Kako uskladiti razvoj softvera s <NIS2 i DORA>

Sponsored by

embarcadero

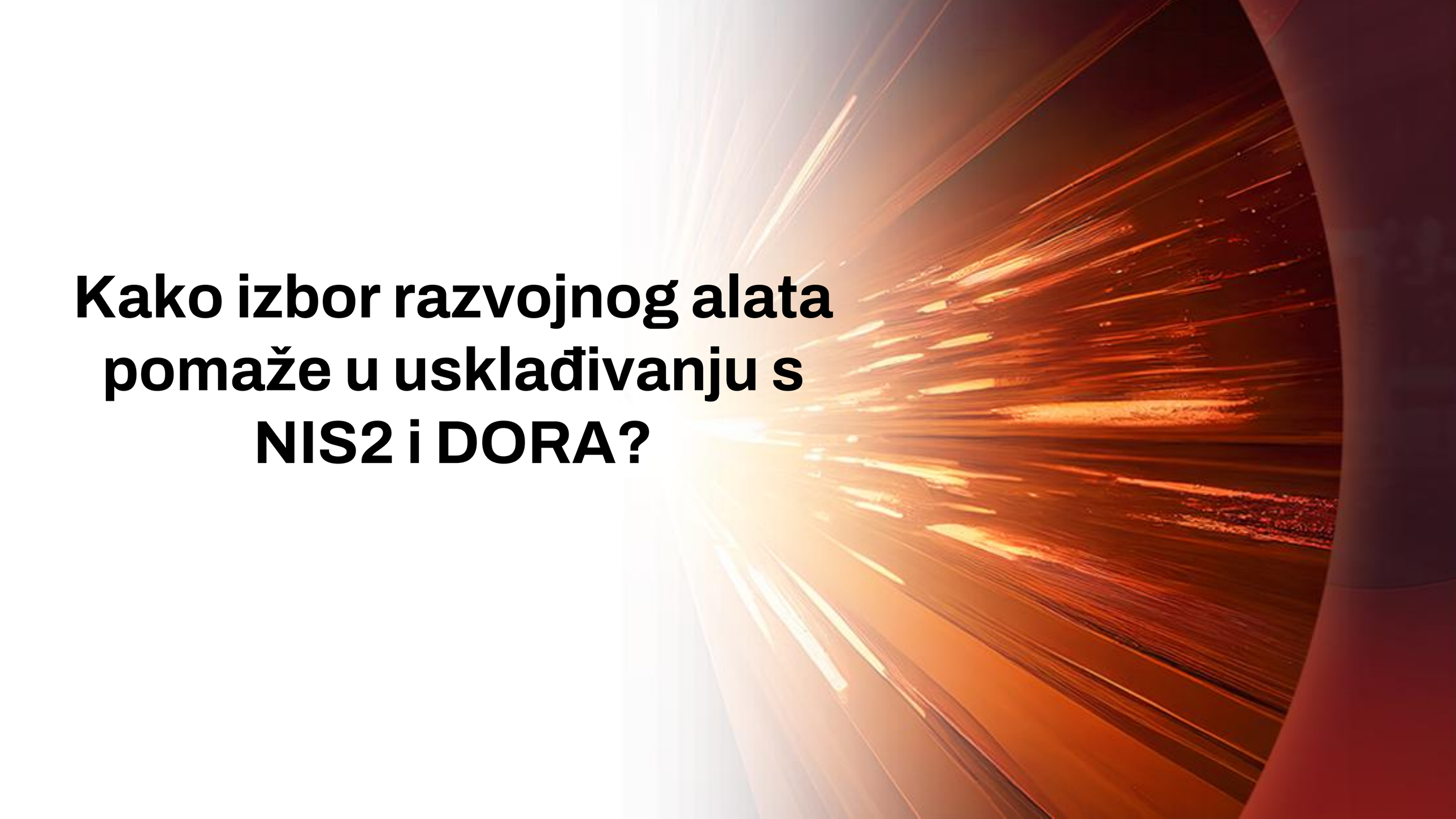
Mladen Kuzminski, mag.inf.

- 25+ godina iskustva u projektiranju informacijskih sustava
- Voditelj predstavništva Embarcadero / IDERA / Sencha / Yellowfin / PreEmptive / Kiuwan za Adriatik - Balkan
- IRCA Lead auditor za ISO 27001
- Autor 14 stručnih knjiga i udžbenika
- https://www.linkedin.com/in/mladen/

KONTO d.o.o. Požega, Varaždin

- Osnovano 1993. Razvoj poslovnih aplikacija.
- ISO 9001, ISO 27001, ISO15489, aAa bonitet
- Distributer Embarcadero / IDERA / Sencha / Yellowfin / PreEmptive / Kiuwan / DerScanner za Adriatik - Balkan
- www.konto.hr

Kako izbor razvojnog alata pomaže u usklađivanju s NIS2 i DORA?



Važne karakteristike

1. **Sigurnost Koda**: Razvojni alati koji pružaju funkcije za statičku i dinamičku analizu koda mogu pomoći u otkrivanju sigurnosnih ranjivosti i osiguravanju da je kod siguran.
2. **Učinkovitost Razvoja**: Alati koji omogućuju brzu i efikasnu izradu aplikacija smanjuju potencijal za ljudske greške i osiguravaju konzistentnost kroz automatizaciju procesa.
3. **Integracija s Drugim Alatima**: Razvojni alati trebaju dobro surađivati s alatima za upravljanje projektima, praćenje verzija i alate za kontinuiranu integraciju (CI/CD), koji su ključni za održavanje visokih standarda sigurnosti i otpornosti.
4. **Podrška za Više Platformi**: Razvojni alati koji omogućuju razvoj aplikacija za različite platforme osiguravaju širinu pokrivenosti i testiranja, čime povećavaju otpornost sustava.
5. **Native razvoj**: Elimiraju se međuslojevi koji mogu biti izvor rizika.

Komercijalni vs OpenSource alati?

Komercijalni vendor: Shared responsibility
- Vendor je odgovoran za security alata
- SLA ugovori
- Support team za security incidente
- Liability insurance
- Možete ih tužiti ako zabrljaju

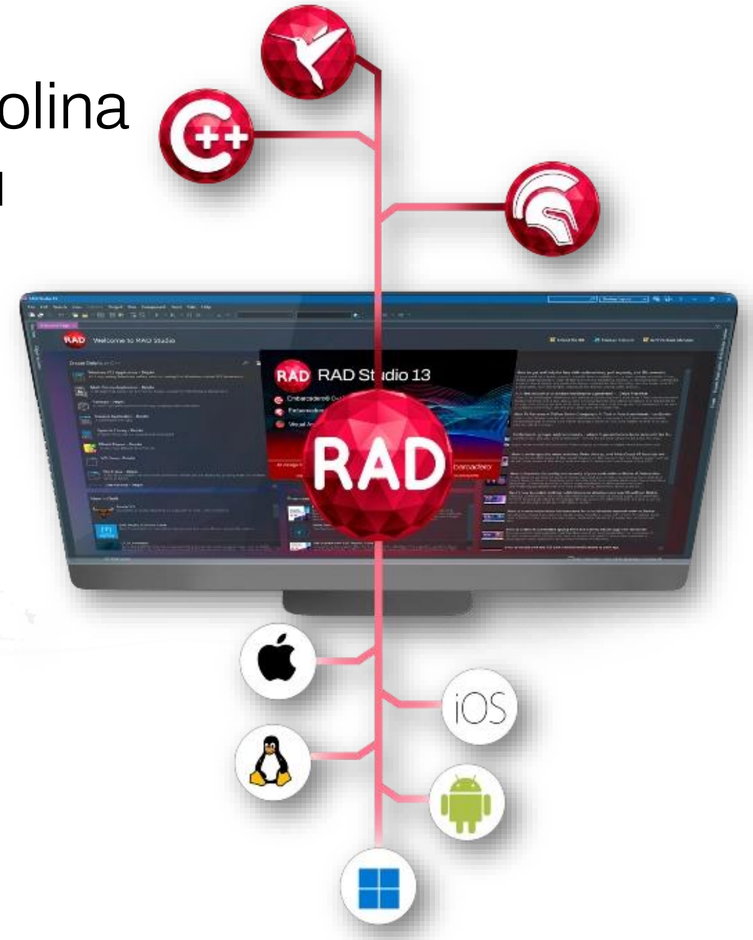
Open source:
- VI ste 100% odgovorni
- "As-is" licence (no warranties)
- Community nema liability
- Ako je ranjivost u alatu, to je VAŠ problem

NIS2 implikacija:
- Sva odgovornost pada na vas
- Morate imati interno stručnjake
- Morate proaktivno pratiti security

Embarcadero RAD Studio

Embarcadero RAD Studio i Usklađenost s NIS2 i DORA

Embarcadero RAD Studio je moćna razvojna okolina koja programerima pruža niz alata za brzu izradu visokokvalitetnih aplikacija za različite platforme.



https://www.embarcadero.com/

Embarcadero RAD Studio i usklađenost s NIS2 i DORA

- **Sigurnost Koda i Analiza**: RAD Studio uključuje alat za statičku analizu koda koji pomaže developerima identificirati i ispraviti slabosti u sigurnosti aplikacija. Bildanje i debagiranje omogućuju kontrolu koda u realnom vremenu, smanjujući rizik od implementacije nesigurnog koda.
- **Učinkovitost i Automatizacija**: Komponente za vizualno razvojno okruženje i drag-and-drop sučelja ubrzavaju razvojni proces i smanjuju prostor za greške. Integracija s popularnim alatima za kontrolu verzija poput Git-a osigurava kontinuirano praćenje promjena i omogućuje brz povratak na prijašnje verzije koda.
- **Integracija CI/CD**: RAD Studio se lako integrira s CI/CD alatima, kao što su Jenkins, TeamCity i drugi, omogućujući automatizirano testiranje i implementaciju, čime se osigurava visok nivo kvalitete i sigurnosti kroz cijeli razvojni ciklus.

https://www.embarcadero.com/

Embarcadero RAD Studio i usklađenost s NIS2 i DORA

- **Podrška za Više Platformi**: Omogućavajući izradu aplikacija za više operativnih sustava, uključujući Windows, macOS, Linux, iOS i Android, RAD Studio osigurava da aplikacije dosljedno rade u različitim okruženjima, što je ključno za procjene otpornosti.
- **Dokumentacija i Planiranje Kontinuiteta**: RAD Studio pruža opsežnu dokumentaciju i podršku za razvojne prakse koje osiguravaju da sustavi ostanu operativni čak i u slučaju kibernetičkih napada ili drugih digitalnih smetnji.
- **Korištenje AI**: Korištenje AI u pisanju, optimizaciji I dokumentiranju koda, a također mogućnost korištenja AI sustava u gotovoj korisničkoj aplikaciji.

https://www.embarcadero.com/

Važnost sigurnosnog audita izvornog koda

Zašto je važan sigurnosni audit source koda?

1. **Identifikacija Ranjivosti:** Otkrivanje sigurnosnih propusta, poput SQL injekcija, XSS (cross-site scripting) napada i drugih, omogućava programerima da poduzmu odgovarajuće mjere za zaštitu aplikacija.
2. **Usklađenost s Regulativama:** Osiguranje da aplikacije zadovoljavaju sigurnosne standarde postavljene od strane regulativa NIS2 i DORA, pomaže u sprječavanju incidenata koji bi mogli uzrokovati regulatorne sankcije.
3. **Poboljšanje Kvalitete Koda:** Sigurnosni audit ne samo da otkriva sigurnosne propuste, već također pomaže u poboljšanju opće kvalitete koda kroz identifikaciju najboljih praksi za programiranje.
4. **Proaktivna Sigurnost:** Rano otkrivanje i rješavanje sigurnosnih ranjivosti smanjuje rizik od kibernetičkih napada, štiteći organizaciju od potencijalnih financijskih i reputacijskih šteta.
5. **Software Bill of Materials (SBOM)** Popis svih komponenti unutar softvera — uključujući open source pakete i ovisnosti.

DerScanner

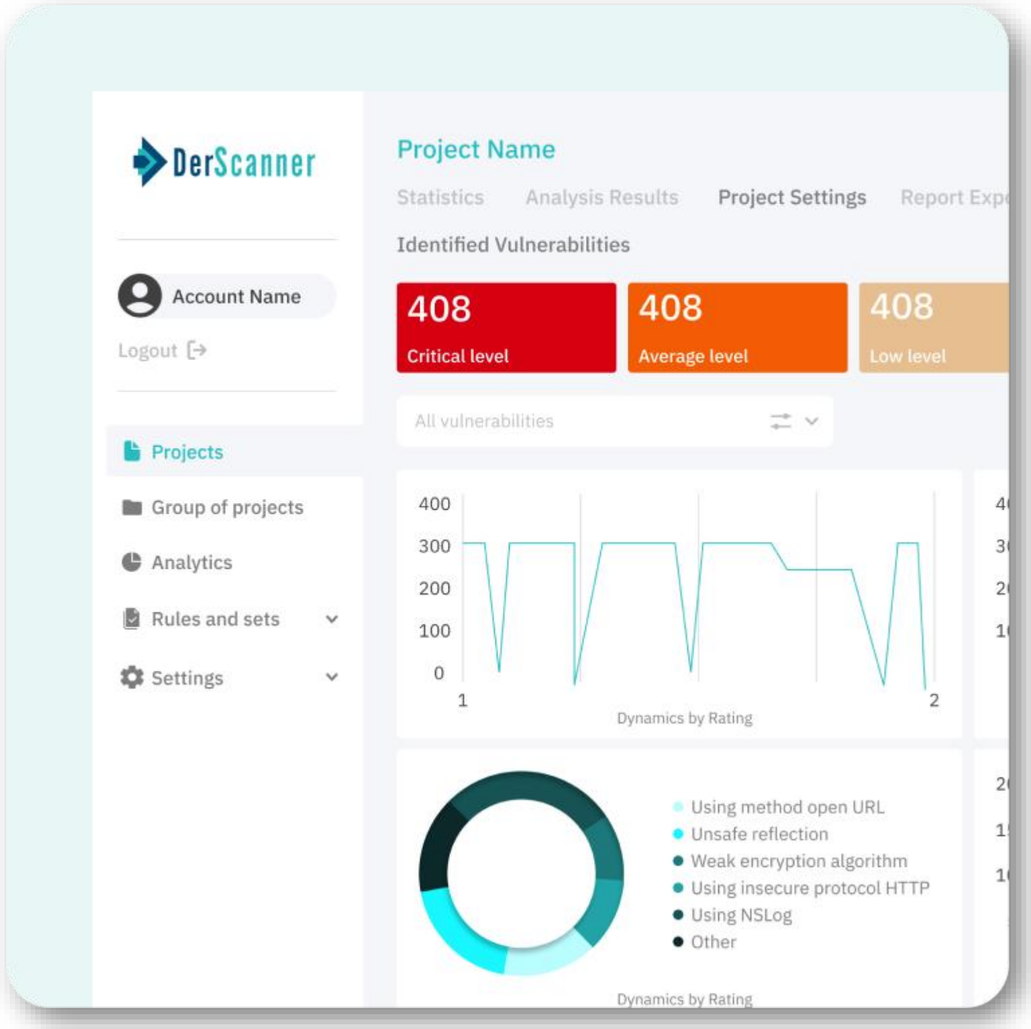
Sigurnosna analiza koda i SBOM za moderne razvojne timove

Što je DerScanner?

- **Opis:** DerScanner je napredna platforma za testiranje sigurnosti aplikacija (AST) koja kombinira više metoda analize u jednom sučelju.

- **Ključne komponente:**
  - **SAST (Static Analysis):** Analiza izvornog koda bez pokretanja aplikacije.
  - **DAST (Dynamic Analysis):** Testiranje aplikacije u radu (runtime).
  - **SCA (Software Composition Analysis):** Analiza open-source komponenti i biblioteka.

- **Cilj:** Identifikacija ranjivosti i "backdoor" prijetnji u ranoj fazi razvoja.

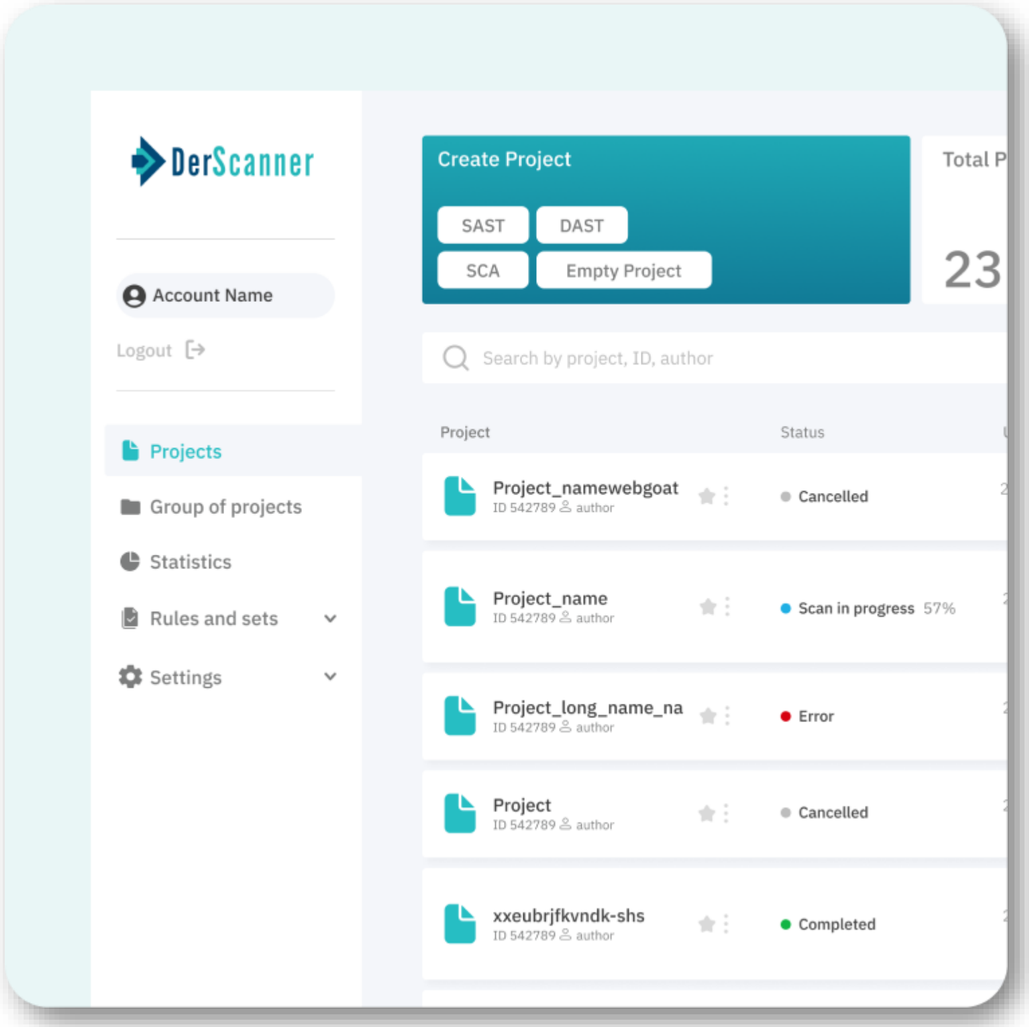


https://derscanner.com/

Ključne mogućnosti

- **DerScanner omogućuje:**
  - Otkrivanje ranjivosti u izvornom kodu
  - Analizu aplikacija bez izvornog koda
  - Analiza kvalitete napisanog koda
  - Integraciju s Jenkins, GitLab, Azure DevOps i drugima
  - Generiranje jasnih izvještaja i preporuka

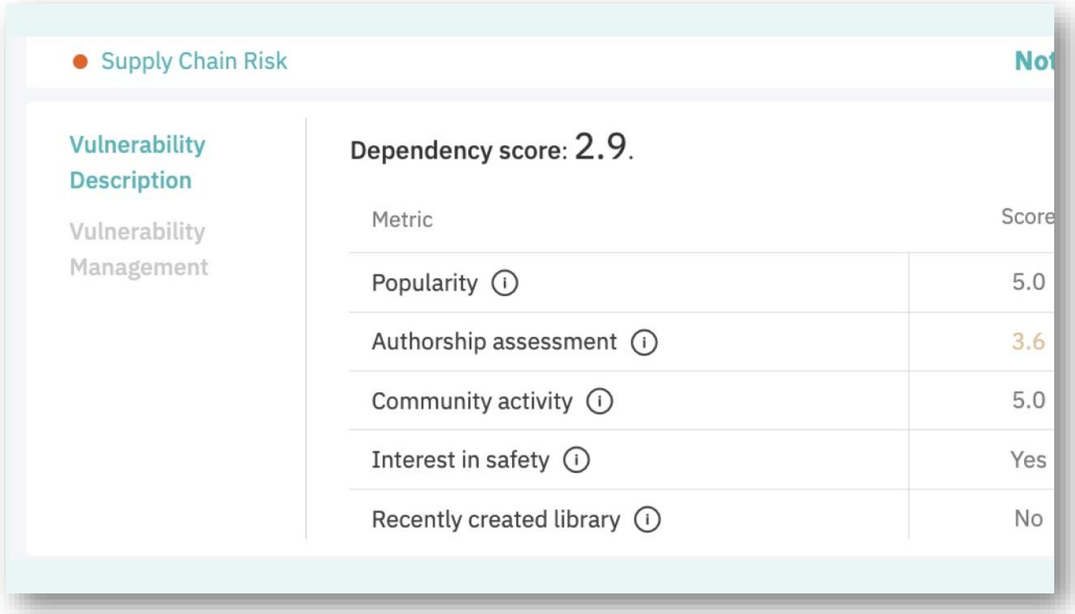
- **Zašto ga koristiti?**
  - Rano otkrivanje sigurnosnih problema
  - Smanjenje troškova ispravaka
  - Ubrzavanje razvoja uklanjanjem ručnih provjera
  - Povećanje kvalitete i stabilnosti aplikacija
  - Lakše ispunjavanje sigurnosnih standarda



https://derscanner.com/

Izazov modernog razvoja: SBOM

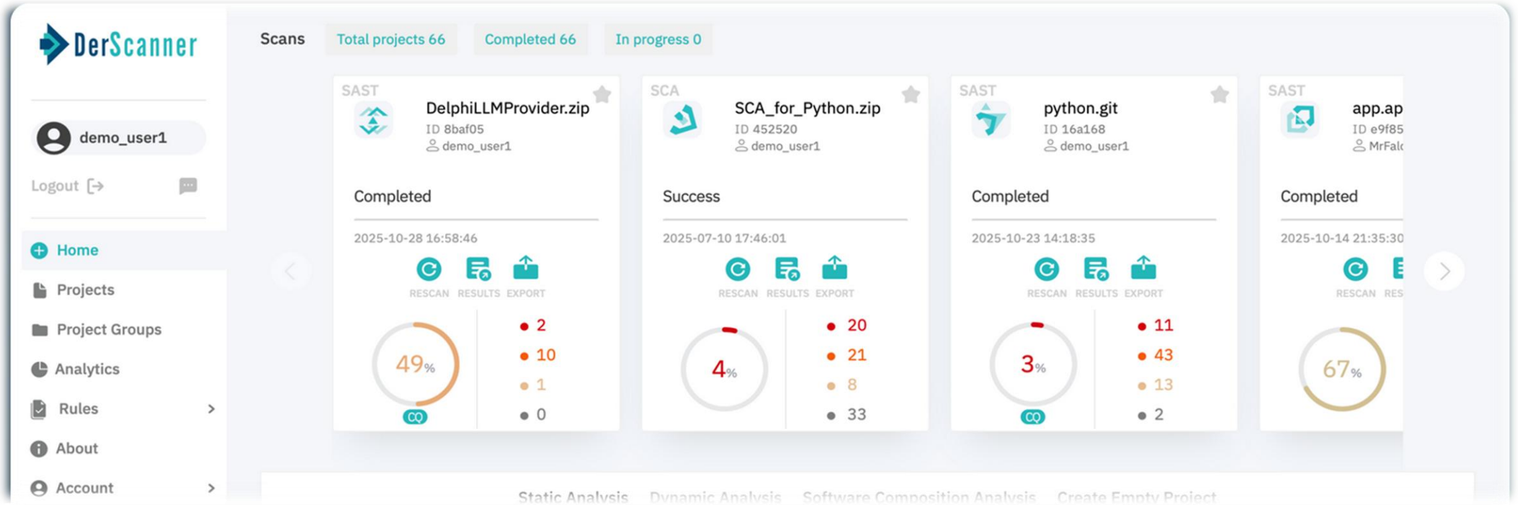
- **Što je SBOM (Software Bill of Materials)?** Digitalni "popis sastojaka" svakog softverskog paketa.
- **Zašto je kritičan?** Moderni softver se sastoji od 60-90% open-source komponenti.
- **Rizici:** Napadi na lanac opskrbe (Supply Chain Attacks), poput Log4j incidenta, pokazali su da organizacije često ne znaju što se točno nalazi u njihovom kodu.
- **Sve veći zakonski zahtjevi** (npr. EU Cyber Resilience Act) traže SBOM za transparentnost i sigurnost.



https://derscanner.com/

DerScanner i SBOM: Potpuna vidljivost

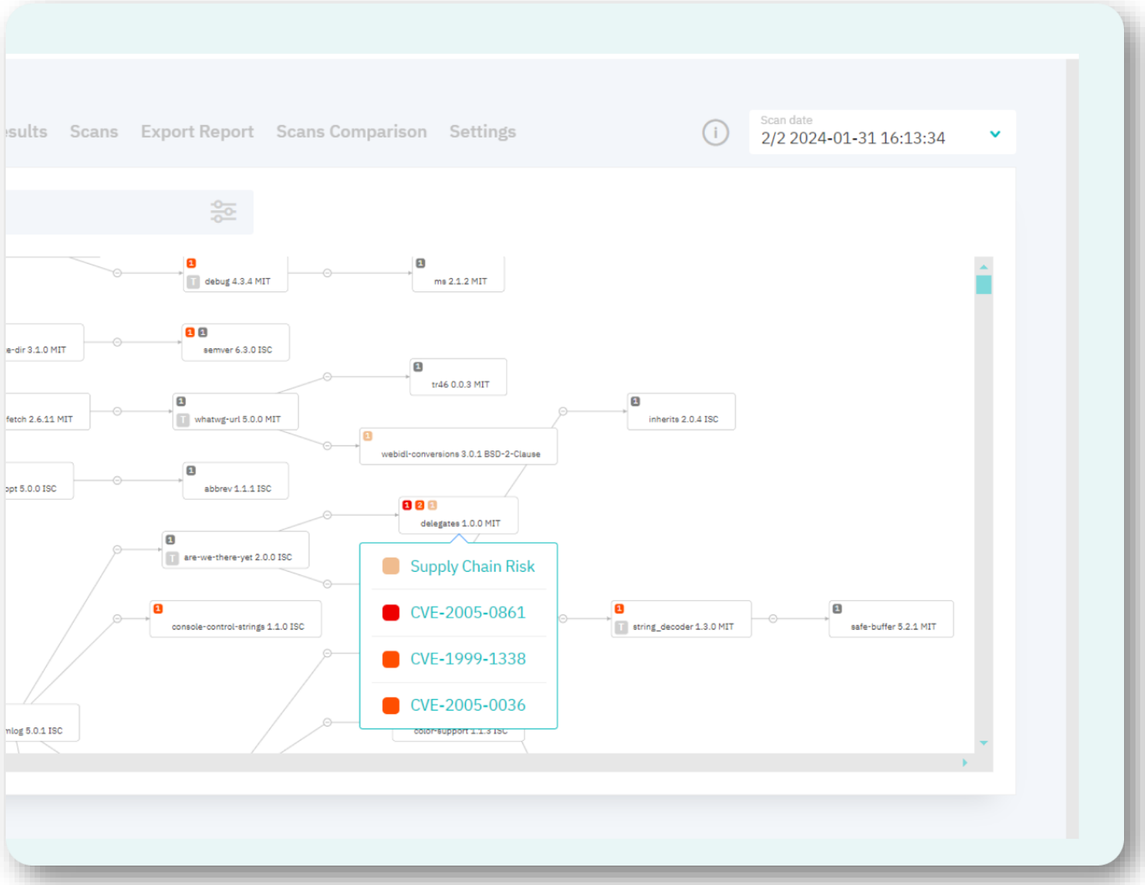
- **Automatsko generiranje:** DerScanner automatski kreira SBOM u standardnim formatima (npr. CycloneDX, SPDX).
- **Identifikacija skrivenih ovisnosti:** Alat mapira ne samo izravne, već i tranzitivne ovisnosti (ono što vaše biblioteke same povlače).
- **Kontinuirano praćenje:** Čim se pojavi nova ranjivost u nekoj komponenti, DerScanner vas obavještava, čak i ako se kod nije mijenjao.



https://derscanner.com/

Ključni benefiti za organizaciju

- **Smanjenje poslovnog rizika:** Brza identifikacija i krpanje kritičnih propusta prije nego što dođu do produkcije.
- **Usklađenost (Compliance):** Ispunjavanje regulatornih zahtjeva (poput EU Cyber Resilience Act) koji sve češće zahtijevaju dostavu SBOM-a.
- **Ušteda vremena i novca:** "Shift Left" pristup – ispravljanje grešaka u fazi razvoja je do 100 puta jeftinije nego nakon instalacije aplikacije.



https://derscanner.com/

Integracija u CI/CD proces

- **Automatizacija:** DerScanner se integrira izravno u vaše razvojne alate (GitLab, GitHub, Jenkins, Azure DevOps).
- **Kvaliteta bez usporavanja:** Automatski "Security Gates" sprječavaju deploy koda koji ne zadovoljava sigurnosne standarde.
- **Podrška za jezike:** Podržava **43 programska jezika**, što ga čini idealnim za heterogena IT okruženja.

https://derscanner.com/

Zašto odabrati DerScanner u odnosu na konkurenciju?

- **Niska stopa lažno pozitivnih rezultata:** Napredni algoritmi osiguravaju da programeri troše vrijeme na stvarne prijetnje, a ne na šum.
- **Analiza bez izvornog koda:** Jedinstvena sposobnost analize binarnih datoteka i izvršnog koda kada izvorni kod nije dostupan.
- **Lokalna ili Cloud instalacija:** Prilagodljivost potrebama organizacije (On-premise za maksimalnu privatnost ili SaaS za brzinu).
- Analitičari poput **Gartnera** i **Forrestera** prate DerScanner unutar tržišta alata za testiranje sigurnosti aplikacija i prepoznat je kao snažan izazivač s nekoliko specifičnih prednosti:
  - Širina podrške za programske jezike (43)
  - Analiza binarnog koda (Binary Analysis)
  - Hibridni pristup (SAST + DAST + SCA)
  - Na platformama poput Gartner Peer Insights, korisnici DerScanner ocjenjuju visokim ocjenama (često 4.5 - 5.0 zvjezdica).

https://derscanner.com/

Kiuwan

Analiza Statike Koda (Static Code Analysis):

- **Otkrivanje Ranjivosti:** Kiuwan koristi napredne alate za statičku analizu koda kako bi identificirao sigurnosne ranjivosti unutar koda. Automatizirano skeniranje omogućuje brzo i temeljito otkrivanje problema prije nego što aplikacija bude implementirana.
- **Provjera Sigurnosnih Standarda:** Implementacija provjerenih sigurnosnih standarda kao što su OWASP, CWE (Common Weakness Enumeration), i SANS Top 25, pomaže organizacijama da zadovolje najbolje industrijske prakse.

https://www.kiuwan.com/

Upravljanje Rizicima:

- **Procjena Rizika:** Kiuwan omogućuje procjenu rizika povezanih s otkrivenim ranjivostima, pomažući timovima da prioritiziraju rješavanje najozbiljnijih prijetnji.
- **Praćenje Sigurnosti:** Platforma omogućava kontinuirano praćenje sigurnosnih prijetnji i ranjivosti kroz cijeli razvojni ciklus aplikacije.

https://www.kiuwan.com/

Automatizacija i Integracija:

- **CI/CD Integracija:** Kiuwan se jednostavno integrira s kontinuiranim integracijskim i kontinuiranim vrstama implementacijskih (CI/CD) alatima poput Jenkins, Azure DevOps, i drugih, omogućavajući automatizirana sigurnosna skeniranja tijekom cijelog razvojnog procesa.
- **Automatsko Izvještavanje:** Pruža detaljne izvještaje o sigurnosnim prijetnjama koje su jednostavno razumljive i koje omogućavaju brzo ispravljanje otkrivenih problema.

https://www.kiuwan.com/

Usklađenost s Regulativama:

1. **Audit Zapisi:** Kiuwan omogućava vođenje detaljnih audit zapisa koji dokumentiraju sve provjere i otkrivene prijetnje, što je ključno za dokazivanje usklađenosti s NIS2 i DORA regulativama.
2. **Sigurnosne Provjere:** Implementacija sigurnosnih politika koje su specifične za NIS2 i DORA zahtjeve osigurava usklađenost aplikacija s regulatornim standardima.

https://www.kiuwan.com/

Sigurnost baze podataka

InterBase baza podataka

Sigurno spremanje podataka uz InterBase

- **Upravljanje Rizicima**
  - **Šifriranje Podataka**: InterBase koristi napredne metode šifriranja, uključujući AES (Advanced Encryption Standard), za zaštitu podataka u mirovanju i prijenosu. Ovim se osigurava povjerljivost i integritet podataka.
  - **Kontrola Pristupa**: InterBase pruža naprednu kontrolu pristupa temeljenu na ulogama (RBAC), omogućavajući administratorima da definiraju i dodijele specifične razine pristupa korisnicima, čime se smanjuje rizik od neovlaštenih pristupa.

https://www.embarcadero.com/products/interbase

IoTA
INTERNET OF THINGS AWARDS
WINNER

Sigurno spremanje podataka uz InterBase

- **Prijava Incidenata i Upravljanje Incidentima**
  - **Auditi i Praćenje Aktivnosti**: InterBase nudi sveobuhvatno praćenje korisničkih aktivnosti i vođenje audit zapisa, omogućujući brzo otkrivanje i reakciju na sumnjive aktivnosti i potencijalna narušavanja sigurnosti.
  - **Automatske Notifikacije**: Implementacija automatskih notifikacija za administratore i sigurnosni tim pomaže u brzom odgovoru na sigurnosne incidente.

https://www.embarcadero.com/products/interbase

IoTA
INTERNET OF THINGS AWARDS
WINNER

Sigurno spremanje podataka uz InterBase

- **Jednostavnost I niska cijena implementacije**
  - **Efikasnost Resursa**: InterBase je poznat po svojoj laganoj arhitekturi visoke performanse, što smanjuje potrebu za skupocjenom infrastrukturom i resursima. Organizacije mogu ostvariti visoke nivoe sigurnosti i otpornosti bez velikih troškova.
  - **Skalabilnost i Fleksibilnost**: InterBase može pratiti rast poslovanja i povećanje podatkovnih potreba, omogućujući efikasno upravljanje resursima u skladu s regulativama.

https://www.embarcadero.com/products/interbase

IoTA
INTERNET OF THINGS AWARDS
WINNER

Sigurno spremanje podataka uz InterBase

- **Backup**
  - **Sigurnosne Kopije i Oporavak**: InterBase uključuje ugrađene alate za sigurnosne kopije i oporavak podataka, osiguravajući kontinuitet poslovanja čak i u slučaju kvara ili sigurnosnih incidenata.
  - **Redundancija i Replikacija Podataka**: Replikacija podataka omogućuje da se ključne informacije automatski sinkroniziraju i pohranjuju na različitim lokacijama, čime se osigurava stalna dostupnost i otpornost sustava.

https://www.embarcadero.com/products/interbase

IoTA
INTERNET OF THINGS AWARDS
WINNER

Sigurno spremanje podataka uz InterBase

1. **Zaštita Podataka i Sigurnosno Upravljanje Podacima**
   1. **Mobilna Sigurnost**: InterBase ToGo osigurava sigurnost podataka na mobilnim uređajima pomoću šifriranja i autentičnosti, čuvajući podatke sigurnima čak i kad se koriste na pokretnim platformama.
   2. **Sigurnosno Upravljanje Aplikacijama**: Softverski razvojni paketi (SDK-ovi) omogućavaju developerima jednostavnu integraciju sigurnosnih značajki InterBase-a, osiguravajući da aplikacije koje koriste bazu podataka zadovoljavaju visoke standarde sigurnosti.

https://www.embarcadero.com/products/interbase

IoTA
INTERNET OF THINGS AWARDS
WINNER

Sigurnosni audit baze podataka

NIS2 Direktiva:

1. **Upravljanje Rizicima:** Implementacija mjera za identifikaciju i upravljanje rizicima vezanim za sigurnost mrežnih i informacijskih sustava.
2. **Prijava Incidenata:** Obavezno prijavljivanje značajnih sigurnosnih incidenata odgovarajućim tijelima.
3. **Zaštita Podataka:** Osiguranje povjerljivosti, cjelovitosti i dostupnosti podataka.

DORA Regulativa:

1. **Sigurnosno Upravljanje Podacima:** Implementacija sigurnosnih tehnika kao što su šifriranje i kontrola pristupa.
2. **Testiranje Sigurnosti:** Redovito testiranje sigurnosti IT sustava, uključujući analizu ranjivosti i penetracijska testiranja.
3. **Upravljanje Incidentima:** Uspostava protokola za otkrivanje, prijavu i odgovor na sigurnosne incidente.

Kako Idera alati pomažu u sigurnosnom auditu baze podataka

SQL Secure:

- **Analiza Rizika:** SQL Secure omogućuje identifikaciju i procjenu sigurnosnih rizika unutar SQL Servera. Pruža detaljne informacije o pravima pristupa i povlasticama korisnika, omogućujući detaljnu kontrolu i reviziju.
- **Izvještavanje o Sigurnosti:** Automatizirana izrada izvještaja koji pokrivaju ključne sigurnosne metrike i upozoravaju na potencijalne ranjivosti. Ovi izvještaji pomažu organizacijama u zadovoljavanju regulativnih zahtjeva za dokumentacijom i audite.

https://www.idera.com/productssolutions/sqlserver/sqlsecure/

SQL Compliance Manager:

- **Praćenje Aktivnosti:** SQL Compliance Manager omogućuje praćenje svih aktivnosti unutar baze podataka, uključujući prijavljivanje i praćenje pristupa, promjene u konfiguraciji i izvršavanje kritičnih SQL naredbi.
- **Auditi i Evidencije:** Alat automatski bilježi sve relevantne događaje i omogućuje vođenje detaljnih audit zapisa, što je ključno za usklađivanje s NIS2 i DORA zahtjevima za praćenje i prijavu incidenata.
- **Alerting System:** Postavljanje automatskih upozorenja za određene sigurnosne događaje, omogućujući brzo reagiranje na neobične ili sumnjive aktivnosti.

https://www.idera.com/products/sql-compliance-manager/

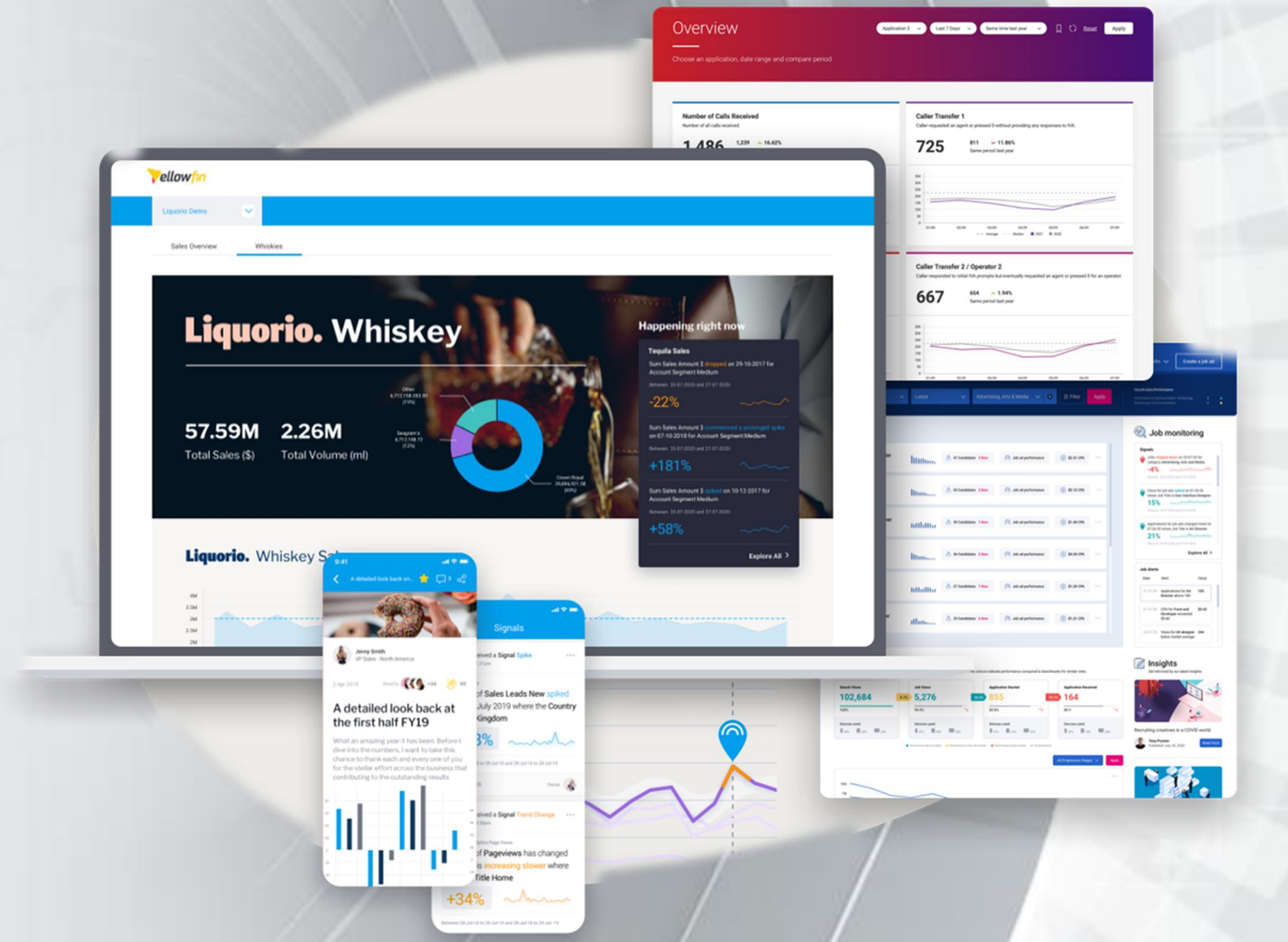
SQL Diagnostic Manager:

- **Performanse i Sigurnost:** SQL Diagnostic Manager prati performanse baze podataka i postavke u realnom vremenu, omogućujući brzu identifikaciju i rješavanje problema koji bi mogli utjecati na ¸dostupnost I performanse.
- **Automatizirani Prijedlozi:** Alat pruža preporuke za optimizaciju performansi, bazirane na najboljim praksama.

https://www.idera.com/products/sql-diagnostic-manager/

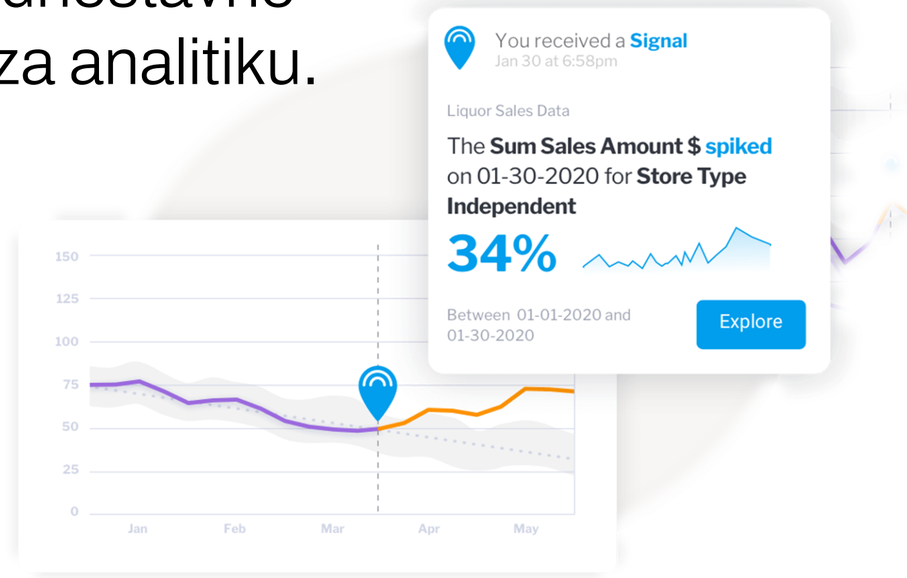
Osiguranje sigurnosti podataka u izvješćima

Yellowfin BI



Što je Yellowfin BI?

Yellowfin BI je napredna platforma za poslovnu inteligenciju koja omogućava organizacijama da prikupljaju, analiziraju i vizualiziraju podatke na učinkovit način. Yellowfin je poznat po svojoj sposobnosti da integrira različite izvore podataka, jednostavno generira prilagodljiva izvješća i nudi napredne alate za analitiku.



https://www.yellowfinbi.com/

1. **Upravljanje Pristupima i Autentikacija**
   - pravila pristupa koja određuju tko može vidjeti ili uređivati određene izvještaje i podatke.
   - Integracija s LDAP i SAML autentikacijom
2. **Šifriranje Podataka**
   - TLS (Transport Layer Security) šifriranje osigurava da su svi podaci koji se prenose između klijenta i servera zaštićeni.
3. **Auditi i Praćenje Aktivnosti**
   - Praćenje aktivnosti unutar Yellowfin BI platforme omogućuje vođenje detaljnih zapisa o tome tko je pristupao kojima podacima i koje promjene su napravljene.

https://www.yellowfinbi.com/

1. **Redukcija podataka (data masking i anonimizacija)**
   - Yellowfin pruža mogućnosti maskiranja osjetljivih podataka ili anonimizacije osobnih informacija, što dodatno smanjuje rizike kao što je gubitak ili krađa podataka.
2. **Sigurnost temeljena na ulogama**
   - Definiranjem uloga i odgovornosti unutar organizacije, Yellowfin BI omogućuje granularnu kontrolu pristupa raznim dijelovima sustava i izvješćima. Korisnicima se mogu dodijeliti specifične uloge koje određuju njihov nivo pristupa i dozvoljene aktivnosti.
3. **Integracija sa sigurnosnim alatima**
   - Mogućnost integracije sa sigurnosnim alatima trećih strana omogućuje proširenje sigurnosnih kapaciteta. Integracija sa SIEM (Security Information and Event Management) rješenjima.

https://www.yellowfinbi.com/

Više na <https://idera.konto.hr/>

<mailto:mladen@konto.hr>

Hvala!