

DESIGN CHALLENGE · SENIOR UX/UI · XOPER0 · 2126

VitaVault — user journey

Pełna ścieżka administratora danych statku ISS Athena: od sygnału o ryzyku, przez tworzenie kopii zapasowej danych o zdrowiu 300 osób, po weryfikację, przywracanie i audyt luk.

Persona	Kai Nowak — administrator danych pokładowych, nie lekarz
Kontekst	Ciągła telemetria: biometria, styl życia, aktywność, nastrój (738 GB / dobę)
Cel główny	Zero luk w danych i sprawdzone, wykonalne przywracanie
Zakres dokumentu	6 etapów ścieżki + 3 scenariusze awaryjne + zasady projektowe

Mapa podróży użytkownika

Jeden przebieg end-to-end. Każdy etap: co użytkownik chce osiągnąć, co widzi w interfejsie, jaką podejmuje decyzję, co czuje i co się stanie, jeśli etap zawiedzie.

ETAP	EKRAN	CEL UŻYTKOWNIKA	CO WIDZI	DECYZJA	EMOCJA	RYZYKO, GDY ZAWIEDZIE
01 SYGNAŁ	Dashboard	Dowiedzieć się, czy dane są bezpieczne — bez czytania raportów.	Status ostatniej kopii, zaległy transfer do chmury, okno łączności zamykające się za 3 h 42 min, alert biometryczny (P-014).	Kliknąć „Uruchom kopię” prosto z alertu.	<i>Czułość, presja czasu</i>	Administrator dowiaduje się o luce dopiero podczas awarii.
02 ZAKRES	Kreator, krok 1/4	Wybrać, co objąć kopią, nie znając architektury systemu.	4 kategorie z rozmiarem, liczbą strumieni, poziomem wrażliwości i czasem ostatniej kopii; odznaczenie kategorii krytycznej oznacza odstępstwo od polityki ISA-2119.	Zostawić pełny zakres lub świadomie go zawęzić.	<i>Kontrola</i>	Cicha luka w danych krytycznych dla życia.
03 CELE	Kreator, krok 2/4	Rozłożyć ryzyko na niezależne lokalizacje.	CORE-01 (2 ms), VAULT-07 (inny moduł, niezależne zasilanie), ISA-CLOUD (42 min opóźnienia, transfer asynchroniczny). Brak celu poza statkiem = czerwone ostrzeżenie.	Zaznaczyć min. jedną kopię poza statkiem.	<i>Jasność</i>	Awaria statku kasuje wszystkie kopie naraz.
04 POLITYKA	Kreator, krok 3/4	Ustalić, ile danych wolno stracić.	Częstotliwość przetłumaczona na ryzyko („co 6 h = do 6 h pomiarów do odtworzenia”), retencja, szyfrowanie end-to-end, kolejkowanie offline.	Skrócić okno RPO dla danych krytycznych.	<i>Pewność</i>	Zbyt duże RPO — nieodtworzalna dziura czasowa.
05 POTWIERDŹ	Kreator, krok 4/4	Sprawdzić skutki decyzji zanim cokolwiek ruszy.	Jedna karta podsumowania: zakres, cele, RPO, szacowany czas, status zgodności z polityką, lista ostrzeżeń.	Uruchomić kopię lub cofnąć się do konkretnego kroku.	<i>Spokój</i>	Uruchomienie konfiguracji, której nikt nie rozumie.
06 WYKONANIE	Progres + sukces	Mieć dowód, że kopia jest odtwarzalna.	Progres per kategoria i per cel, suma kontrolna integralności, utworzony punkt przywracania (RP-2842), skrót do testu odtworzenia.	Wykonać test recovery / wrócić do dashboardu.	<i>Ułga, zamknięcie</i>	Fałszywe poczucie bezpieczeństwa — kopia istnieje, ale nie działa.

Trzy scenariusze awaryjne

Sytuacje z briefu, przełożone na konkretne ekrany i działania w produkcji.

Ostry ból brzucha u pasażerki (P-014)

Ekran: Raport medyczny 72 h

- Biometria: tętno, HRV, temperatura, ciśnienie, saturacja, markery zapalne.
- Żywienie i hydratacja z numerami partii posiłków; ekspozycja na promieniowanie i grawitację.
- Sen, poziom stresu, zgłoszenia samopoczucia, odwiedzone strefy statku.
- Korelacja: kto jeszcze jadł tę partię i był w tych strefach (wykrycie ogniska).
- Wskaźnik kompletności okna — administrator ręczy za pełność, nie za diagnozę.

Utrata wszystkich danych na statku

Ekran: Plan przywracania wg ryzyka

- Źródło: ISA-CLOUD — jedyna kopia poza statkiem, dlatego jest wymagana przez politykę.
- Kolejność: alerty i bieżąca biometria → profile zdrowotne → logi dostępu → dane analityczne.
- Strata ograniczona do okna RPO; dane krytyczne replikowane strumieniowo, nie tylko harmonogramem.
- Po przywróceniu: weryfikacja integralności, rekonstrukcja luki z pamięci lokalnej opasek, raport do dowództwa.

Brak danych o działaniach w sterowni

Ekran: Audyt luk (GAP-102)

- Zapis append-only: dane można dopisać, nie da się skasować bez śladu — system sam podnosi alert o luce.
- Dokładne okno: 2126-04-10 21:14 - 23:02, brakujące logi dostępu i aktywność 3 osób.
- Rekonstrukcja pośrednia: biometria opasek, logi śluz i drzwi, zużycie energii konsol, telemetria kursu, kopia w chmurze.
- Zamrożenie punktów przywracania jako materiału dowodowego i przegląd uprawnień.

Założenia i zasady projektowe

Brief celowo zostawia luki — poniżej to, co przyjąłem, i reguły, które utrzymują spójność ścieżki.

Przyjęte założenia · Administrator widzi metadane i status strumieni, nie treść medyczną. · Backup działa na migawkach i nigdy nie przerywa zbierania telemetrii. · Łączność z Ziemią jest okresowa i opóźniona — chmura jest asynchroniczna. · Polityka ISA-2119 wymaga wszystkich 4 kategorii i jednej kopii poza statkiem. · Załoga: ok. 300 osób; prototyp pokazuje reprezentatywną próbkę. · Dostęp do danych o zdrowiu i nastroju jest logowany i wymaga uzasadnienia.	Zasady projektowe Kreator zamiast tabeli ustawień Backup pod presją nie może wymagać wiedzy o architekturze: 4 decyzje, każda z widocznym skutkiem. Konsekwencja zamiast opcji Nie „wybierz cel”, tylko „bez kopii poza statkiem tracisz wszystko przy awarii statku”. Priorytet ludzki, nie techniczny Kolejność przywracania wg ryzyka dla życia, nie wg rozmiaru danych. Weryfikacja jako część sukcesu Ścieżka kończy się dopiero po sprawdzeniu integralności i propozycji testu recovery.
---	--

Mierniki sukcesu ścieżki

MIERNIK	CEL	GDZIE WIDOCZNY W PRODUKCIE
Czas od sygnału do uruchomienia kopii	< 90 sekund	Akcja startuje z alertu na dashboardzie, nie z menu
Udział kopii z kopią poza statkiem	100%	Ostrzeżenie blokujące w kroku 2/4
Punkty przywracania z potwierdzoną integralnością	> 99%	Suma kontrolna po wykonaniu + lista RP
Wykryte luki w danych obsłużone < 24 h	100%	Ekran audytu z automatycznym alertem o luce