Stop account takeovers by cybercriminals

Protect your organization against the biggest cybercrime threat, simple and effective

- 🔐 **Full control:** sensitive information doesn't leave your organization
- 🛡️ **Maximum security & efficiency:** no false alarms, only true positives
- ⚡ **Peace of mind:** Scattered Secrets handles the heavy lifting & analysis
- ✅ **In-control:** protect all accounts & demonstrate compliance (EU CRA/NIS2)
- 🛠️ **Accessible:** no code updates required for the target application
- 🇳🇱 **Sovereignty:** Scattered Secrets is a 100% Dutch company (EU)

The Process

Step 1: Preparation

- On your secure system:
  - Export account information
  - Convert sensitive account information into securely exchangeable data (pseudonymization & encryption)
- Only pseudonymized and encrypted data leaves the organization
- Works with virtually all IAM systems and account databases

Step 3: Follow-up

- The organization converts the pseudonymized results into vulnerable accounts
- Take action for vulnerable accounts:
  - Block accounts
  - Conduct fraud investigations, etc.

Step 2: Match leaked data

- Compare against billions of leaked credentials
- No false alarms, only true positives
- Results contain pseudonymized data

Pseudonymization? Encryption?

Step 1: Preparation

Your organization pseudonymizes the account names and encrypts the password hashes using asymmetric cryptography. The translation table for (de)pseudonymization and the private key never leave the organization. Scattered Secrets therefore does not receive sensitive information.

Step 2: Match leaked data

Scattered Secrets matches the pseudonymized and encrypted data against billions of leaked accounts originating from hacked third parties and stealer logs. We cannot reconstruct account names or password hashes, as we do not have access to the translation table or private key.

Step 3: Follow-up

Your organization reconnects the pseudonymized results to account names using the translation table. By integrating the process within your organization, fully automated protection becomes possible without time-consuming manual analysis and without false alarms.