BEZPEČNOSTNÉ KONTROLY DATABÁZ S JASNÝM VÝSLEDKOM

GuardVea

Databáza funguje.
Je aj bezpečne nastavená?

Overte nastavenia. Pochopte zistenia.
Rozhodnite, čo treba napraviť.



Od bezpečnostných odporúčaní
ku konkrétnym krokom pre váš tím.

SoftVea, s.r.o.

www.guardvea.com · info@softvea.com · +421 940 404 737

NA ČO JE GUARDVEA DOBRÁ

Majte jasno v nastavení databáz.

Aplikácia beží a používatelia pracujú. To ešte neodpovedá na otázku, ako je databáza zabezpečená.



Firma uchováva v databáze objednávky, kontakty či prevádzkové údaje. Správca pozná jej technickú stránku, vedenie sa však potrebuje rozhodnúť, čomu venovať čas a peniaze. GuardVea pomáha overiť vybrané bezpečnostné nastavenia a ukázať, ktoré odporúčania sú splnené a ktoré si vyžadujú pozornosť.

Kontrola má konkrétne pravidlá

Zvolíte súbor odporúčaní pre svoje databázové prostredie. Pri jednotlivých kontrolách nájdete, čo sa overuje, prečo to má význam a aký výsledok sa očakáva. Rozhovor o bezpečnosti tak môžete oprieť o konkrétne nastavenia.

Výsledok pomôže určiť ďalšiu prácu

V prehľade sa dostanete od databázového servera ku konkrétnej kontrole a jej výsledku. Správca môže preveriť podrobnosti a odporúčaný postup nápravy. Vedenie získa zrozumiteľnejší podklad na dohodu o ďalších krokoch.

> ### Keď sa vedenie pýta na bezpečnosť
> Namiesto všeobecného uistenia môžete prejsť vybrané kontroly, ich výsledky a zistenia, ktoré ešte treba riešiť.

ČO SI V SYSTÉME PRIPRAVÍTE

Vaše servery. Váš rozsah kontroly.

Začnite tým, čo potrebujete overiť a na ktorom databázovom prostredí.

Určíte databázové servery

Do objednávky pridáte adresy serverov a podľa potreby ich pomenujete. Máte tak jasno, na ktoré prostredia sa kontrola vzťahuje. Pri príprave sa oplatí dohodnúť aj správcu, ktorý zabezpečí pripojenie a bude vedieť vysvetliť prevádzkové súvislosti.

Vaše servery	Vaše kontroly	Vaše výsledky
Databázy, ktoré chcete preveriť.	Odporúčania a zvolený profil.	Zistenia a podklady na nápravu.

Vyberiete vhodné odporúčania

CIS benchmark je súbor odporúčaní pre bezpečné nastavenie konkrétnej technológie. Vyberiete si dostupný súbor, jeho verziu a vhodný profil. Kontrola potom vychádza z určeného rozsahu, ku ktorému sa môžete pri čítaní výsledkov vrátiť.

Zohľadníte spôsob prevádzky

Databáza na vlastnom serveri a spravovaná cloudová služba ponúkajú správcovi odlišné možnosti. Pri výbere profilu preto záleží aj na tom, ku ktorým nastaveniam máte prístup. Rozsah overovania má zodpovedať tomu, ako databázu používate.

Pracujete v internetovom prehliadači

V spoločnom prostredí otvoríte knižnicu odporúčaní, pripravíte objednávku a prejdete výsledky kontrol. Nástroje sa otvárajú v samostatných oknách nad pracovnou plochou. K jednotlivým častiam sa dostanete cez panel s ikonami.

> ### Pred kontrolou si ujasnite rozsah
> Ktorý server preverujete, podľa akej verzie odporúčaní a s akým profilom? Tieto údaje dávajú výsledku potrebný kontext.

AKO KONTROLA PREBIEHA

Od výberu servera po výsledok.

Jednotlivé kroky na seba nadväzujú. Vy viete, čo pripraviť a kde hľadať zistenia.



01 Vyberiete rozsah

Určíte databázové servery, dostupný benchmark a profil kontroly. V objednávke si zvolíte položky z cenníka a skontrolujete údaje.

02 Pripravíte pripojenie

Správca vytvorí určený databázový účet a zabezpečí potrebný prístup. Overenie pripojenia pomôže zistiť, či je možné so serverom komunikovať.

03 Prebehne overovanie

Po úhrade objednávky sa spustí bezpečnostný audit. Automatické kontroly overujú nastavenia; pri manuálnych kontrolách doplníte odpovede a vyjadrenie.

04 Prejdete zistenia

Pozriete si stav, skóre a podrobnosti jednotlivých kontrol. Pri zisteniach prejdete odporúčanú nápravu a dohodnete ďalšie kroky so správcom.

> Výsledok má viesť k ďalšiemu kroku
> Dôležité je rozumieť zisteniu, jeho významu pre vaše prostredie aj tomu, kto sa bude venovať prípadnej náprave.

KNIŽNICA BEZPEČNOSTNÝCH ODPORÚČANÍ

Viete, podľa čoho sa kontroluje.

Pri každom odporúčaní sa môžete pozrieť na jeho obsah aj dôvod, prečo sa mu venovať.



Súbor a verzia

V knižnici vyberiete konkrétny súbor odporúčaní. Rozlíšenie verzie pomáha pomenovať, z akých podkladov kontrola vychádza. Pri ďalšej práci tak môžete hovoriť o tom istom rozsahu.

Popis kontroly

Pri vybranom odporúčaní si prečítate, čo sa má overiť. Technický názov dostane vysvetlenie a správca sa ľahšie zorientuje v tom, ktorého nastavenia sa požiadavka týka.

Odôvodnenie a dopad

Nestačí vedieť, že sa nastavenie odporúča. Potrebujete rozumieť aj dôvodu a možnému dopadu zmeny. Tieto informácie pomáhajú pri posúdení odporúčania vo vašej prevádzke.

Postup overenia a nápravy

Detail môže obsahovať kroky auditu, očakávaný výsledok aj postup nápravy. Správca má poruke podklady, ktoré mu pomôžu zistenie preveriť a pripraviť riešenie.

> ### Keď sa kolega pýta, prečo to meniť
> Otvorte konkrétne odporúčanie. Spolu prejdete jeho účel, výsledok kontroly aj dopad navrhovanej zmeny.

VÝBER PROFILU

Kontrola podľa vášho prostredia.

Vyberte si dostupný profil, ktorý zodpovedá spôsobu prevádzky a požadovanej prísnosti.



Základný serverový profil

Profil L1_server je určený pre databázový server s prístupom k operačnému systému. Predstavuje východisko pre overenie základných odporúčaní v prostredí, ktoré spravujete.

Cloudový profil

Profil L1_cloud je v objednávke určený pre SQL Server na AWS RDS. Zohľadňuje prostredie spravovanej služby. Pri výbere preto vychádzajte z konkrétnej databázovej technológie aj spôsobu jej prevádzky.

Prísnejší serverový profil

Profil L2_server rozširuje požiadavky na prísnejšie nastavenie. Niektoré odporúčania môžu ovplyvniť prevádzku alebo výkon. Pred ich použitím je potrebné posúdiť, ako sa prejavia vo vašich aplikáciách.

> Napríklad pri databáze obchodnej aplikácie
> Správca spolu s vlastníkom aplikácie vyberie profil a preverí dopad odporúčaní. Výsledok potom hodnotíte v dohodnutom rozsahu.

Konkrétny benchmark a dostupné profily si overíte pri príprave objednávky. Výber má vychádzať z vášho prostredia.

AUTOMATICKÉ KONTROLY

Overte konkrétne nastavenia.

Pri podporovaných kontrolách získate výsledok z overenia databázy, ku ktorému sa môžete vrátiť.



Pripojenie k serveru

Pred samotným overovaním je potrebné funkčné pripojenie. V prehľade vidíte, či sa spojenie podarilo. Ak nie, správca má dôvod preveriť dostupnosť servera, účet alebo potrebné oprávnenia.

Priebeh overovania

Pri spustení kontrol sledujete ich stav a priebeh. Rozlíšite čakanie, prebiehajúce spracovanie, dokončenie aj zlyhanie. Viete tak, či už máte výsledok alebo sa ešte treba venovať samotnému behu.

Výsledok pri odporúčaní

Každú kontrolu posudzujete v súvislosti s tým, čo mala overiť. K dispozícii máte skóre a podrobnosti výsledku. Správca môže prejsť zistenie spolu s očakávaným nastavením.

Podklad na rozhovor

Vedenie a správca nemusia začínať od všeobecnej otázky, či je všetko v poriadku. Vyberú konkrétnu kontrolu, pozrú sa na jej výsledok a určia, čo ešte treba preveriť.

> ### Keď sa kontrola nedokončí
> Najprv preveríte príčinu spracovania. Nedostupný server alebo chyba kontroly potrebujú iný ďalší krok než zistené nevyhovujúce nastavenie.

MANUÁLNE OVEROVANIE

Niečo musí potvrdiť človek.

Tam, kde treba poznať postupy alebo prevádzkové súvislosti, doplníte odpovede v dotazníku.



Otázky k odporúčaniu

Manuálna kontrola otvorí dotazník k vybranému odporúčaniu. Zodpovedná osoba odpovie na otázky a môže pridať krátke vyjadrenie. Kontrola tak zachytí aj informácie, ktoré nemožno vyčítať iba z technického nastavenia.

Vyjadrenie k výsledku

K odpovediam doplníte záverečné vyjadrenie o celkovom plnení odporúčania. Kolega, ktorý sa k výsledku vráti neskôr, má k dispozícii aj slovné vysvetlenie.

Automatické a manuálne kroky sa dopĺňajú

Automatické overenie pomáha pri konkrétnych nastaveniach. Manuálny dotazník využije znalosť ľudí, ktorí prostredie spravujú. V prehľade sú tieto typy kontrol rozlíšené, takže viete, akým spôsobom sa k výsledku dospelo.

> Napríklad pri firemnom postupe
> Technický výsledok nemusí vysvetliť, ako tím v praxi postupuje. Odpoveď a poznámka zodpovednej osoby doplnia potrebný kontext.

VÝSLEDKY A PREHĽAD

Od prehľadu ku konkrétnemu zisteniu.

Najprv si pozriete stav servera a kontrol. Potom otvoríte to, čomu sa potrebujete venovať.



Objednávky a servery

V prehľade vyberiete objednávku a jej databázové ciele. Máte pri sebe rozsah kontroly aj informácie o jej priebehu. Pri viacerých serveroch si viete určiť, ktorého prostredia sa výsledok týka.

Skóre a detail výsledku

Pri vybranej kontrole vidíte skóre, stav a report. Skóre slúži na rýchlu orientáciu. Pri rozhodovaní o ďalšom postupe ho doplníte čítaním zistení a obsahu odporúčania.

Výsledok čítajte v súvislostiach

Záleží na profile, rozsahu kontroly aj na tom, ako databázu používate. Správca vie vysvetliť technické podrobnosti a vlastník aplikácie doplniť význam pre prevádzku. Spolu tak určia vhodný ďalší krok.

> ### Na pracovnom stretnutí
> Vyberiete server a otvoríte konkrétnu kontrolu. Z výsledku prejdete rovno k otázke, čo treba preveriť, kto to vybaví a kedy sa k tomu vrátite.

ODPORÚČANIA NA NÁPRAVU

Zistenie je začiatok ďalšej práce.

Keď kontrola ukáže problém, potrebujete rozumieť odporúčanej zmene a jej dopadu.



Postup máte pri odporúčaní

V detaile nájdete časť venovanú náprave. Správca sa môže oprieť o popísané kroky a porovnať ich s aktuálnym stavom databázy. Nemusí začínať iba od stručného označenia nevyhovujúceho výsledku.

Rozhodnutie patrí k vašej prevádzke

Odporúčanú zmenu posúďte spolu s tým, ktoré aplikácie databázu používajú a čo od nej potrebujú. Pri plánovaní pomôže poznať možný dopad, zodpovednú osobu a vhodný termín zásahu.

Po zmene si overíte výsledok

Po vykonaní nápravy má zmysel príslušnú kontrolu zopakovať a prejsť nový výsledok. Tak zistíte, či sa nastavenie dostalo do očakávaného stavu alebo si ešte vyžaduje ďalšiu pozornosť.

> ### Keď sa má meniť dôležité nastavenie
> Správca prejde odporúčanie s vlastníkom aplikácie a dohodnú postup. Výsledok kontroly je podkladom pre túto prácu.

PRÍPRAVA PRÍSTUPU

Pripojenie pripraví váš správca.

Pred kontrolou si ujasníte potrebný účet, dostupnosť servera a zodpovednosť za prípravu.



Určený databázový účet

Objednávka pracuje s databázovým používateľom guardvea. Správca ho vytvorí na uvedených serveroch podľa požiadaviek kontroly. V systéme potvrdíte, že je účet pripravený.

Prístupové údaje

Pri príprave objednávky vygenerujete heslo pre určený účet. Správca zabezpečí jeho nastavenie na serveroch, ktoré patria do rozsahu. Údaje musia zodpovedať pripravenému pripojeniu.

Overenie dostupnosti

Pred spustením je potrebné preveriť, či je možné server dosiahnuť a prihlásiť sa. Stav pripojenia pomáha oddeliť problém s prípravou prístupu od samotného výsledku bezpečnostnej kontroly.

Ukončenie prístupu

Súčasťou objednávky je aj potvrdenie, že po dokončení auditu bude používateľ guardvea zmazaný. Dohodnite preto so správcom aj tento záverečný krok.

> ### Príprava má svojho človeka
> Určite správcu, ktorý pripraví účet, preverí spojenie a po dokončení auditu zabezpečí zrušenie prístupu.

PRE KOHO JE GUARDVEA

Každý potrebuje iný pohľad.

Spoločný výsledok pomáha spojiť technické zistenia s rozhodovaním o firemnej prevádzke.



Vedenie firmy

Získa konkrétnejší podklad na rozhovor o zabezpečení databáz. Vie sa pýtať na zistenia, potrebnú prácu aj ďalší postup.

Správca databáz

Prejde odporúčania, výsledky a postupy nápravy pri konkrétnom prostredí. Má z čoho vychádzať pri príprave zmien.

Bezpečnostný tím

Pracuje s určeným rozsahom kontroly a jej výsledkami. Pri technických zisteniach môže nadviazať na prácu správcu.

Vlastník aplikácie

Doplní, čo aplikácia od databázy potrebuje. Pomáha posúdiť, ako by sa odporúčaná zmena prejavila v každodennej práci.

Externý IT partner

Môže s firmou prejsť rozsah overovania a prípravu prostredia. Pri zisteniach sa rozhovor opiera o konkrétne kontroly.

> ### Spoločný jazyk pre ďalší krok
> Správca vysvetlí zistenie, vlastník aplikácie doplní prevádzkové súvislosti a vedenie určí čas a zdroje na riešenie.

SÚVISLOSTI A VYSVETLENIA

Rozumiete aj dôvodu kontroly.

Odporúčanie má svoj účel. Pri posudzovaní výsledku pomôže poznať aj jeho širší kontext.



Prečo sa to overuje

Odôvodnenie pri odporúčaní vysvetľuje, prečo má dané nastavenie význam. Správca môže lepšie objasniť, prečo sa zisteniu venovať a čo treba pri rozhodovaní zvážiť.

Čo môže zmena ovplyvniť

Časť venovaná dopadu pomáha pri plánovaní nápravy. Technické odporúčanie tak môžete čítať spolu s tým, aké požiadavky majú aplikácie a prevádzka.

Referencie a nadväzujúce informácie

V detaile sú k dispozícii aj referencie a väzby na CIS Controls, ak ich podklady obsahujú. Pri potrebe podrobnejšieho posúdenia máte kam pokračovať.

> ### Keď potrebujete odporúčanie vysvetliť vedeniu
> Začnite jeho účelom, ukážte výsledok a doplňte možný dopad nápravy. Z technického detailu vznikne podklad na rozhodnutie.

BEŽNÁ SITUÁCIA Z PRAXE

Nová aplikácia. Nové otázky.

Firma pripravuje nasadenie aplikácie a chce si preveriť nastavenie jej databázového prostredia.



Pred kontrolou

Správca určí databázový server a dostupný benchmark. S vlastníkom aplikácie vyberie profil, pripraví potrebný účet a preverí pripojenie.

Počas overovania

Tím sleduje priebeh automatických kontrol. Pri manuálnych odporúčaniach zodpovedná osoba doplní odpovede a vysvetlenie k tomu, ako firma postupuje.

Pri čítaní výsledkov

Správca otvorí zistenia a prejde ich s vlastníkom aplikácie. Pri nevyhovujúcich nastaveniach posúdia odporúčanú nápravu a jej dopad.

Pri plánovaní ďalšej práce

Firma si určí zodpovednosť a termín prípadných úprav. Po zmene môže príslušné kontroly zopakovať a overiť nový stav databázy.

> ### Od otázky k rozhodnutiu
> Namiesto všeobecnej diskusie má tím konkrétne zistenia. Vie, čo potrebuje preveriť a na čom sa dohodnúť pred ďalším krokom.

ČO SI Z KONTROLY ODNESIETE

Jasnejší podklad pre váš tím.

Hodnota kontroly je v tom, že pomôže pochopiť stav a pripraviť ďalšiu prácu.



Prehľad o overenom rozsahu

Viete, ktoré servery a odporúčania patrili do kontroly a aký profil ste zvolili. K výsledkom sa vraciate spolu s týmto kontextom, takže je jasné, čo presne bolo predmetom overovania.

Konkrétne zistenia

Pri jednotlivých odporúčaniach vidíte výsledok a podrobnosti. Správca má podklad na preverenie nastavenia a vedenie sa môže pýtať na ďalší postup pri konkrétnych zisteniach.

Podklady na ďalšie kroky

Popis, odôvodnenie, dopad a postup nápravy pomáhajú pripraviť riešenie. Výsledok sa týka vybraných kontrol; pri rozhodovaní ho hodnotíte spolu s ostatnými informáciami o bezpečnosti firmy.

> ### Keď kontrola skončí
> Dohodnite, ktoré zistenia preveríte, kto sa im bude venovať a ako overíte výsledok zmien. Tak môže kontrola pomôcť aj pri ďalšej práci.

AKO ZAČAŤ

Začnite jedným databázovým prostredím.

Vyberme konkrétny server a otázky, na ktoré potrebujete odpoveď. Rozsah pripravíme podľa vášho prostredia.

1. Povedzte nám, čo prevádzkujete

Pripravte si typ a verziu databázy, spôsob jej prevádzky a stručný opis aplikácií, ktoré ju používajú. Spolu prejdeme, čo potrebujete overiť a kto sa u vás stará o technickú prípravu.

2. Dohodneme vhodný rozsah

Pozrieme sa na dostupné benchmarky, profily a požadované kontroly. Správca pripraví prístup a pripojenie. Pred vytvorením objednávky si prejdete jej položky a cenu.

3. Prejdete výsledky a ďalšiu prácu

Po vykonaní kontroly sa pozriete na zistenia aj odporúčania. S tímom určíte, ktoré nastavenia treba preveriť a aké zmeny pripraviť. Podľa výsledku môžete pokračovať ďalšími databázami.

Vaše prostredie

Typ a verzia databázy · Spôsob prevádzky

Rozsah kontroly

Databázové servery · Benchmark · Profil

Ďalší postup

Výsledky · Posúdenie zistení · Náprava

Máte konkrétne požiadavky?

Opíšte svoje databázové prostredie a cieľ overovania. Prejdeme s vami dostupnosť vhodných kontrol aj potrebnú prípravu. Už na začiatku tak bude jasnejšie, čo má byť výsledkom.

> **Na prvý rozhovor stačí konkrétny príklad**
> Napríklad databáza vašej hlavnej aplikácie, jej verzia a spôsob prevádzky. Na tom si ukážeme vhodný ďalší postup.

OZVITE SA NÁM

Pozrime sa na vaše databázy.

Radi s vami prejdeme, čo potrebujete overiť a ako vám pri tom môže pomôcť GuardVea.



Každé prostredie má svoje požiadavky. Niekto pripravuje novú aplikáciu, iný chce preveriť existujúci server alebo získať podklad na bezpečnostné úpravy. Začnime tým, čo je dôležité pre vašu firmu.

Dohodnime prvý rozsah kontroly

Napíšte nám alebo zavolajte. Prejdeme typ databázy, spôsob prevádzky a cieľ overovania. Spolu si ujasníme dostupné možnosti aj to, čo bude potrebné pripraviť pred kontrolou.

SoftVea, s.r.o.

info@softvea.com

+421 940 404 737

www.guardvea.com · www.softvea.com

Overte nastavenia. Pochopte zistenia.