Intelligently Automate SQL Server

DB24LIVE

KommITS

När ni har ett intrång – Vad önskar du då att du redan gjort?_

Så skyddar du din dataplattform innan det är för sent

Ett urval av de kommuner som vi arbetar med idag

När du har ett intrång – vad önskar du att du redan gjort?_

”Går systemet ner är det en fråga om rikets säkerhet”_

MSB har tydligt metodstöd och konsekvenserna när data läcker är allvarliga.

Konsekvensnivåer

Värdering	Invånare/medarbetare	Avbrott i verksamheten	Ekonomisk skada	Minskat förtroende
4. Allvarlig	Allvarlig påverkan för medarbete, invånare eller brukare. Individers liv och hälsa kan äventyras.	Allvarlig påverkan på verksamheters förmåga, omöjligt eller nästan omöjligt att fullfölja uppdragen.	Mycket stor ekonomiska skada. 2 miljoner kronor och uppåt eller avvikelse på 15% av budget.	Förtroendet för kommunen är negativt påverkat i allvarlig grad. Ihållande drev i rikstäckande medier eller av organiserade grupperingar i sociala medier.
3. Betydande	Större påverkan för medarbete, invånare eller brukare. Enskilda individer kan uppleva konsekvenser, såsom stora besvär.	Verksamheten kan fullfölja sina uppdrag men med trolig risk för kännbar påverkan exempelvis genom att behöva vidta extraordinära åtgärder.	Stor ekonomiska skada. 500 000 – 2 miljoner kronor eller avvikelse på 10–15% av budget.	Förtroendet för kommunen är negativt påverkat i hög grad. Nyheter i både riks- och lokalmedia men begränsat till enskilda händelser eller enskilda individers agerande.
2. Måttlig	Viss påverkan för medarbete, invånare eller brukare. Enskilda individer kan notera störningen eller uppleva lindriga besvär.	Viss påverkan på verksamheters förmåga, inga större svårigheter att fullfölja uppdragen.	Viss ekonomisk skada. 1 – 500 000 kronor eller avvikelse på 5–10% av budget.	Förtroendet för kommunen är negativt påverkat till liten grad. Enstaka missnöjda individer uttalar sig i sociala medier eller lokalmedia.
1. Försumbar	Ingen eller försumbar påverkan för me	Obetydlig påverkan på verksamheters	Ingen märkbar ekonomisk skada	Liten negativ uppmärksamhet

Sannolikhetsnivåer

Värdering	Beskrivning/kriterier
4. Sannolik	Har inträffat förr, förväntas hända inom 12 månader.
3. Möjlig	Finns flera kända fall, förväntas hända inom fem år.
2. Mindre sannolik	Finns kända fall, kan hända inom fem år.
1. Osannolik	Har aldrig hänt förr, förväntas inte hända inom överskådlig framtid.

Summering: Vad står på spel? _

Kort om mig _

Andreas Evander

Partner/Founder DB24

DB24 CEO & Stategic Lead
Data- & säkerhetsnörd med förkärlek för verkliga problem
Föreläsare, rådgivare & orädd SQL-evangelist
Tidigare drifttekniker som fortfarande gillar att skruva på saker
SQL User Group Board Member
50+ Kommuner kör DB24 programvaran

En nörd i kostym – som hjälper Sveriges kommuner att sova lite tryggare om nätterna.

(Fortfarande med drömmen om att äga en grävmaskin.)

Hur kan detta hända? _
Vi saknar data över vårt data…

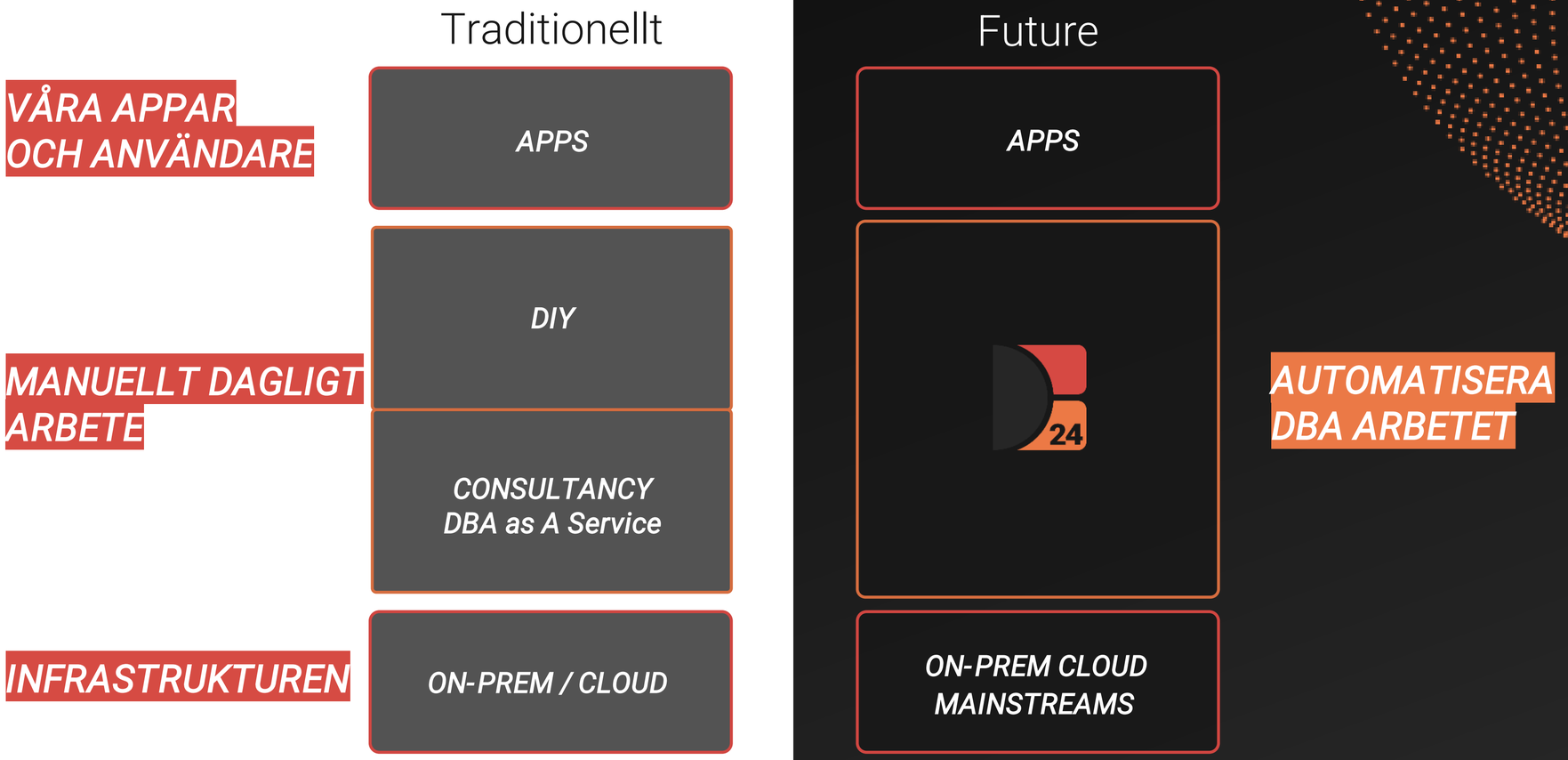
- Har vi audit på dataplattformen,
- Nej vi kan ta fram info om någon vill ha den

- Har vi antivirus
- Nej vi kan installera strax innan någon tänker attackera oss

0% **av de 354 organisationer som DB24 träffade under 2024 hade ett CMDB över sin mest värdefulla asset, sin data.**

0% **hade spårning av förändringar i dataplattformen**

Traditionella lösningar fungerar inte längre



Det är databasen som är Er akilleshäl! _

När en dataläcka inträffar, vad är det som går fel? _

MITRE | ATT&CK®

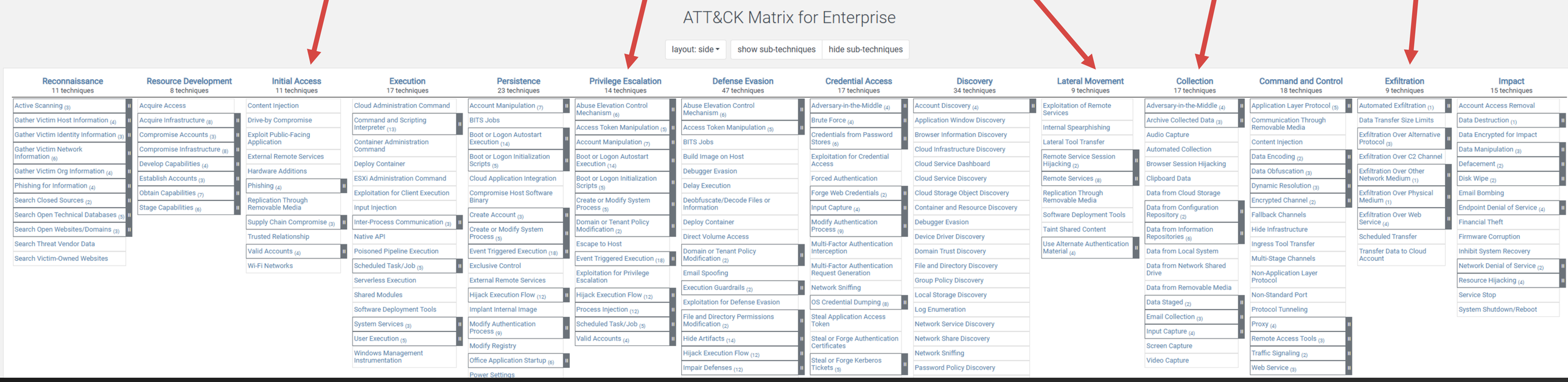
Här är Era system en guldgruva pga höga behörigheter i många led

Här är dataplattformarna utsatta, det saknas nästan alltid lösenordspolicies för SQL konton ”sommar1” är absolut gångbart lösenord

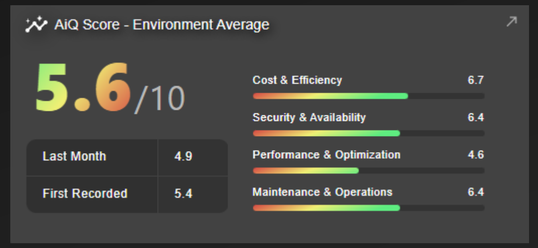
Här börjar det blir väldigt enkelt, ofta eftersatt livscykling, ofta dåligt säkrade test system.

Nu är det som att stjäla godis ifrån barn, oskyddat och okrypterat. Sannolikt hittas en backup som ligger och skräpar så coola data extraction script behövs inte ens

Sista steget är att via TOR network ladda upp databasbackuper, ingen audit fanns på plats så ingen kommer dessutom upptäcka vad som gjorts.



Summering, varför är våra dataplattformar så utsatta och eftersatta _



~~*När du har ett intrång…*~~
~~*= vad önskar du att du redan gjort?*~~ _

- *Vad skall vi hem och göra direkt för att minimera påverkan av ett intrång*

En plan att införa i sju steg _

1. Börja med inventering, skapa ett databas över era databaser.

En plan att införa i sju steg _

2. *Delegera ut ägarskap över system och databaser, både tekniskt och verksamhetsmässigt.*

En plan att införa i sju steg _

3. *När inventeringen är klar, se över livscykelhantering så att allt är patchat och up-to-date*

En plan att införa i sju steg _

4. *Se över konfiguration och åtgärda felaktigheter*

En plan att införa i sju steg _

5. Ifrågasätt alla högre behörigheter kring er dataplattform

En plan att införa i sju steg _

6. *Implementera en standardiserat databasunderhåll*

En plan att införa i sju steg _

7. *Sist och störtinsats, Inför kryptering på bred front, både av data i vila samt data i transit.*

Summering _

1. Börja med inventering, skapa ett databas över ert data.
2. Delegera ut ägarskap över system och databaser, både tekniskt och verksamhetsmässigt.
3. När inventeringen är klar, se över livscykelhantering så att allt är patchat och up-to-date.
4. Se över konfiguration och åtgärda felaktigheter
5. Ifrågasätt alla högre behörigheter kring er dataplattform
6. Implementera en standardiserat databasunderhåll
7. Inför kryptering på bred front, både av data i vila samt data i transit.

Det är inte Rocketscience!_

Punkt 1-6 kan man införa på minde än 4 veckor
Några exempel på kommuner och förbund som gjort det i närtid, och som gör det väligt bra!

Punkt 7 – Kryptering är betydligt mer komplicerat men även väldigt viktigt, Soltak AB på västkusten är med sina ägarkommuner väldigt långt framme och är en förebild för hur kommunal dataplattformsdrift skall göras.

Frågor att ställa till Era organisationer:

Har vi koll på vår (näst)viktigaste tillgång, vårt data _

Vad har vi för data?

Vem ändrar?

Vem ansluter

Vilka risker finns

Vem äger riskerna

Avslutningsvis frågestund _

Jag connectar gärna på Linkedin!

https://www.linkedin.com/in/andreas-evander-db24/

"Soltak AB has used DB24 for a couple of years now and the service has truly exceeded the value we were hoping for and has evolved even more.

Daniel Bjurström,
CIO at Soltak AB

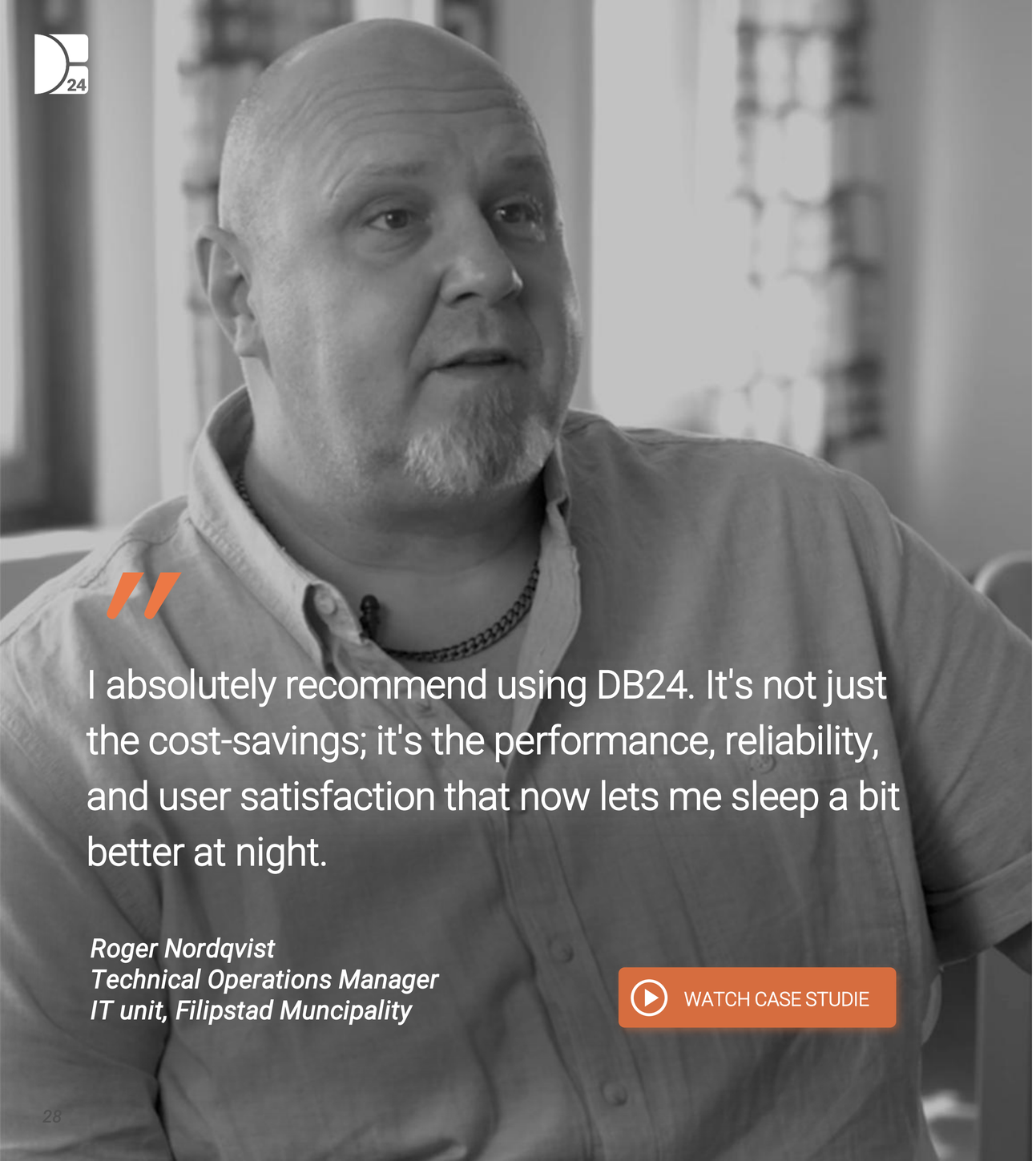
soltak ab

Soltak Modernizing Municipal IT Solutions Together with DB24_

100%

Uptime since 2019

Through DB24, Soltak AB met higher demands of availability, assuring uninterrupted service and heightened efficiency.



"I absolutely recommend using DB24. It's not just the cost-savings; it's the performance, reliability, and user satisfaction that now lets me sleep a bit better at night.

Roger Nordqvist
Technical Operations Manager
IT unit, Filipstad Muncipality

WATCH CASE STUDIE

FILIPSTADS KOMMUN

Filipstad Municipality Amplifies Efficiency and Reduces Costs with DB24_

80%

Reduction in Servers

Server consolidation reduced the database server count from 20 to just 4, enhancing resource utilization.

"I would recommend all companies that are using MS SQL Server for their Business-Critical Applications to look at what DB24 have to offer.

Stefan Lindström,
Key Account Manager at Shibuya

Shibuya
PART OF PULSEN

Shibuya Optimizes their SQL Server Environments with DB24_

Time to complete workload reduced by more than

50%