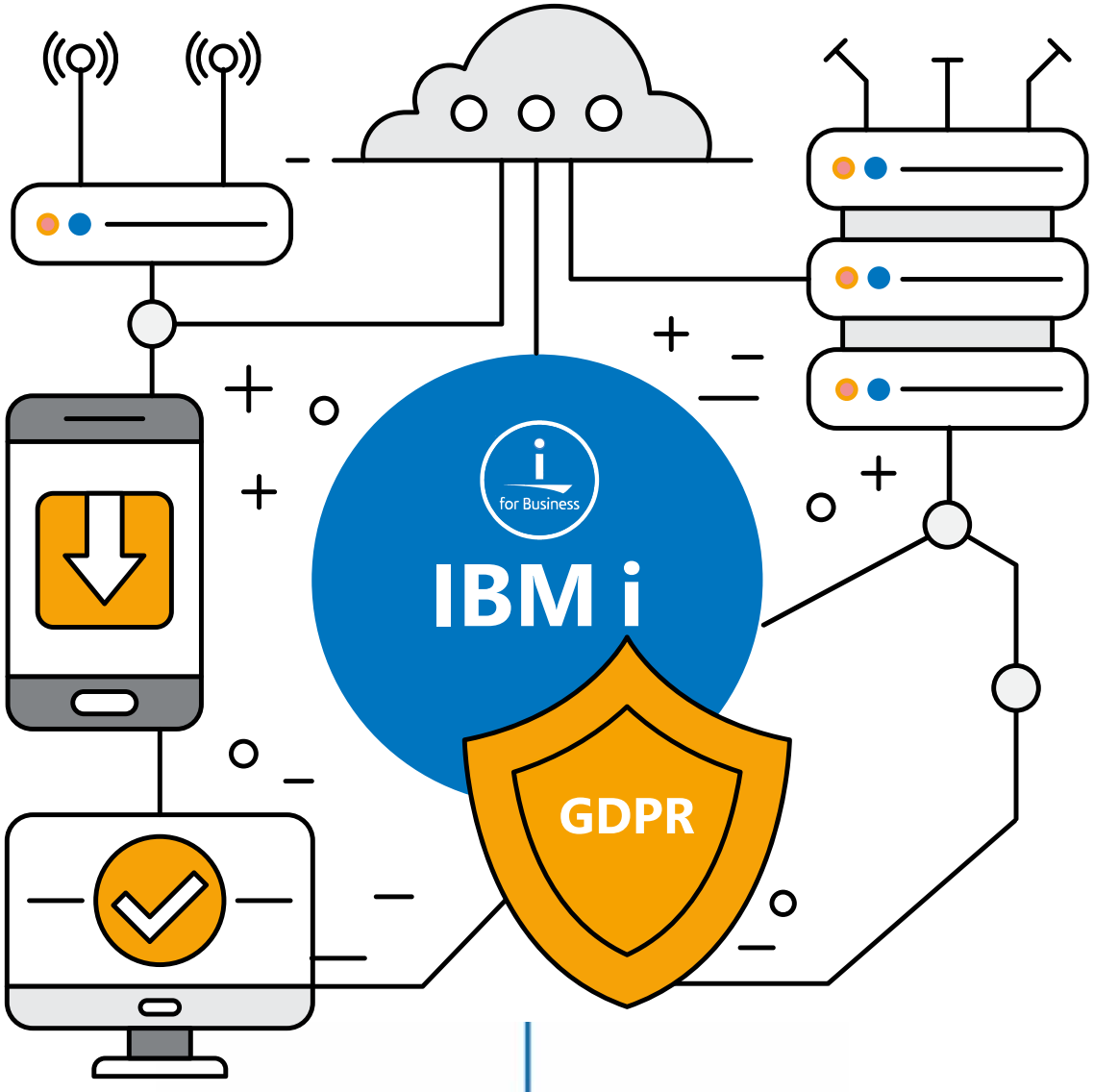
OS/400 Security Alerting

MONITORING SOLUTION



SOLUZIONI EDP

Consulenza completa e su misura, dall'IT al Business.

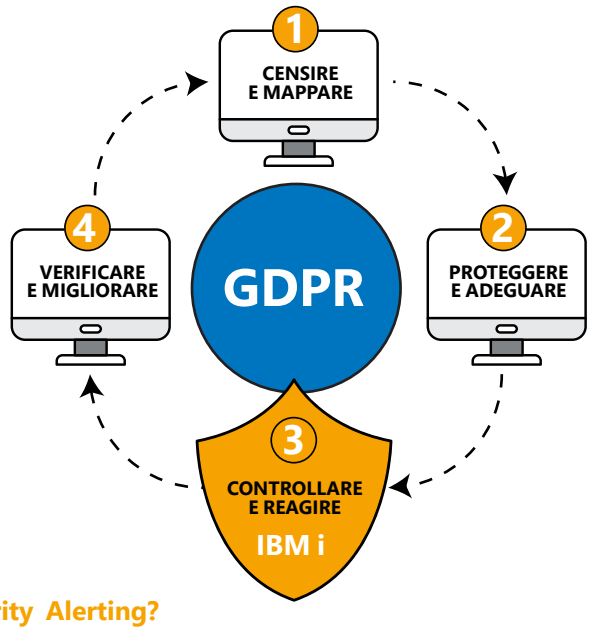
OS/400 Security Alerting

Obiettivo sicurezza IBM i

Su **IBM i** vengono eseguite le più importanti applicazioni aziendali. Il sistema registra già di suo tutta una serie di attività critiche fatte dai suoi utenti.
È quindi fondamentale, per una corretta gestione della sicurezza, poter **attivare, elaborare ed interpretare** questi eventi.

Ad esempio, la digitazione di una password errata o relativa ad un utente inesistente, che nel giro di pochi minuti tenta un accesso simultaneo da IP diversi, può essere considerato un tentativo d'intrusione. Allo stesso modo il collegamento da parte di un utente disabilitato, che viene abilitato e subito dopo l'attività disabilitato nuovamente, è sintomatico di un'azione critica avvenuta.

Per questi motivi un'opportuna **analisi dei dati** registrati dal sistema diventa la base di partenza per un corretto **controllo della sicurezza in ambiente IBM i.**



Cosa possiamo fare con il modulo di sicurezza OS400 Security Alerting?

- Configurare una reportistica schedulata e automatizzata degli eventi critici avvenuti per le analisi e le verifiche di ciò che è accaduto
- Correlare azioni diverse per rilevare gli eventi anomali
- Avvisare istantaneamente la presenza di una situazione anomala

Quali azioni possiamo collezionare ed analizzare con OS/400 Security Alerting?

- Creazione di utenti o gruppi
- Cancellazione di utenti o gruppi
- Gruppi aggiunti o cancellati sugli utenti
- Utenti disabilitati o abilitati
- IP di provenienza di alcune azioni
- Logon e logoff
- Password errate
- Tentativi di accesso con utenti inesistenti
- Gruppi aggiunti o cancellati sugli utenti
- Lettura o modifica di files critici
- Lettura o modifica di una cartella IFS
- Cambio delle regole di audit
- Cancellazione dell'audit

Quali eventi critici possiamo rilevare con OS/400 Security Alerting?

- Utenti creati e cancellati in un tempo ristretto
- Troppi utenti disabilitati in poco tempo
- Utenti creati e collegati immediatamente dopo
- Un utente che si collega da IP diversi
- Password errate multiple di più utenti in poco tempo
- Utente inesistente che prova più volte l'accesso
- Riconfigurazione o cancellazione dell'audit non prevista
- Modifica di file critici da parte di utenti non previsti

OS/400 Security Alerting è una soluzione che si basa sul prodotto **TANGO/04**, il software leader nel Monitoraggio aziendale della Tecnologia ed il Controllo del Business.
OS/400 Security Alerting nasce dalla nostra conoscenza pluritrentennale del mondo IBM i (AS/400), unita all'esperienza raccolta dai numerosi progetti realizzati con la suite TANGO/04 HelpSystems.
Così è nata OS/400 Security Alerting: la nostra esperienza racchiusa in un'unica soluzione facile e di immediata implementazione pensata e **dedicata al mondo IBM i.**

OS/400 Security Alerting è un prodotto
SOLUZIONI EDP

0161.56924 www.soluzioniedp.it info@soluzioniedp.it