisi forense.

3000+

Clienti
aziendali

585+

Professionisti
del settore
informatico