Чек-лист внедрения PCI DSS 6.4.3

Контроль клиентских скриптов на платёжной странице

Назначение: помочь e-commerce-команде корректно и быстро внедрить требования PCI DSS 6.4.3 по контролю клиентских скриптов. Документ можно использовать как рабочий план и как набор артефактов для аудита.

Сфокусируйтесь на шагах, где вводятся данные карты/плательщика, а также на «около-чекаутных» экранах (итог заказа, доставка, купоны), откуда возможен перехват данных.

Чек-лист разбит на шесть обязательных областей. Для каждой указаны критерии приёмки и артефакты для аудита.

Шаги и критерии приёмки

- **Инвентаризация точек загрузки JavaScript**
  - Найдены все места загрузки: HTML/SSR-шаблоны, SPA, Tag Manager, сторонние виджеты/SDK, динамические вставки.
  - Сформирован реестр с полями: URL/имя, источник (1st/3rd party), назначение, владелец, среда (prod/stage), дата последнего ревью.
  - Назначен владелец реестра, описан процесс актуализации.
- **Бизнес-обоснование и владение**
  - Для каждого скрипта зафиксированы: бизнес-цель, согласующий владелец, дата следующего пересмотра, риски при отключении.
  - Описан процесс заявки на добавление/удаление скрипта (RFC/Jira) и критерии одобрения.
- **SRI-подписи (Subresource Integrity) в CI/CD**
  - В пайплайне настроена автогенерация SRI-хешей (SHA-256) для внешних и статических скриптов.
  - Деплой блокируется при несоответствии хеша (quality gate).
  - Документирован порядок обновления SRI при релизе.

Шаги и критерии приёмки (продолжение)

- **Client-side-мониторинг страниц оплаты (≤ 60 мин)**
  - Работает контроль целостности в том виде, как страницу получает браузер клиента (не ретроспективно).
  - Частота проверок ≤ 60 мин; собираются события: новые/изменённые скрипты, неизвестные источники, подозрительные слушатели.
  - Определены приоритеты алертов и каналы уведомлений.
- **Алерты и интеграция с SOC/эквайером**
  - События поступают в SIEM/SOC (MaxPatrol/другое), настроены корреляции и эскалация.
  - При критике выполняется план реагирования; при необходимости уведомляется банк-эквайер (например, через FinCERT API).
- **Хранение логов и отчётность**
  - Логи/результаты мониторинга хранятся ≥ 12 месяцев (PCI DSS) и по 152-ФЗ ст. 18.1.
  - Готовы артефакты для аудита: выгрузки из SIEM, копии политик, экспорт реестра скриптов.

Mapping на требования и роли

Соответствие требованиям и распределение ролей (RACI):

PCI DSS 6.4.3: Контроль изменения скриптов на страницах оплаты: инвентаризация, авторизация и мониторинг.

PCI DSS 11.6.1: Контроль изменения веб-страниц: мониторинг в том виде, как их получает браузер клиента.

Сопутствующее: CSP (report-only), SRI, политика сторонних скриптов, процесс RFC на добавление кода.

Роли и ответственность:

— CISO/ISO: Утверждение политики, приёмка рисков, взаимодействие с эквайером.

— Front-end Lead: Инвентаризация скриптов, внедрение SRI, исправления.

— DevOps/CI: Автогенерация SRI, quality gate, деплой.

— SOC/SIEM: Приём событий, корреляции, эскалация, отчёты.

— DPO/Юр.: Аспекты персональных данных/152-ФЗ, уведомления РКН (при необходимости).

Шаблон реестра скриптов

Шаблон реестра скриптов (минимальные поля). Ведите его в системе задач или в отдельном репозитории; по запросу аудитора предоставляйте экспорт в CSV/PDF.

Колонки: ID | URL/Имя скрипта | Источник (1st/3rd) | Назначение | Владелец | Среда (prod/stage) | SRI (SHA-256) | Дата ревью | Статус

Примеры:

001 | https://cdn.example.com/analytics.js | 3rd | Аналитика | Маркетинг | prod | sha256-XXXXX | 01.09.2025 | approved

002 | /static/js/checkout.bundle.js | 1st | Чекаут | FE-Lead | prod | sha256-YYYYY | 01.10.2025 | approved