AI dla administratorów IT (kod: AI-Admin-IT)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Opis i cel szkolenia

Większość administratorów używa dziś AI dorywczo: wkleja komunikat błędu do przeglądarki, kopiuje odpowiedź, wraca do pracy. To działa, ale jest to margines tego, co te narzędzia dziś potrafią — i przy okazji najprostszy sposób, żeby wysłać na zewnątrz fragment konfiguracji, który nie powinien tam trafić. Nasze szkolenie "jest o przeniesieniu AI z poziomu czata z zakładki w przeglądarce" do codziennego **warsztatu administratora, z ustalonym sposobem pracy, granicami i kontrolą nad tym, co się dzieje**.

Prawdziwe zmiany ostatnich lat nie polegają na tym, że czat podpowie nam składnię polecenia. Polegają na tym, że agent uruchomiony w terminalu ma dostęp do systemu i sam wykonuje zadania: przegląda konfiguracje, czyta logi, proponuje i wprowadza zmiany. Jest to jednocześnie naprawdę użyteczne i ryzykowne. Dlatego drugi dzień poświęcamy w dużej części temu, **jak wpuścić agenta AI na własne systemy i nie zrobić sobie krzywdy**. Jakie nadać mu uprawnienia, co mu zlecać, jak zapewnić sobie możliwość cofnięcia zmian. Ale też: jak rozpoznać, że treść, którą nasze AI właśnie analizuje — log, plik od klienta, zgłoszenie — próbuje nim sterować (nowe sposoby ataków!).

Podczas szkolenia pracujemy na symulowanym, ciągłym scenariuszu - tak, aby nie było to kilkanaście oderwanych demonstracji. Uczestnik dostaje nieudokumentowane środowisko i przez dwa dni doprowadza je do porządku: rozpoznaje, co i jak w nim działa, porządkuje odziedziczone skrypty, odtwarza z logów przebieg awarii, buduje dokumentację i runbooki - a na koniec spisuje zasady, według których będzie z AI pracował dalej.

Osobny wątek to **praca bez wysyłania czegokolwiek na zewnątrz**. Część administratorów — w administracji publicznej, w instytucjach, w firmach z twardą polityką danych — nie może przekazać logu ani konfiguracji do usługi chmurowej. Pokazujemy więc, jak uruchomić model lokalnie, udostępnić go zespołowi i podpiąć pod własną dokumentację. Porównujemy też uczciwie jakość odpowiedzi modelu lokalnego i chmurowego na tym samym zadaniu — nie sprzedajemy tezy, że lokalnie zawsze wychodzi tak samo dobrze.

Czego na tym szkoleniu świadomie nie ma:

- **Nie jest to szkolenie programistyczne**. Nie budujemy własnych agentów w kodzie, nie piszemy integracji z API modeli i nie robimy firmowych czatbotów. Uczymy korzystać z gotowych narzędzi w pracy administracyjnej — bez wymagania umiejętności programowania.
- **Nie jest to szkolenie z cyberbezpieczeństwa**. Bezpieczeństwo traktujemy tu jako higienę codziennej pracy administratora: co wolno przekazać modelowi, jak zweryfikować wygenerowane polecenie przed uruchomieniem na produkcji, jak ograniczyć uprawnienia agenta. Ofensywne i defensywne zastosowania AI w bezpieczeństwie, ataki na modele językowe i praca zespołów SOC to zakres osobnego szkolenia — "AI w cyberbezpieczeństwie":https://www.alx.pl/szkolenia/bezpieczenstwo-systemow-ai/.
- **Nie ma przeglądu platform AIOps ani uczenia maszynowego w monitoringu**. Wykrywanie anomalii i predykcja awarii to obecnie najczęściej funkcje kupowanych platform, albo konfigurowane samodzielnie modele machine learning. Nie jest to jednak umiejętność do zdobycia w dwa dni razem ze wszystkimi pozostałymi tematami.

Po szkoleniu uczestnik będzie potrafił:

- dobrać tryb pracy z AI do zadania — czat, asystent w terminalu, agent z dostępem do systemu, model lokalny;
- prowadzić z modelem techniczną rozmowę opartą na właściwym kontekście i weryfikować odpowiedź, zamiast przenosić ją wprost na produkcję;
- używać agenta uruchomionego w terminalu do rozpoznania środowiska, pracy ze skryptami i triage'u logów, przy jawnie ograniczonych uprawnieniach;
- uruchomić model lokalnie, podpiąć pod niego własną dokumentację i ocenić, kiedy ma to sens;
- rozpoznać treść próbującą sterować modelem i wskazać, co nigdy nie powinno trafić do promptu;
- spisać dla swojego zespołu zasady korzystania z AI, które da się egzekwować.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

W grupach ogólnodostępnych ćwiczenia prowadzimy w środowisku Linux. PowerShell i specyfika świata Windows pojawiają się jako dodatek, tam, gdzie różnica jest istotna. Dla grup, na życzenie, możliwa jest realizacja i dostosowanie przykładów do dowolnego środowiska.

Czas trwania

2 dni

Program

1. Model językowy z perspektywy administratora
   - Czym model dysponuje, a czego nie wie: okno kontekstu, granica wiedzy, brak dostępu do Twojego systemu
   - Dlaczego modele mylą składnię, opcje poleceń i nazwy pakietów, i kiedy jest to groźne
   - Cztery tryby pracy: czat, asystent w terminalu, agent z dostępem do systemu, model lokalny
   - Dobór trybu pracy do zadania administracyjnego
   - Co dzieje się z danymi przekazywanymi do modelu: chmura, on-premises, retencja, ustawienia firmowe
2. Techniczna rozmowa z modelem: kontekst i weryfikacja
   - Podawanie kontekstu: dystrybucja, wersje, konfiguracja, wyjścia poleceń, pełna treść błędu
   - Praca iteracyjna: zawężanie problemu, proszenie o alternatywy i o uzasadnienie rozwiązania
   - Typowe pułapki: przestarzała składnia, wymyślone opcje, mieszanie dystrybucji i wersji
   - Weryfikacja odpowiedzi zanim cokolwiek uruchomisz: dokumentacja, tryb próbny, środowisko testowe
   - Ćwiczenie: diagnoza usługi, która nie startuje po zmianie konfiguracji
3. Skrypty administracyjne: pisanie, czytanie, refaktoryzacja, debugowanie
   - Generowanie skryptów powłoki bash z pomocą AI - pod konkretne zadanie administracyjne
   - Czytanie i opisywanie cudzych, nieudokumentowanych skryptów
   - Uodpornianie skryptu: obsługa błędów, idempotentność, logowanie, tryb próbny
   - Debugowanie skryptu, który działa, ale nie tak jak powinien
   - Specyfika pracy z modelem w środowisku PowerShell

— Ćwiczenie: uporządkowanie zestawu odziedziczonych skryptów; przygotowywanie prostej dokumentacji technicznej przy wsparciu AI

4. Logi, komunikaty systemowe i odtwarzanie zdarzeń
   — Triage: od tysięcy linii do hipotezy, którą da się sprawdzić
   — Korelacja zdarzeń z kilku źródeł i budowa osi czasu incydentu
   — Praca z journalctl, syslogiem i wyjściami narzędzi diagnostycznych
   — Gdzie model realnie pomaga, a gdzie "wymyśla" przyczynę i tylko brzmi przy tym wiarygodnie
   — Ćwiczenie: ustalenie przebiegu awarii na podstawie materiału z systemu
5. Agent AI w terminalu na własnym systemie
   — Czym agent różni się od asystenta: pętla działania, narzędzia, dostęp do systemu plików i poleceń
   — Przegląd agentów uruchamianych w terminalu i kryteria wyboru: rozwiązania komercyjne i otwarte
   — Konfiguracja pracy: katalog roboczy, zakres uprawnień, tryb tylko do odczytu, zatwierdzanie poleceń
   — Siatka bezpieczeństwa: konto o ograniczonych uprawnieniach, migawka lub kontener, repozytorium jako historia zmian
   — Zadania, które warto zlecać agentowi, i takie, których nie należy
   — Ćwiczenie: rozpoznanie nieznanego środowiska agentem w trybie tylko do odczytu, a następnie kontrolowana zmiana
6. Modele lokalne i praca z własną dokumentacją
   — Kiedy model lokalny ma sens: dane, które nie mogą opuścić organizacji, praca offline, koszt
   — Uruchomienie modelu lokalnie (Ollama lub narzędzie analogiczne) i udostępnienie go zespołowi
   — Realne ograniczenia: jakość odpowiedzi, wymagania sprzętowe, długość kontekstu
   — Porównanie modelu lokalnego i chmurowego na tym samym zadaniu administracyjnym
   — Podpięcie własnej dokumentacji i runbooków (RAG) oraz czego nie należy się po tym spodziewać
   — Ćwiczenie: pytania do dokumentacji środowiska na modelu uruchomionym lokalnie
7. Dokumentacja, runbooki i raporty
   — Opisanie przejętego środowiska: inwentarz, zależności, decyzje konfiguracyjne
   — Budowa runbooka na podstawie sesji pracy nad problemem
   — Raport i post-mortem po incydencie
   — Utrzymanie dokumentacji w czasie zamiast jednorazowego wygenerowania ściany tekstu
8. Bezpieczeństwo i zasady pracy z AI
   — Co nigdy nie trafia do promptu: dane uwierzytelniające, klucze, konfiguracje zabezpieczeń, dane osobowe, topologia sieci
   — Anonimizacja materiału przekazywanego do analizy i automatyzacja tego kroku
   — Prompt injection w treści, którą sam analizujesz: logi, pliki od klienta, zgłoszenia, strony WWW
   — Dlaczego agent z jednoczesnym dostępem do danych, niezaufanej treści i sieci jest konfiguracją wysokiego ryzyka
   — Weryfikacja poleceń i skryptów przed uruchomieniem w środowisku produkcyjnym
   — Granice automatyzacji: gdzie decyzja musi pozostać przy człowieku

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

— Ćwiczenie: własne, krótkie zasady korzystania z AI dla zespołu administratorów

Przeznaczenie i wymagania

Szkolenie jest przeznaczone dla osób, które faktycznie administrują, zarządzają systemami, czy kierowników działów informatycznych — nie dla osób zupełnie początkujących w IT. W szczególności:

— administratorzy systemów i sieci odpowiadający w firmie lub instytucji „za wszystko";
— administratorzy Linuksa i inżynierowie utrzymania, także w środowiskach mieszanych;
— osoby prowadzące utrzymanie w organizacjach, które nie mogą przekazywać danych do usług chmurowych;
— starsi administratorzy i liderzy zespołów, którzy muszą ustalić zasady korzystania z AI dla swojego zespołu;
— specjaliści drugiej linii wsparcia z praktycznym doświadczeniem w terminalu.

Od uczestników oczekiwane jest:

— praktyczne doświadczenie w administrowaniu systemami lub sieciami;
— znajomość i praca w terminalu systemu Linux;
— podstawy skryptowania w powłoce bash; znajomość PowerShella - miły dodatek, ale nie jest wymagana;
— umiejętność czytania wybranych logów i plików konfiguracyjnych;
— nie jest wymagana wiedza o uczeniu maszynowym ani doświadczenie w programowaniu;
— ćwiczenia z modelami uruchamianymi lokalnie realizujemy na komputerach udostępnionych przez ALX - nie potrzeba posiadać własnego, odpowiedniego sprzętu.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

1890 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl