SERVIZIO PASSWORD HEALTH CHECK

Password Health Check è un servizio di **Security Assessment** realizzato e gestito dal Team Cybersecurity di Mead e rivolto alle credenziali degli utenti presenti nell'Active Directory aziendale.

Le password deboli sono spesso citate come una delle più gravi minacce alla sicurezza del sistema aziendale.
Molti utenti scelgono password semplici e facili da ricordare per l'utilizzo quotidiano.

Tali password, anche se rispettano le policy aziendali nell'ambito delle "password sicure", sono molto spesso facili da indovinare e/o "bucare".

Il servizio di password Health Check offre all'impresa un **quadro generale sullo stato attuale in termini di robustezza delle password** degli utenti ed **indentifica le aree di debolezza** in modo da porre immediato rimedio.

In particolare, si cercherà di "violare" le credenziali d'accesso degli utenti dell'azienda in modo da misurare la robustezza delle password ed essere preparati in caso di un attacco al perimetro aziendale.

L'attività viene eseguita presso i laboratori Mead e prevede numerosi controlli e funzionalità specifiche.

Grazie ad un algoritmo particolare, sarà anche possibile **verificare se gli indirizzi email aziendali sono stati già vittima in passato di data-breach**, e porre quindi rimedio ad eventuali compromissioni di sicurezza.

Il servizio Password Health Check si quota volta per volta in base al numero degli utenti dell'Active Directory presente e rispetto alla severità di controlli di sicurezza che si desidera effettuare.

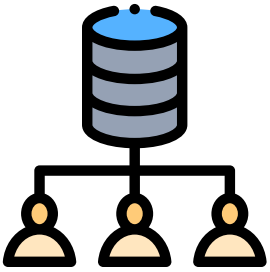
E' possibile costruire un **dizionario password personalizzato** per ogni Azienda in modo da **aumentare la raffinatezza** dell'attività di Assessment. Verranno utilizzati ad esempio i nomi dei prodotti aziendali o dei dipendenti, in modo da rafforzare la qualità del servizio.

VANTAGGI DELLA SOLUZIONE

- Innalzamento dei livelli di sicurezza interna
- Conoscenza dei punti deboli e possibilità immediata di rimedio
- Riduzione dei costi dovuti ad azioni errate dei dipendenti
- Aumento della consapevolezza dei pericoli per gli utenti
- Analisi dei punti critici
- Compliance alle normative

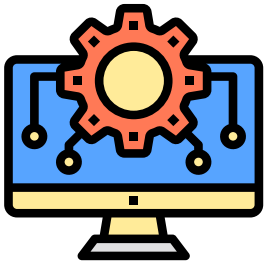
SCHEMA DI FUNZIONAMENTO

Il database della password viene estratto dal Domain Controller

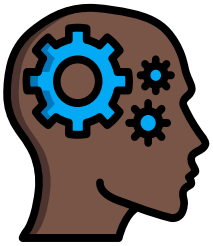


Il database viene cifrato e trasferito verso Mead

Il database viene decifrato e processato dall'algoritmo



I risultati vengono analizzati da un Consulente di Sicurezza



Il report finale viene inviato al cliente

START