BEZPEČNOSTNÍ KONTROLY DATABÁZ S JASNÝM VÝSLEDKEM

GuardVea

Databáze funguje.
Je i bezpečně nastavená?

Ověřte nastavení. Pochopte zjištění.
Rozhodněte, co je třeba napravit.



Od bezpečnostních doporučení
ke konkrétním krokům pro váš tým.

SoftVea, s.r.o.

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

CO PRO VÁS GuardVea MŮŽE UDĚLAT

Mějte jasno v nastavení databází.

Aplikace běží a uživatelé pracují. To ještě neodpovídá na otázku, jak je databáze zabezpečena.



Firma uchovává v databázi objednávky, kontakty či provozní údaje. Správce zná její technickou stránku, vedení se však potřebuje rozhodnout, čemu věnovat čas a peníze. GuardVea pomáhá ověřit vybraná bezpečnostní nastavení a ukázat, která doporučení jsou splněna a která vyžadují pozornost.

Kontrola má konkrétní pravidla

Zvolíte soubor doporučení pro své databázové prostředí. Při jednotlivých kontrolách najdete, co se ověřuje, proč to má význam a jaký výsledek se očekává. Rozhovor o bezpečnosti tak můžete opřít o konkrétní nastavení.

Výsledek pomůže určit další práci

V přehledu se dostanete od databázového serveru ke konkrétní kontrole a jejímu výsledku. Správce může prověřit podrobnosti a doporučený postup nápravy. Vedení získá srozumitelnější podklad pro dohodu o dalších krocích.

> ### Když se vedení ptá na bezpečnost
> Namísto všeobecného ujištění můžete projít vybrané kontroly, jejich výsledky a zjištění, která je ještě třeba řešit.

CO SI V SYSTÉMU PŘIPRAVÍTE

Vaše servery. Rozsah vašeho auditu.

Začněte tím, co potřebujete ověřit a na kterém databázovém prostředí.

Určíte databázové servery

Do objednávky přidáte adresy serverů a podle potřeby je pojmenujete. Máte tak jasno, na které prostředí se kontrola vztahuje. Při přípravě se vyplatí dohodnout i správce, který zajistí připojení a bude umět vysvětlit provozní souvislosti.

Vaše servery

Databáze, které chcete prověřit.

Vaše kontroly

Doporučení a zvolený profil.

Vaše výsledky

Zjištění a podklady k nápravě.

Vyberete vhodná doporučení

CIS benchmark je soubor doporučení pro bezpečné nastavení konkrétní technologie. Vyberete si dostupný soubor, jeho verzi a vhodný profil. Kontrola pak vychází z určeného rozsahu, ke kterému se můžete při čtení výsledků vrátit.

Zohledníte způsob provozu

Databáze na vlastním serveru a spravovaná cloudová služba nabízejí správci odlišné možnosti. Při výběru profilu proto záleží také na tom, ke kterým nastavením máte přístup. Rozsah ověřování má odpovídat tomu, jak databázi používáte.

Pracujte ve svém webovém prohlížeči

Otevřete knihovnu doporučení, připravte objednávku a zkontrolujte výsledky kontroly ve sdíleném pracovním prostoru. Nástroje se otevírají v samostatných oknech nad pracovní plochou s panelem ikon, který umožňuje přístup ke každé sekci.

> **Před kontrolou si ujasněte rozsah**
> Který server prověřujete, podle jaké verze doporučení as jakým profilem? Tyto údaje dávají výsledku potřebný kontext.

JAK KONTROLA FUNGUJE

Od výběru serveru po výsledek.

Jednotlivé kroky na sebe navazují. Vy víte, co připravit a kde hledat zjištění.



01 Definujte rozsah auditu

Určíte databázové servery, dostupný benchmark a profil kontroly. V objednávce si zvolíte položky z ceníku a zkontrolujete údaje.

02 Připravíte připojení

Správce vytvoří určený databázový účet a zajistí potřebný přístup. Ověření připojení pomůže zjistit, zda je možné se serverem komunikovat.

03 Proběhne ověřování

Po úhradě objednávky se spustí bezpečnostní audit. Automatické kontroly ověřují nastavení; při manuálních kontrolách doplníte odpovědi a vyjádření.

04 Projdete zjištění

Prohlédnete si stav, skóre a podrobnosti jednotlivých kontrol. Při zjištěních projdete doporučenou nápravu a dohodnete další kroky se správcem.

> Výsledek má vést k dalšímu kroku
> Důležité je rozumět zjištění, jeho významu pro vaše prostředí i tomu, kdo se bude věnovat případné nápravě.

KNIHOVNA BEZPEČNOSTNÍCH DOPORUČENÍ

Vědět, které požadavky se kontrolují.

Při každém doporučení se můžete podívat na jeho obsah i důvod, proč se mu věnovat.



Benchmark a verze

V knihovně vyberete konkrétní soubor doporučení. Rozlišení verze pomáhá pojmenovat, z jakých podkladů kontrola vychází. Při další práci tak můžete mluvit o stejném rozsahu.

Zkontrolujte popis

Při vybraném doporučení si přečtete, co se má ověřit. Technický název obdrží vysvětlení a správce se snáze zorientuje v tom, jehož nastavení se požadavek týká.

Odůvodnění a dopad

Nestačí vědět, že nastavení je doporučeno. Musíte také pochopit, proč a jak může změna ovlivnit vaše systémy. Tyto informace vám pomohou posoudit doporučení pro vaše prostředí.

Postup ověření a nápravy

Detail může obsahovat kroky auditu, očekávaný výsledek i postup nápravy. Správce má po ruce podklady, které mu pomohou zjištění prověřit a připravit řešení.

> ### Když se kolega ptá, proč to měnit
> Otevřete konkrétní doporučení. Spolu projdete jeho účel, výsledek kontroly i dopad navrhované změny.

VÝBĚR PROFILU

Kontrola podle vašeho prostředí.

Vyberte si dostupný profil, který odpovídá způsobu provozu a požadované přísnosti.



Základní serverový profil

Profil L1_server je určen pro databázový server s přístupem k operačnímu systému. Představuje východisko pro ověření základních doporučení v prostředí, které spravujete.

Cloudový profil

Profil L1_cloud je v objednávce určen pro SQL Server na AWS RDS. Zohledňuje prostředí spravované služby. Při výběru proto vycházejte z konkrétní databázové technologie i způsobu jejího provozu.

Přísnější serverový profil

Profil L2_server rozšiřuje požadavky na přísnější nastavení. Některá doporučení mohou ovlivnit provoz nebo výkon. Před jejich použitím je třeba posoudit, jak se projeví ve vašich aplikacích.

> Například u databáze obchodní aplikace
> Správce spolu s vlastníkem aplikace vybere profil a prověří dopad doporučení. Výsledek pak hodnotíte v dohodnutém rozsahu.

Konkrétní benchmark a dostupné profily si ověříte při přípravě objednávky. Výběr má vycházet z vašeho prostředí.

AUTOMATICKÉ KONTROLY

Ověřte konkrétní nastavení.

Při podporovaných kontrolách získáte výsledek z ověření databáze, ke kterému se můžete vrátit.



Připojení k serveru

Před samotným ověřováním je zapotřebí funkční připojení. V přehledu vidíte, zda se spojení podařilo. Pokud ne, správce má důvod prověřit dostupnost serveru, účet nebo potřebná oprávnění.

Průběh ověřování

Při spuštění kontrol sledujete jejich stav a průběh. Rozlišíte čekání, probíhající zpracování, dokončení i selhání. Víte tak, ať už máte výsledek nebo je třeba se ještě věnovat samotnému běhu.

Výsledek při doporučení

Posuďte každou kontrolu podle toho, co měla ověřit. Jeho skóre a podrobné výsledky pomáhají správci zkontrolovat nález spolu s očekávaným nastavením.

Základ pro informovanou diskusi

Vedení a správce nemusí začínat od obecné otázky, zda je vše v pořádku. Vyberou konkrétní kontrolu, podívají se na její výsledek a určí, co je ještě třeba prověřit.

> ### Když se kontrola nedokončí
> Nejprve prověříte příčinu zpracování. Nedostupný server nebo chyba kontroly potřebují jiný další krok než zjištěné nevyhovující nastavení.

MANUÁLNÍ OVĚŘOVÁNÍ

Něco musí potvrdit člověk.

Tam, kde je třeba znát postupy nebo provozní souvislosti, doplníte odpovědi v dotazníku.



Otázky ohledně doporučení

Manuální kontrola otevře dotazník k vybranému doporučení. Odpovědná osoba odpoví na otázky a může přidat krátké vyjádření. Kontrola tak zachytí i informace, které nelze vyčítat pouze z technického nastavení.

Vyjádření k výsledku

K odpovědím doplníte závěrečné vyjádření o celkovém plnění doporučení. Kolega, který se k výsledku vrátí později, má k dispozici i slovní vysvětlení.

Automatické a ruční kroky se doplňují

Automatické ověření pomáhá při konkrétních nastaveních. Manuální dotazník využije znalost lidí, kteří prostředí spravují. V přehledu jsou tyto typy kontrol rozlišeny, takže víte, jakým způsobem se k výsledku dospělo.

> Například při firemním postupu
> Technický výsledek nemusí vysvětlit, jak tým v praxi postupuje. Odpověď a poznámka odpovědné osoby doplní potřebný kontext.

VÝSLEDKY A PŘEHLED

Od přehledu ke konkrétnímu zjištění.

Nejprve si prohlédnete stav serveru a kontrol. Potom otevřete to, čemu se potřebujete věnovat.



Objednávky a servery

V přehledu vyberete objednávku a její databázové cíle. Máte u sebe rozsah kontroly i informace o jejím průběhu. U více serverů si umíte určit, jehož prostředí se výsledek týká.

Skóre a detail výsledku

Při vybrané kontrole vidíte skóre, stav a report. Skóre slouží k rychlé orientaci. Při rozhodování o dalším postupu jej doplníte čtením zjištění a obsahu doporučení.

Výsledek čtěte v souvislostech

Záleží na profilu, rozsahu kontroly i na tom, jak databázi používáte. Správce umí vysvětlit technické podrobnosti a vlastník aplikace doplnit význam pro provoz. Společně tak určí vhodný další krok.

> ### Na pracovní schůzce
> Vyberete server a otevřete konkrétní kontrolu. Z výsledku přejdete rovnou k otázce, co je třeba prověřit, kdo to vyřídí a kdy se k tomu vrátíte.

DOPORUČENÍ K NÁPRAVĚ

Zjištění je začátek další práce.

Když kontrola ukáže problém, potřebujete rozumět doporučené změně a jejímu dopadu.



U každého doporučení vyhledejte kroky k nápravě

V detailu naleznete část věnovanou nápravě. Správce se může opřít o popsané kroky a porovnat je s aktuálním stavem databáze. Nemusí začínat pouze od stručného označení nevyhovujícího výsledku.

Rozhodujte se s ohledem na vaše provozní prostředí

Doporučenou změnu posuďte spolu s tím, které aplikace databázi používají a co od ní potřebují. Při plánování pomůže znát možný dopad, zodpovědnou osobu a vhodný termín zásahu.

Po změně si ověřte výsledek

Po nápravě zopakujte příslušnou kontrolu a zkontrolujte nový výsledek. To ukazuje, zda nastavení nyní splňuje očekávaný stav nebo stále vyžaduje pozornost.

> ### Když se má měnit důležité nastavení
> Správce posoudí doporučení s vlastníkem aplikace a dohodne se na dalším postupu. Výsledek kontroly poskytuje základ pro tuto práci.

PŘÍPRAVA PŘÍSTUPU

Připojení připraví váš správce.

Před kontrolou si ujasníte potřebný účet, dostupnost serveru a odpovědnost za přípravu.



Určený databázový účet

Objednávka pracuje s databázovým uživatelem guardvea. Správce jej vytvoří na uvedených serverech podle požadavků kontroly. V systému potvrdíte, že je účet připraven.

Pověření pro připojení

Při přípravě objednávky vygenerujete heslo pro určený účet. Správce zajistí jeho nastavení na serverech, které patří do rozsahu. Údaje musí odpovídat připravenému připojení.

Ověření dostupnosti

Před spuštěním je třeba prověřit, zda je možné server dosáhnout a přihlásit se. Stav připojení pomáhá oddělit problém s přípravou přístupu od samotného výsledku bezpečnostní kontroly.

Ukončení přístupu

Součástí objednávky je i potvrzení, že po dokončení auditu bude uživatel guardvea smazán. Dohodněte proto se správcem i tento závěrečný krok.

> ### Příprava má svého člověka
> Určete správce, který připraví účet, prověří spojení a po dokončení auditu zajistí zrušení přístupu.

PRO KOHO JE GuardVea

Každý potřebuje jiný pohled.

Společný výsledek pomáhá spojit technická zjištění s rozhodováním o firemním provozu.



Vedení firmy

Získá konkrétnější podklad pro rozhovor o zabezpečení databází. Umí se ptát na zjištění, potřebnou práci i další postup.

Správce databází

Projde doporučení, výsledky a postupy nápravy při konkrétním prostředí. Má z čeho vycházet při přípravě změn.

Bezpečnostní tým

Pracuje s určeným rozsahem kontroly a jejími výsledky. Při technických zjištěních může navázat na práci správce.

Vlastník aplikace

Doplní, co aplikace od databáze potřebuje. Pomáhá posoudit, jak by se doporučená změna projevila v každodenní práci.

Externí IT partner

Může projít rozsahem validace a přípravou prostředí se společností. Diskuse je založena na konkrétních kontrolách zjištění.

> ### Společný jazyk pro další krok
> Správce vysvětlí zjištění, vlastník aplikace doplní provozní souvislosti a vedení určí čas a zdroje na řešení.

SOUVISLOSTI A VYSVĚTLENÍ

Rozumíte i důvodu kontroly.

Doporučení má svůj účel. Při posuzování výsledku pomůže znát i jeho širší kontext.



Proč se to ověřuje

Odůvodnění při doporučení vysvětluje, proč má dané nastavení význam. Správce může lépe objasnit, proč se zjištění věnovat a co je třeba při rozhodování zvážit.

Co může změna ovlivnit

Část věnovaná dopadu pomáhá při plánování nápravy. Technické doporučení tak můžete číst spolu s tím, jaké požadavky mají aplikace a provoz.

Reference a navazující informace

V detailu jsou k dispozici i reference a vazby na CIS Controls, pokud jejich podklady obsahují. Při potřebě podrobnějšího posouzení máte kam pokračovat.

> ### Když potřebujete doporučení vysvětlit vedení
> Začněte jeho účelem, ukažte výsledek a doplňte možný dopad nápravy. Z technického detailu vznikne podklad pro rozhodnutí.

BĚŽNÁ SITUACE Z PRAXE

Nová aplikace. Nové otázky.

Firma připravuje nasazení aplikace a chce si prověřit nastavení jejího databázového prostředí.



Před kontrolou

Správce určí databázový server a dostupný benchmark. S vlastníkem aplikace vybere profil, připraví potřebný účet a prověří připojení.

Během ověřování

Tým sleduje průběh automatických kontrol. U ručních doporučení odpovědná osoba přidává odpovědi a vysvětluje, jak společnost s požadavkem nakládá.

Při čtení výsledků

Správce otevře zjištění a přejde je s vlastníkem aplikace. Při nevyhovujících nastaveních posoudí doporučenou nápravu a její dopad.

Při plánování další práce

Firma si určí zodpovědnost a termín případných úprav. Po změně může příslušné kontroly zopakovat a ověřit nový stav databáze.

> ### Od otázky k rozhodnutí
> Namísto všeobecné diskuse má tým konkrétní zjištění. Ví, co potřebuje prověřit a na čem se dohodnout před dalším krokem.

CO ZÍSKÁTE ŠEKEM

Jasnější základ pro další kroky vašeho týmu.

Hodnota kontroly je v tom, že pomůže pochopit stav a připravit další práci.



Přehled o ověřeném rozsahu

Můžete určit, které servery a doporučení byly zkontrolovány a který profil byl vybrán. Tento kontext zůstává u výsledků, takže rozsah kontroly je jasný.

Konkrétní zjištění

U jednotlivých doporučení vidíte výsledek a podrobnosti. Správce má podklad pro prověření nastavení a vedení se může ptát na další postup při konkrétních zjištěních.

Informace pro plánování dalších kroků

Popis, odůvodnění, dopad a postup nápravy pomáhají připravit řešení. Výsledek se týká vybraných kontrol; při rozhodování jej hodnotíte spolu s ostatními informacemi o bezpečnosti firmy.

> ### Když kontrola skončí
> Dohodněte, která zjištění prověříte, kdo se jim bude věnovat a jak ověříte výsledek změn. Tak může kontrola pomoci i při další práci.

JAK ZAČÍT

Začněte jedním databázovým prostředím.

Vyberme konkrétní server a otázky, na které potřebujete odpověď. Rozsah připravíme dle vašeho prostředí.

1. Řekněte nám, co provozujete

Připravte si typ a verzi databáze, způsob jejího provozu a stručný popis aplikací, které ji používají. Spolu projdeme, co potřebujete ověřit a kdo se u vás stará o technickou přípravu.

2. Dohodněte se na vhodném rozsahu auditu

Podíváme se na dostupné benchmarky, profily a požadované kontroly. Správce připraví přístup a připojení. Před vytvořením objednávky si přejdete její položky a cenu.

3. Projdete výsledky a další práci

Po provedení kontroly se podíváte na zjištění i doporučení. S tímem určíte, která nastavení je třeba prověřit a jaké změny připravit. Podle výsledku můžete pokračovat dalšími databázemi.

Vaše prostředí

Typ a verze databáze · Způsob provozu

Rozsah kontroly

Databázové servery · Benchmark · Profil

Další postup

Výsledky · Posouzení zjištění · Náprava

Máte konkrétní požadavky?

Popište své databázové prostředí a cíl ověřování. Projdeme s vámi dostupnost vhodných kontrol i potřebnou přípravu. Už na začátku tak bude jasnější, co má být výsledkem.

> **Na první rozhovor stačí konkrétní příklad**
> Například databáze vaší hlavní aplikace, její verze a způsob provozu. Na tom si ukážeme vhodný další postup.

KONTAKTUJTE SE

Podívejme se na vaše databáze.

Rádi s vámi projdeme, co potřebujete ověřit a jak vám při tom může pomoci GuardVea.



Každé prostředí má své požadavky. Někdo připravuje novou aplikaci, jiný chce prověřit stávající server nebo získat podklad pro bezpečnostní úpravy. Začněme tím, co je důležité pro vaši firmu.

Dohodněte se na rozsahu vaší první kontroly

Napište nám nebo zavolejte. Projdeme typ databáze, způsob provozu a cíl ověřování. Spolu si ujasníme dostupné možnosti i to, co bude třeba připravit před kontrolou.

SoftVea, s.r.o.

info@softvea.com

+421 940 404 737

www.guardvea.com · www.softvea.com

Ověřte nastavení. Pochopte zjištění.