Aspekty technologiczne, a naruszenia ochrony danych osobowych

iSecure

2 luty 2023 r.

Prowadzący

Mateusz Jakubik

Oficer Bezpieczeństwa Informacji w iSecure Sp. z o.o.

Absolwent Wydziału Prawa i Administracji Uniwersytetu Śląskiego w Katowicach, AGH studiów podyplomowych cyberbezpieczeństwo w praktyce oraz Collegium Humanum w Warszawie w zakresie MBA. Doktorant na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego. Czynnie uczestniczy w pracach podgrup ds. ram polityki, ds. badań, innowacyjności i wdrożeń oraz ds. umiejętności cyfrowych w zespole eksperckim Ministerstwa Cyfryzacji ds. programu działań w zakresie AI. Interesuje się prawem nowych technologii ze szczególnym uwzględnieniem IT.

Marcin Paciorkowski

Solutions Architect w CyberArk, CISSP, CEH

Absolwent specjalizacji Systemy Teleinformatyczne na Wydziale Elektroniki Wojskowej Akademii Technicznej oraz studiów podyplomowych „Bezpieczeństwo Systemów Informatycznych" realizowanych na Politechnice Warszawskiej. Jako Solutions Architect w firmie CyberArk, zajmuje się zagadnieniami związanymi z szeroko rozumianą ochroną tożsamości. Posiada ponad 15-letnie doświadczenie zawodowe w obszarze bezpieczeństwa teleinformatycznego potwierdzone licznymi certyfikatami w zakresie wiodących technologii zabezpieczeń (między innymi CISSP, CEH). W trakcie swojej pracy zawodowej brał udział w implementacjach zaawansowanych systemów zabezpieczeń oraz testach penetracyjnych i audytach bezpieczeństwa dużych instytucji w Polsce i regionie.

Plan szkolenia

1. Rozliczalność
2. Kara UODO
3. Kara Finlandia
4. Techniczne aspekty ochrony danych
5. Ochrona tożsamości
6. Plan działania

1. Rozliczalność

Rozliczalność w systemach IT

Rozliczalność danych w systemach IT to zdolność do śledzenia i weryfikowania przemieszczania i wykorzystania danych w systemie informatycznym. Pozwala to na zapewnienie bezpieczeństwa i integralności danych, a także umożliwia odpowiedzialność za ich wykorzystanie.

2. Kara UODO

przetwarzanie danych osobowych w sposób niezapewniający odpowiedniego bezpieczeństwa danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, za pomocą odpowiednich środków technicznych

Wójt Gminy Dobrzyniewo Duże

art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2

Integralność, poufność i rozliczalność

3. Kara Finlandia

Bezprawne przechowywanie danych o stanie zdrowia pracowników w systemie zarządzania zasobami ludzkimi

Viking Line Oy Abp

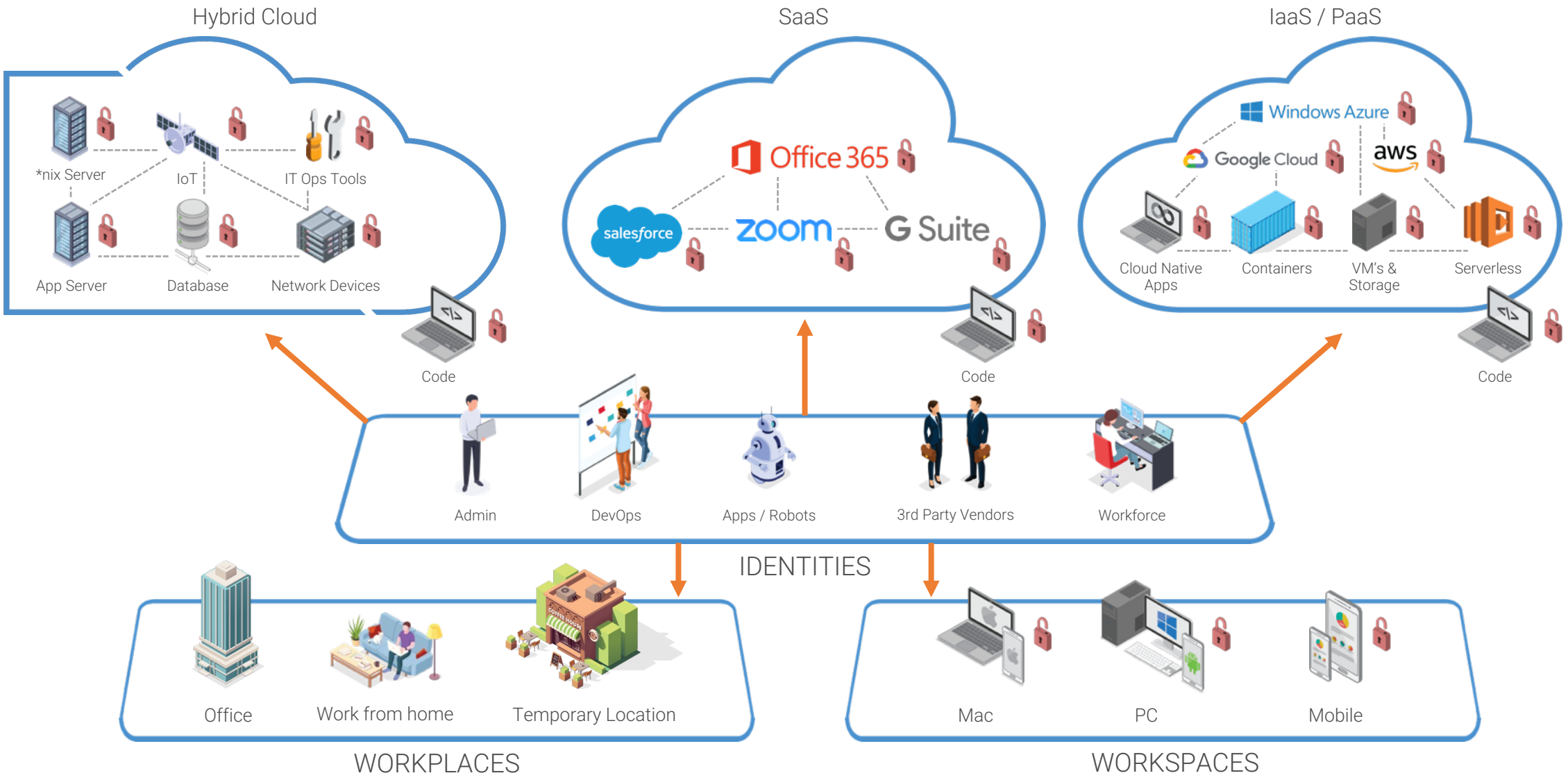
Art. 5 (1) a), d) GDPR, Art. 12 (3) GDPR, Art. 13 GDPR, Art. 15 (1) GDPR, Art. 25 (1) GDPR

Rozliczalność

naruszenia ochrony danych związane z przetwarzaniem danych zdrowotnych pracowników

4. Techniczne aspekty ochrony danych

Zbiór naczyń połączonych

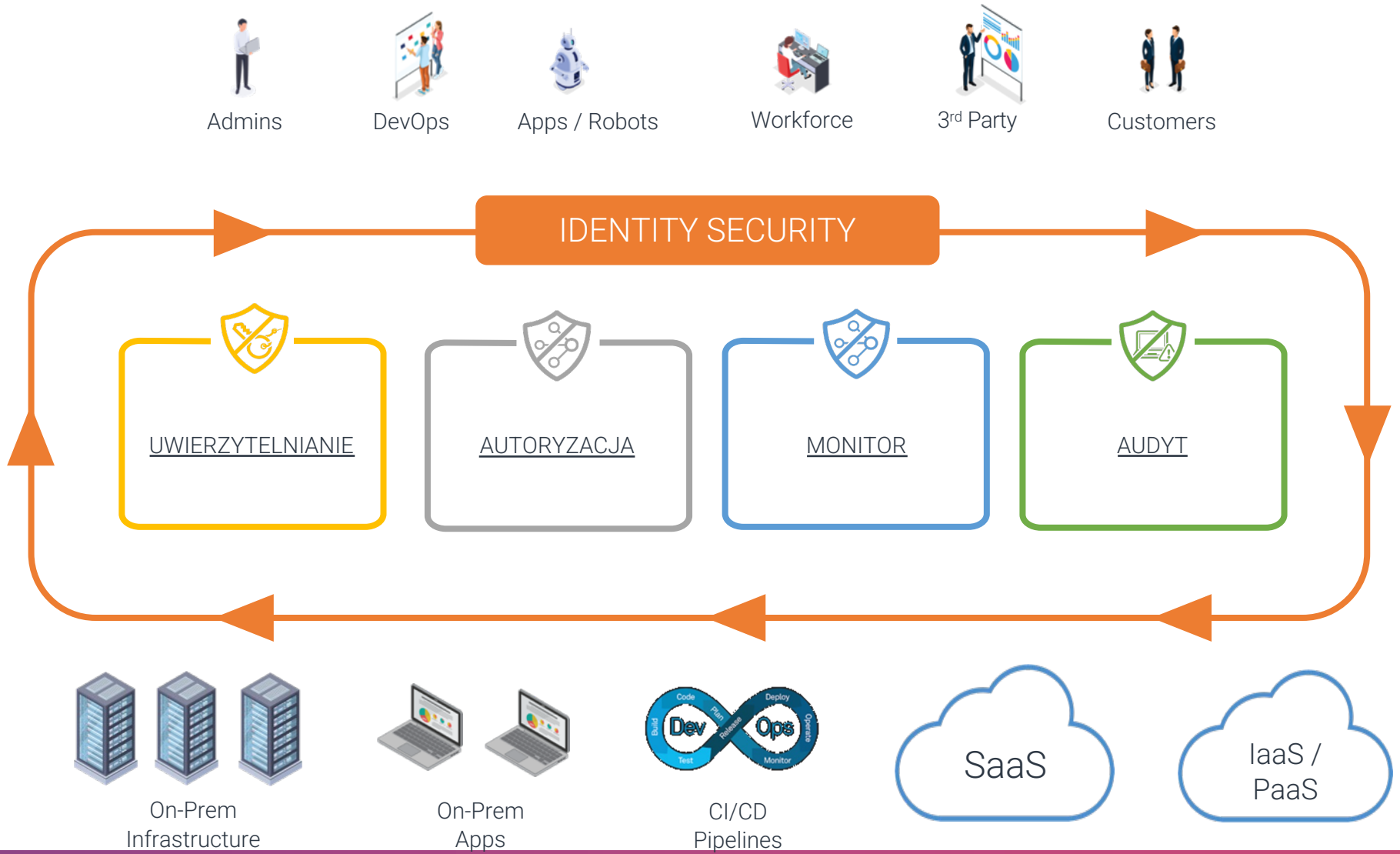


5. Ochrona tożsamości

iSecure

Kluczem jest tożsamość

Podstawowe zasady ochrony tożsamości

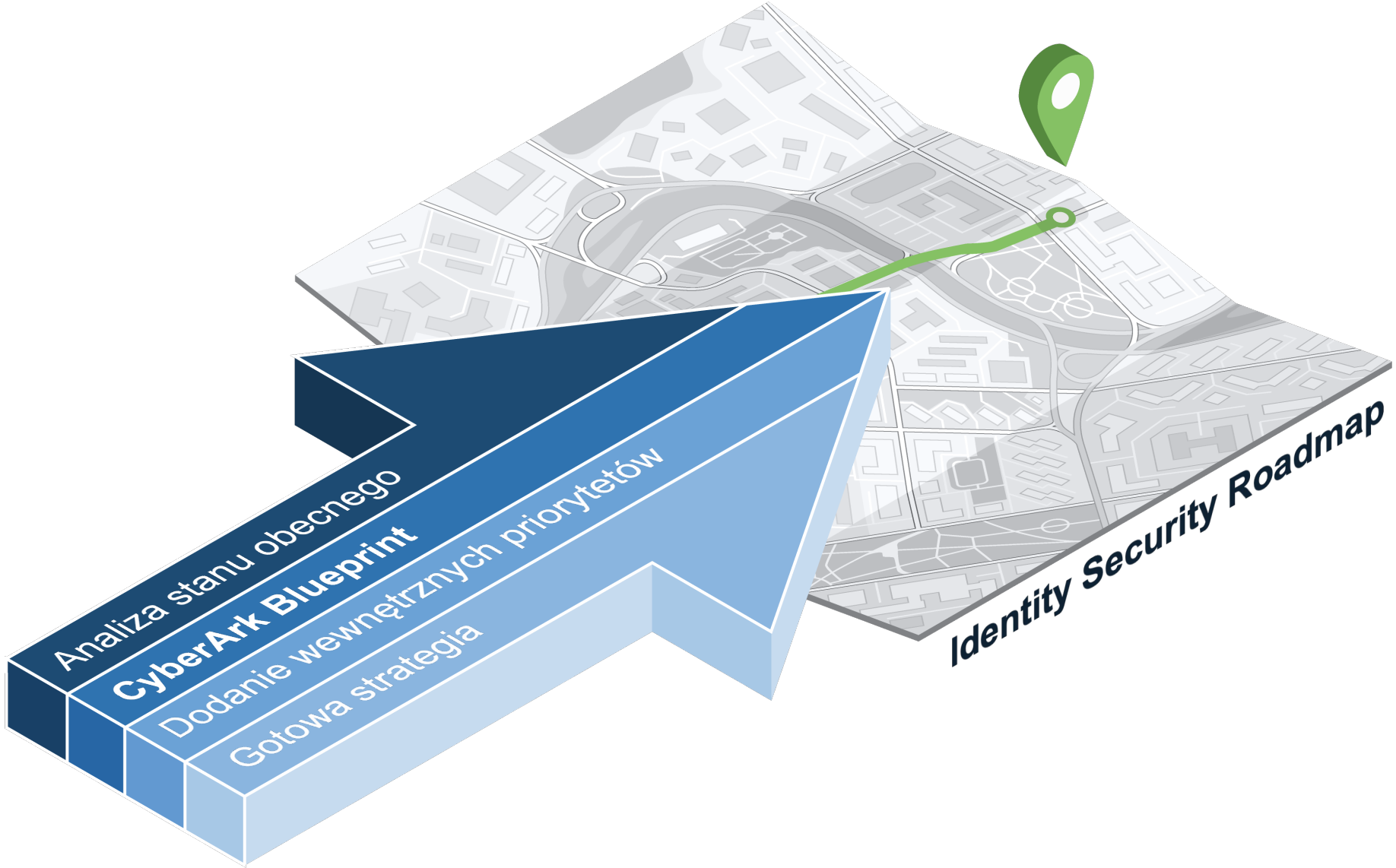


6. Plan działania

iSecure

Powody rozpoczęcia projektów ochrony tożsamości

Tworzenie strategii ochrony tożsamości



Etap 2

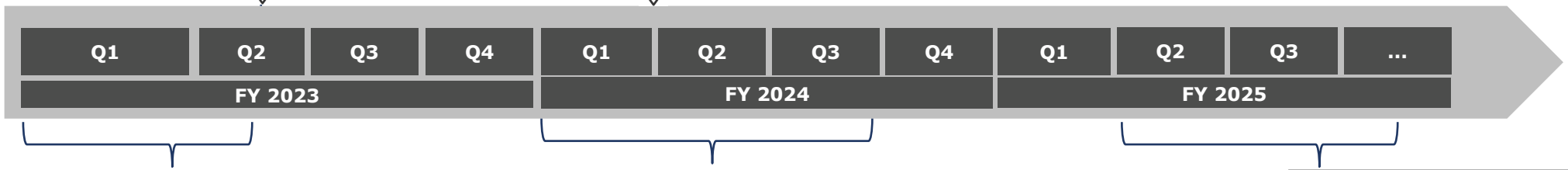
- Konta lokalne stacji roboczych Windows
- Uprzywilejowani użytkownicy AD
- Administratorzy narzędzi CI/CD (Konsole)
- *NIX root
- Integracja z SIEM
- Uprzywilejowani użytkownicy chmur
- Uprzywilejowani użytkownicy chmur
- Stacje administratorów IT oraz deweloperów
- Narzędzia RPA
- DevOps (kontenery, CI/CD) – Pilot
- MFA & SSO dla krytycznych aplikacji biznesowych
- Lifecycle Mgt – Pilot
- Monitoring biznesowych sesji web
- Repozytorium poświadczeń dla użytkowników biznesowych
- MFA / SSO dla Klientów (CIAM) - Pilot

Etap 4

- Urządzenia sieciowe
- Konta administratorów baz danych
- Aplikacje w architekturze Client-Server (krytyczne)
- Wszystkie serwery Windows
- Aplikacje statyczne
  Skrypty administracyjne (krytyczne)

Legenda

- Punkt aktualizacji strategii
- Zdalny dostęp & PAS
- Minimalne uprawnienia
- Zarządzanie sekretami
- Użytkownicy biznesowi



Etap 1 (Sprint)

- Administratorzy domeny
- Lokalne konta serwerów Windows
- Administratorzy wirtualizatorów
- Bezpieczny zdalny dostęp firm zewnętrznych
- MFA, SSO dla dostępu uprzywilejowanego
- Globalni administratorzy chmur
- Administratorzy chmur
- Narzędzia/systemy bezpieczeństwa (skanery podatności)
- MFA, SSO dla użytkowników biznesowych – Pilot
- Repozytorium poświadczeń dla użytkowników biznesowych - Pilot

Etap 3

- Administratorzy *NIX (o podobnych uprawnieniach jak root)
- Klucze SSH w środowisku *NIX
- Konta systemowe baz danych
- Krytyczne usługi w środowisku MS
- Dostęp Out of Band
- Ochrona kontrolerów domeny
- Stacje robocze wszystkich użytkowników
- Krytyczne serwery Windows
- DevOps (kontenery, mikroserwisy, CI/CD)
- MFA & SSO dla wszystkich aplikacji biznesowych
- MFA / SSO dla Klientów (CIAM)
- Lifecycle Mgt

Etap 5

- Wszystkie plikacje w architekturze Client-Server
- Konta usług Windows*
- Kontrolery domeny
- Serwery *NIX
- Wszystkie aplikacje statyczne
- Wszystkie skrypty administracyjne


A GOAL
WITHOUT A PLAN
IS JUST A
WISH

Dziękujemy

iSecure

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa

tel. +48 22 126 58 54
fax. +48 22 378 26 34
kontakt@isecure.pl