

CASE STUDY: Reflectiz bestätigt die PCI-DSS-Fähigkeiten seiner Plattform durch Integrity360

Der Kunde

Reflectiz bietet eine agentenlose Plattform für Web Exposure Management, die Unternehmen dabei unterstützt, Skripte, Drittanbieter-Komponenten und digitale Lieferketten auf ihren Websites zu identifizieren und zu verwalten.

Die dedizierte PCI-DSS-Plattform unterstützt E-Commerce-Unternehmen bei den Anforderungen in Bezug auf Überwachung, Autorisierung und Nachweisführung gemäß PCI DSS v4.0.1 Anforderungen 6.4.3 und 11.6.1.

Die Plattform überwacht Zahlungsseiten aus der Ferne, ohne Codeänderungen, Softwareinstallationen oder eingebettete Monitoring-Tags zu erfordern.

Selection Criteria

Reflectiz benötigte einen Prüfer, der:

- Spezialisierte PCI-DSS-Expertise bereitstellen kann
- Technische und organisatorische Plattformfähigkeiten bewertet
- Die Übereinstimmung mit den Anforderungen 6.4.3 und 11.6.1 beurteilt
- Monitoring-, Freigabe- und Reporting-Prozesse überprüft
- Eine unabhängige und glaubwürdige Bewertung liefert
- Die Nachweisanforderungen eines QSA-Assessments versteht

Integrity360 Europe ist ein PCI Qualified Security Assessor und Mitglied des PCI Security Standards Council Global Executive Assessor Roundtable.

reflectiz



Branche

Zahlungs-Compliance



Herausforderung

Reflectiz benötigte eine unabhängige Bewertung, wie gut seine PCI-DSS-Plattform mit den Anforderungen 6.4.3 und 11.6.1 von PCI DSS v4.0.1 übereinstimmt.

Die Bewertung sollte feststellen, ob die Plattform effektiv Folgendes unterstützen kann:

- Inventarisierung und Autorisierung von Skripten auf Zahlungsseiten
- Sicherstellung der Skriptintegrität
- Schriftlich dokumentierte geschäftliche und technische Begründungen
- Erkennung von Manipulationen an Zahlungsseiten und HTTP-Headern
- Kontinuierliche Überwachung und Alarmierung
- Sammlung von Nachweisen für PCI-DSS-Assessments

Die Beauftragung umfasste eine Überprüfung der Plattformfunktionen und keine Zertifizierung oder Compliance-Bewertung einer bestimmten Kundenumgebung.

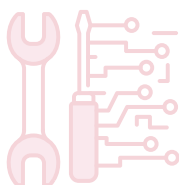
Lösung

Integrity360 überprüfte die Architektur, Überwachungsfunktionen und Compliance-Workflows der PCI-DSS-Plattform von Reflectiz.

Dabei wurde untersucht, wie Reflectiz:

- First-, Third- und Fourth-Party-Skripte identifiziert
- Das Verhalten von Skripten im Browser überwacht
- Änderungen an Zahlungsseiten und HTTP-Headern erkennt
- Skriptinventare und schriftliche Begründungen verwaltet
- Freigaben über zeitgestempelte Audit-Trails dokumentiert
- Warnmeldungen und prüfungsreife Nachweise erstellt

Integrity360 bewertete außerdem das agentenlose Bereitstellungsmodell, die konfigurierbare Monitoring-Frequenz, Smart-Approval-Funktionen sowie Integrationen mit Sicherheits- und Workflow-Plattformen.



Bewertung von Integrity360

Integrity360 kam zu dem Ergebnis, dass die Reflectiz PCI DSS Plattform sehr gut positioniert ist, um Unternehmen bei der Umsetzung der Anforderungen 6.4.3 und 11.6.1 von PCI DSS v4.0.1 zu unterstützen.

Die automatisierte Skriptinventarisierung, die verhaltensbasierte Integritätsanalyse, strukturierte Freigabeprozesse, die kontinuierliche Überwachung von HTTP-Headern sowie Audit- und Reporting-Funktionen unterstützen direkt die relevanten Kontrollziele. Die agentenlose Architektur ermöglicht darüber hinaus eine verbesserte Überwachung von Zahlungsseiten ohne erheblichen Entwicklungs- oder Betriebsaufwand.



Compliance-Teams sind zu Recht skeptisch gegenüber den Aussagen von Anbietern. Dass Integrity360 Europe, ein unabhängiges Qualified Security Assessor Company, geprüft hat, wie unsere Plattform mit den PCI-DSS-Anforderungen 6.4.3 und 11.6.1 übereinstimmt, macht aus unseren Zusicherungen etwas, das Händler auf Grundlage konkreter Fakten bewerten können. Genau diese Unabhängigkeit macht die Bewertung so wertvoll."

Idan Cohen

Mitgründer und CEO von Reflectiz



Vorteile

- Unabhängige Bestätigung durch eine PCI Qualified Security Assessor Company
- Klare Ausrichtung an zentralen PCI-DSS-Kontrollzielen
- Mehr Vertrauen für Kunden und Prüfer
- Nachweisliche Unterstützung für Skriptinventarisierung und Autorisierung
- Verhaltensbasierte Überwachung über statische Dateihashes hinaus
- Kontinuierliche Überwachung von Zahlungsseiten und HTTP-Headern
- Reduzierter Aufwand bei der Vorbereitung von Nachweisen für QSA-Assessments
- Anerkennung des zusätzlichen Nutzens für die Sicherheit digitaler Lieferketten

Bei korrekter Konfiguration und Integration in ein umfassendes Governance-, Risk- und Compliance-Programm kann Reflectiz eine effizientere und nachhaltigere Alternative zu manuellen Skriptprüfungen und statischen Monitoring-Ansätzen bieten.

Blick in die Zukunft

Die unabhängige Bewertung bietet Reflectiz eine solide Grundlage, um aufzuzeigen, wie die Plattform Unternehmen bei der Erfüllung der PCI-DSS-Anforderungen für die Sicherheit von Zahlungsseiten unterstützen kann.

Darüber hinaus kann die Plattform einen breiteren Mehrwert schaffen, indem sie die Transparenz digitaler Lieferketten erhöht, Client-Side-Bedrohungen identifiziert und umfassendere Governance-, Datenschutz- und Compliance-Programme unterstützt.

Für berechnete SAQ-A-Händler kann eine korrekte Implementierung außerdem helfen nachzuweisen, dass Zahlungsseiten nicht anfällig für skriptbasierte Angriffe sind. Die tatsächliche Eignung und Compliance hängen jedoch weiterhin von der jeweiligen Umgebung und den eingesetzten Kontrollen des Händlers ab.



Über Integrity360

Integrity360 ist ein führender unabhängiger Spezialist für Cybersicherheit und PCI mit Aktivitäten in der EMEA-Region und Nordamerika und verfügt über Niederlassungen im Vereinigten Königreich und Irland, in Bulgarien, Italien, Schweden, Spanien, Deutschland, der Schweiz, Frankreich, Belgien, Litauen, der Ukraine, Afrika, der Karibik und Kanada. Das Unternehmen betreibt Security Operations Center (SOCs) in Dublin, Madrid, Sofia, Stockholm, Rom und Kapstadt und bietet eine kontinuierliche Überwachung und Incident Response über mehrere Zeitzeonen hinweg.

Mit mehr als 700 Mitarbeitenden, darunter über 580 dedizierte Cybersicherheitsexperten, bietet Integrity360 ein umfassendes Portfolio an Professional Services, Support- und Managed-Security-Services, das den gesamten Cyber-Risiko-Lebenszyklus abdeckt, von der Identifizierung und Prävention bis hin zu Erkennung, Reaktion und Wiederherstellung.

Gartner

Integrity360 wird in sechs Gartner-Marktübersichten zu den Themen „Managed Security Service Providers“, „Managed SIEM Services“, „Managed Detection and Response“, „Co-Managed Security Services“, „Incident Response“ und „Forensics“ aufgeführt.

3000+
Unternehmenskunden

585+
IT-Fachkräfte