Moc jednej platformy

System specjalnie zaprojektowany pod kątem długoterminowej wartości, cyberbezpieczeństwa i integracji

AXIS COMMUNICATIONS

Serce urządzeń sieciowych Axis

AXIS OS to oparty na Linuksie system operacyjny używany w większości urządzeń sieciowych Axis. Jest on sercem ponad 200 produktów Axis i kilkudziesięciu milionów urządzeń wdrożonych u klientów. Axis OS to wyraz zaangażowania na rzecz innowacji, niezawodności i płynnej integracji. To właśnie dzięki oprogramowaniu Axis nasze urządzenia są tak niezawodne i zapewniają tak znakomitą jakość obrazu, natomiast my ulepszamy to oprogramowanie z każdą nową wersją. Aż 80% naszych projektów badawczo-rozwojowych dotyczy prac nad oprogramowaniem.

Nieustannie dodajemy nowe funkcje i ulepszamy istniejące. Ponadto stale zwiększamy bezpieczeństwo przez usuwanie luk w zabezpieczeniach urządzeń opartych na systemie AXIS OS, dzięki czemu stają się one lepsze i bezpieczniejsze w coraz szerszej gamie zastosowań.

System AXIS OS został specjalnie zaprojektowany, aby spełniać najważniejsze kryteria dotyczące urządzeń sieciowych, do których należą długoterminowa wartość, wysokie standardy cyberbezpieczeństwa i łatwość integracji.

Specjalnie zaprojektowany dla urządzeń Axis
AXIS OS, stworzony przez dział programistyczny zajmujący się wyłącznie tym systemem i wykorzystujący stabilność platformy Linux Yocto OpenEmbedded, przewyższa systemy ogólnego przeznaczenia, ponieważ jest doskonale zoptymalizowany pod kątem szczególnych wymagań urządzeń brzegowych Axis, takich jak kamery, głośniki i urządzenia kontroli dostępu.

Długoterminowa wartość
System AXIS OS zapewnia nieprzerwaną dostępność urządzeń. Został zaprojektowany do pracy w trybie 24/7 oraz cechuje się spójnym i responsywnym działaniem, które spełnia długofalowe wymagania aplikacji niezależnie od pory dnia i nocy.

Solidne cyberzabezpieczenia
Fundamentem systemu AXIS OS jest przywiązanie do cyberbezpieczeństwa. Za sprawą wbudowanej architektury zabezpieczeń AXIS OS pomaga w ochronie urządzeń. Dzięki praktykom bezpiecznego rozwoju oprogramowania i aktywnemu zarządzaniu lukami zabezpieczeń AXIS OS uodparnia dane i urządzenia klienta na pojawiające się zagrożenia.

Płynna integracja
System AXIS OS jest zgodny ze standardami VAPIX, ONVIF itp., ułatwiając integrację urządzeń sieciowych Axis z różnymi ekosystemami. Dzięki tej łatwości integracji użytkownicy i programiści zyskują płynnie działające i wzajemnie połączone środowisko.

AXIS OS w liczbach

900 programistów

24 000 000 napisanych linijek kodu

4000 operacji commit dziennie

4 000 000 zautomatyzowanych testów dziennie

Ponad 200 produktów Axis objętych aktywną ścieżką wsparcia

Ponad 500 produktów Axis objętych ścieżkami wsparcia długoterminowego

Ponad 6 wydań oprogramowania rocznie na ścieżce aktywnej

Ponad 2000 komponentów oprogramowania

Ponad 95% komponentów open source

Specjalnie zaprojektowany dla urządzeń Axis

Podczas projektowania systemu AXIS OS koncentrowaliśmy się na wydajności, integracji, bezpieczeństwie i jakości oprogramowania do urządzeń brzegowych.

Wykorzystując stabilność środowiska Linux Yocto OpenEmbedded, AXIS OS stanowi kompleksową, zunifikowaną platformę dla wszystkich urządzeń sieciowych Axis, która zapewnia spójne wrażenia użytkowe w zróżnicowanej gamie produktów.

Na kolejnych stronach bardziej szczegółowo opisano zalety systemu operacyjnego stworzonego specjalnie z myślą o urządzeniach brzegowych, a także atuty jednej platformy.

Doskonałość na brzegu sieci

W otoczeniu zdominowanym przez rozwiązania ogólnego przeznaczenia AXIS OS nie jest jedynie kolejnym systemem operacyjnym opartym na Linuksie. Wbrew konwencjom typowym dla ogólnych kompilacji Linuksa zapewnia on rozwiązanie ściśle odpowiadające specyfice urządzeń brzegowych. Ta specjalizacja sprzyja wydajności, niezawodności i bezpieczeństwu, które można spotkać wyłącznie w produktach Axis.

Fundament: Linux Yocto
Solidny fundament w postaci Linux Yocto OpenEmbedded zapewnia stabilność i wydajność. Linux Yocto OpenEmbedded oferuje także znajome środowisko programistom. Platforma ta jest podstawą płynnego działania urządzeń sieciowych Axis.

Obsługa różnych procesorów
AXIS OS to system z definicji wszechstronny. Udostępnia on dedykowaną obsługę procesora Axis ARTPEC obecnego w większości urządzeń Axis, a ponadto jest zgodny z chipami innych firm. Dzięki temu możliwości systemu AXIS OS są dostępne dla szerokiej gamy urządzeń sieciowych.

Zaprojektowany pod kątem długoterminowej wartości
Od naszych urządzeń oczekujemy wieloletniego działania. Dlatego system AXIS OS zaprojektowaliśmy z myślą o solidności i trwałości. Ponadto na stronie axis.com jasno informujemy o oczekiwanym okresie funkcjonowania naszych urządzeń.

Rygorystyczne, ukierunkowane testy
System AXIS OS jest poddawany rygorystycznym testom mającym zapewnić jego znakomite działanie w docelowym obszarze zastosowań. Testujemy go dokładnie, ponieważ chcemy, aby przewyższał oczekiwania w zakresie wydajności, cyberbezpieczeństwa i integracji.

Jakość oprogramowania
AXIS OS jest dowodem niezłomnego dążenia do znakomitej jakości oprogramowania. System został zaprojektowany zgodnie z wysokimi standardami, aby zapewnić znajome, niezawodne i bezpieczne środowisko obsługi przez cały okres korzystania z urządzeń Axis.

Moc jednej platformy

Nasze dążenie do doskonałości wykracza poza kategorie produktów i znajduje swój praktyczny wyraz w czymś, co nazywamy mocą jednej platformy. Dzięki wsparciu ponad 200 produktów — od kamer nasobnych po rozwiązania z ochroną przeciwwybuchową, od kamer PTZ po syreny i od głośników po interkomy — nasza zunifikowana platforma skutecznie odpowiada na potrzeby partnerów i klientów.

Spójność w działaniu
System AXIS OS napędza zróżnicowaną gamę produktów. Wszystkie nasze urządzenia korzystają z tych samych interfejsów API i cechują się tym samym sposobem działania. Jedna platforma sprawia, że integratorzy i programiści mogą wdrażać w systemach nowe urządzenia Axis bez potrzeby stosowania złożonych sterowników przeznaczonych dla poszczególnych urządzeń. To nie tylko przyspiesza integrację, ale też zabezpiecza rozwiązania na przyszłość, umożliwiając szybkie wprowadzanie nowych produktów ze stale rozrastającego się ekosystemu Axis. Dla klientów oznacza to spójne wrażenia użytkowe, natomiast programistom pozwala zaoszczędzić czas i pieniądze, ponieważ każde rozwiązanie z zakresu integracji działa na każdym urządzeniu z systemem AXIS OS.

Wszechstronność bez złożoności
Moc jednej platformy polega także na tym, że zunifikowana platforma otwiera drogę do różnorodności, z którą w parze nie idzie złożoność. Niezależnie od tego, czy chodzi o integrację kamery PTZ z systemem dozoru czy o dodanie głośnika do inteligentnego rozwiązania audio, proces przebiega bardzo podobnie. Wszechstronność nie ogranicza się do samej zgodności, lecz obejmuje spójne wrażenia użytkowe i liczne możliwości tworzenia zintegrowanych rozwiązań odpowiadających indywidualnym potrzebom.

Zunifikowane zabezpieczenia
W świecie, w którym ogromną rolę odgrywa cyberbezpieczeństwo, moc jednej platformy przejawia się także we wsparciu zunifikowanego rozwiązania w całym spektrum produktów. Dbanie o bezpieczeństwo nie wymaga żmudnych działań na poziomie poszczególnych produktów. W przypadku zidentyfikowania i zneutralizowania luki w zabezpieczeniach odpowiednia poprawka jest przekazywana do wszystkich obsługiwanych urządzeń. To nie tylko usprawnia zarządzanie zabezpieczeniami, ale też ułatwia sprawne, zbiorcze reagowanie na nowe zagrożenia. Kolejną ważną zaletą są oszczędności czasu i zasobów oraz wzmocnienie odporności całego ekosystemu Axis.

Długoterminowa wartość

System AXIS OS kształtuje przewidywalną wartość w całym cyklu istnienia urządzeń. Stabilna i solidna architektura ogranicza przestoje do minimum.

Aktualizacje oprogramowania — w tym zupełnie owe funkcje — są dostarczane przez wiele lat. Dzięki obszernej dokumentacji, pomocnym narzędziom i intuicyjnemu interfejsowi urządzenia Axis są łatwe w użytkowaniu i konserwacji. Natomiast przejrzyste i niezawodne harmonogramy wydań pozwalają planować konserwację z uwzględnieniem indywidualnych potrzeb przedsiębiorstwa.

Na kolejnych stronach bardziej szczegółowo opisano jakość oprogramowania Axis oraz zasady zarządzania cyklem istnienia systemu AXIS OS i wsparcia programowego.

Oprogramowanie godne zaufania

Jakość systemu AXIS OS ma dla nas duże znaczenie. Nad naszym systemem operacyjnym pracuje około 900 programistów, a do głównej gałęzi AXIS OS codziennie wprowadzanych jest około 4000 modyfikacji kodu, które dostosowują system do ewoluujących potrzeb rynkowych. Każdy z ponad 200 naszych produktów otrzymuje dwie kompilacje oprogramowania dziennie, co przekłada się na zawrotną liczbę 182 500 kompilacji rocznie, stwarzających możliwość prowadzenia testów iteracyjnych i zapewniających wartość dodaną.

Rygorystyczne testy
Dbanie o stabilność oprogramowania wymaga także prowadzenia rygorystycznych testów. Dlatego warto wspomnieć, że w naszych systemach codziennie wykonywane są aż 4 miliony różnych przypadków testowych. Ich uzupełnieniem jest ponad 4000 dziennych modyfikacji kodu, które usuwają luki i podnoszą jakość oprogramowania. Rocznie daje to ponad 1 miliard testów i ponad 1 000 000 modyfikacji kodu. Ponadto umożliwiamy klientom i partnerom bezpośrednie przekazywanie uwag na temat systemu AXIS OS.

Ciągłe doskonalenie
System AXIS OS nie jest tworem statycznym, lecz dynamicznym, ponieważ stale go ulepszamy. Dzięki regularnym aktualizacjom i udoskonaleniom urządzenia Axis objęte aktywną ścieżką wsparcia systemu AXIS OS ewoluują wraz z rozwojem technologii. Oznacza to, że raz kupiony produkt przez cały okres swojej eksploatacji jest wzbogacany o nowe funkcje, a jego wartość rośnie.

Wsparcie cyklu istnienia urządzeń

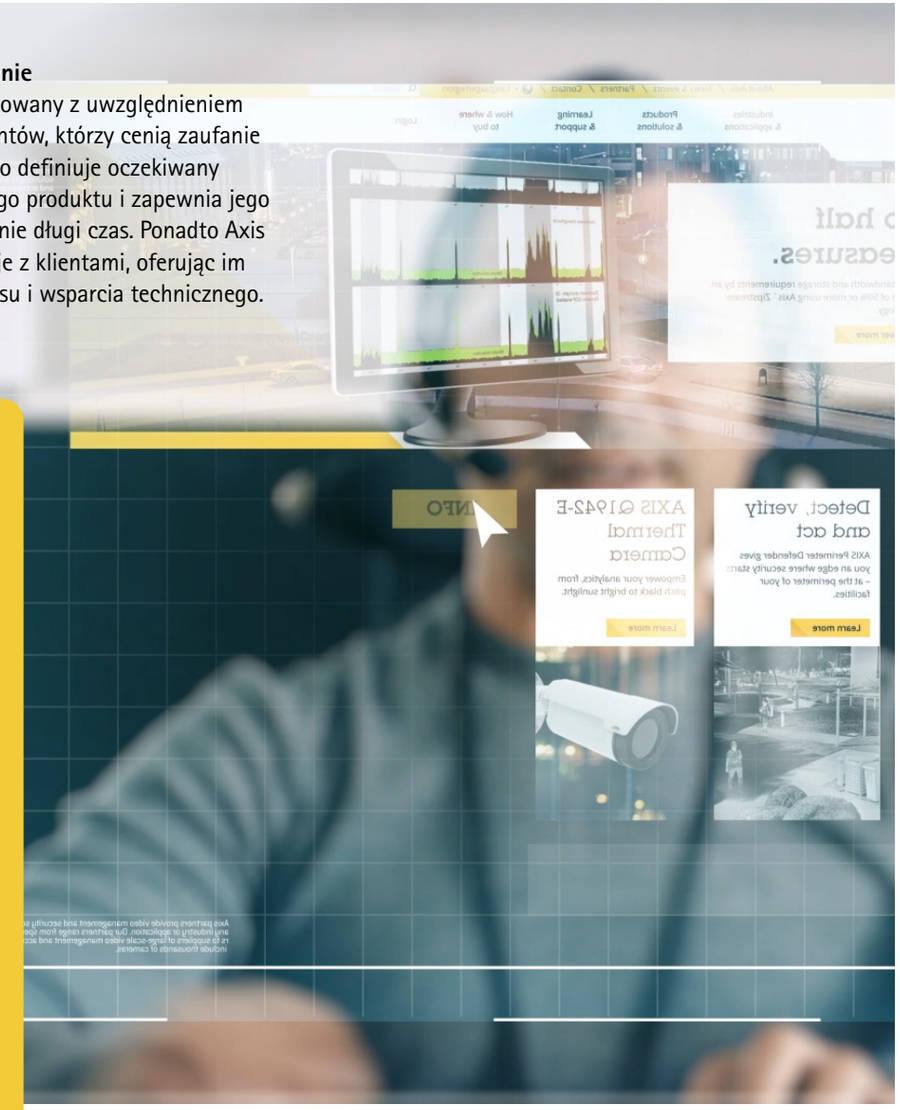
Jedną z zalet korzystania z systemu AXIS OS jest jego przystosowanie do pełnego cyklu eksploatacji urządzeń, od instalacji przez konserwację po wymianę. AXIS OS udostępnia narzędzia i zasoby ułatwiające zarządzanie urządzeniami Axis oraz ich optymalizację w całym cyklu istnienia.

Łatwa instalacja i konfiguracja
System AXIS OS upraszcza instalację i konfigurację urządzeń Axis, ponieważ udostępnia kreatory, szablony i profile pomagające w tym procesie. Aby zaoszczędzić czas i energię, można także używać narzędzi AXIS Device Manager (ADM) i AXIS Device Manager Extend (ADMX) w celu jednoczesnego instalowania i konfigurowania wielu urządzeń.

Ciągłe monitorowanie i diagnostyka
Za zgodą użytkownika system AXIS OS monitoruje i analizuje działanie i status urządzeń Axis, zbierając odpowiednie dane w postaci dzienników, raportów oraz alertów. Ułatwia to użytkownikom identyfikację i rozwiązywanie ewentualnych problemów, a nam pomaga w doskonaleniu oprogramowania z wersji na wersję.

Długoterminowe wsparcie i zgodność
System AXIS OS zapewnia długoterminowe wsparcie urządzeń Axis dzięki regularnym aktualizacjom zabezpieczeń i poprawkom błędów. Ścieżka wsparcia długoterminowego, w której priorytetem jest zgodność z urządzeniami i aplikacjami Axis, minimalizuje liczbę zmian i przerw w działaniu. Czas eksploatacji urządzeń korzystających z systemu AXIS OS zazwyczaj wynosi minimum 10 lat. W niektórych przypadkach zapewniamy ich wsparcie nawet przez 13 lat.

Zaufanie i zaangażowanie
AXIS OS został zaprojektowany z uwzględnieniem oczekiwań i potrzeb klientów, którzy cenią zaufanie i jakość. System ten jasno definiuje oczekiwany okres eksploatacji każdego produktu i zapewnia jego obsługę przez maksymalnie długi czas. Ponadto Axis dba o długofalowe relacje z klientami, oferując im optymalny poziom serwisu i wsparcia technicznego.



AXIS OS beta

Wersja beta systemu AXIS OS przydaje się programistom i integratorom, którym zależy na testowaniu i ocenie najnowszych funkcji tego systemu przed ich oficjalnym udostępnieniem. Systemu AXIS OS w wersji beta można używać do wczesnego testowania zgodności na wybranych urządzeniach, weryfikowania nadchodzących aktualizacji zabezpieczeń i zapoznawania się z przygotowywanymi funkcjami.

Oto wybrane zalety korzystania z systemu AXIS OS w wersji beta:

> Możliwość zapoznania się z nowymi i udoskonalonymi funkcjami, które w przyszłości będą dostępne w systemie AXIS OS, takimi jak analizy na brzegu sieci, łączność IoT i modularyzacja platformy
> Możliwość przekazywania do firmy Axis uwag i sugestii mogących wpłynąć na prace rozwojowe oraz udoskonalenia wprowadzane w systemie AXIS OS
> Możliwość przygotowania i przystosowania własnych aplikacji i systemów pod kątem nadchodzących zmian i aktualizacji systemu AXIS OS w celu uniknięcia potencjalnych problemów

Więcej informacji na temat wersji beta systemu AXIS OS można znaleźć tutaj.

AXIS OS — wsparcie programowe w cyklu istnienia produktów

Wsparcie systemu AXIS OS w cyklu istnienia produktów obejmuje różne ścieżki. Główne z nich to ścieżka aktywna i ścieżka wsparcia długoterminowego. Istnieją także ścieżki wsparcia związane z określonymi produktami, które odpowiadają ich indywidualnym cyklom istnienia.

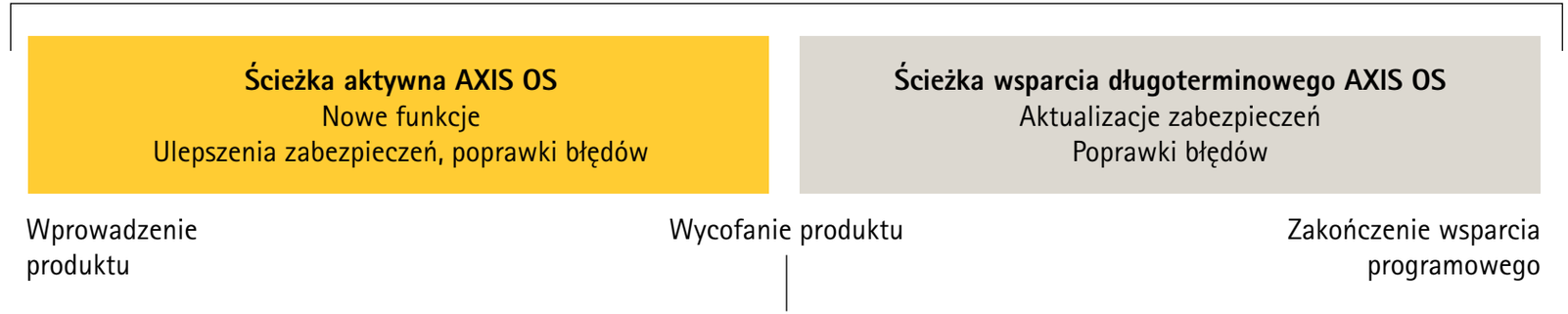
Minimalny okres eksploatacji urządzenia Axis przewyższa standardy branżowe. Uzupełnieniem atrakcyjnej 5-letniej gwarancji sprzętowej jest wieloletnie wsparcie programowe w systemie AXIS OS. Okres obsługi większości urządzeń w systemie AXIS OS wynosi aż 8–12 lat.

Wygląda to następująco:

1. Kiedy Axis wprowadza nowe urządzenie, dostępna jest tylko ścieżka aktywna AXIS OS. W początkowym okresie po wprowadzeniu produktu klient na bieżąco otrzymuje aktualizacje i udoskonalenia, w tym nowe funkcje.
2. W ciągu dwóch lat od wprowadzenia produktu udostępniana jest ścieżka wsparcia długoterminowego, stanowiąca alternatywę dla ścieżki aktywnej. Wówczas klient może wybrać ścieżkę aktywną lub ścieżkę wsparcia długoterminowego. Wsparcie produktów w ramach ścieżki długoterminowej ogranicza się do aktualizacji zabezpieczeń i poprawek błędów.
3. Od dwóch do czterech lat po premierze, gdy urządzenie zostaje wycofane, końca dobiega również związana z nim ścieżka aktywna. Na tym etapie wszystkie urządzenia są automatycznie przenoszone do ścieżki wsparcia długoterminowego, w ramach której otrzymują aktualizacje zabezpieczeń i poprawki błędów przez minimum 5 lat.

AXIS OS — wsparcie programowe w cyklu istnienia produktów

Wsparcie programowe (8–12 lat)



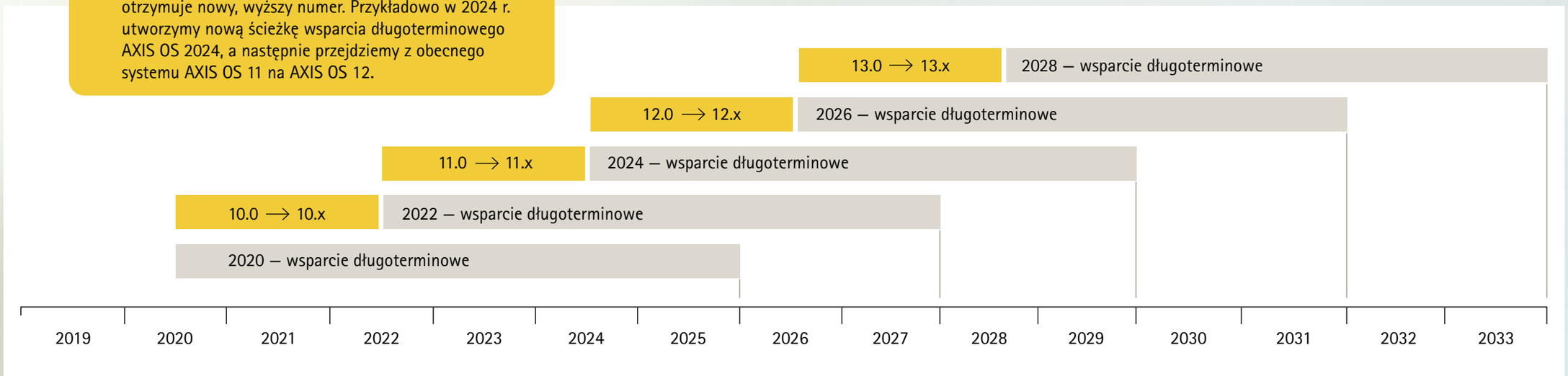
Która ścieżka wsparcia programowego będzie dla Ciebie odpowiednia?

Gdy są dostępne zarówno ścieżka aktywna, jak i ścieżka wsparcia długoterminowego, klient na podstawie wskazówek oferowanych przez Axis może wybrać tę z nich, która optymalnie odpowiada jego potrzebom.

Ścieżka aktywna
W ramach ścieżki aktywnej dostępne jest najbardziej aktualne środowisko systemu operacyjnego AXIS OS z najszerszą zakresem funkcji. Ścieżka aktywna odpowiada potrzebom klientów, którym zależy na natychmiastowym dostępie do najnowszych funkcji i udoskonaleń, oraz jest jedyną ścieżką dostępną w przypadku nowo wprowadzonych urządzeń. Dzięki niej klienci są na bieżąco z ewoluującymi możliwościami urządzeń: wprowadzane są nowe cyberzabezpieczenia, które zwiększają bezpieczeństwo działania, a istniejące funkcje są na bieżąco doskonalone. Ścieżka aktywna AXIS OS pozwala pełniej wykorzystywać możliwości urządzeń bez ponoszenia dodatkowych kosztów nawet po upływie wielu lat od zakupu. Jeśli zgodność nie jest warunkiem koniecznym, warto korzystać z tej właśnie ścieżki przez możliwie najdłuższy czas.

Ścieżka wsparcia długoterminowego
Jeśli dla klienta ważna jest zgodność i spójność interfejsu API, z chwilą udostępnienia ścieżki wsparcia długoterminowego powinien ją wybrać. Ścieżka ta koncentruje się na zgodności wstecznej oraz udostępnia regularne aktualizacje zabezpieczeń i poprawki błędów. Główny nacisk położono w niej na zachowanie cyberbezpieczeństwa, a nie dostarczanie nowych funkcji zabezpieczających. Nie wprowadza się w niej też nowych funkcji, ale dąży do minimalizacji zmian w celu ograniczenia przerw w pracy. Ścieżka wsparcia długoterminowego jest odpowiednia dla klientów, którzy cenią zaufanie i jakość oraz chcą dysponować dobrze zintegrowanym systemem obejmującym komponenty podmiotów zewnętrznych. Każda ścieżka wsparcia długoterminowego jest obsługiwana przez 5 lat, przy czym ścieżki długoterminowe są wprowadzane co 24 miesiące, zgodnie z harmonogramem wydań ścieżek aktywnych. Wszystkie urządzenia z chwilą wycofania z oferty automatycznie przechodzą na ścieżkę wsparcia długoterminowego.

Na ilustracji pokazano ścieżkę aktywną AXIS OS w zestawieniu z wprowadzanymi na przestrzeni lat ścieżkami wsparcia długoterminowego. Mniej więcej co 24 miesiące powstaje nowa ścieżka wsparcia długoterminowego, a główna wersja systemu AXIS OS otrzymuje nowy, wyższy numer. Przykładowo w 2024 r. utworzymy nową ścieżkę wsparcia długoterminowego AXIS OS 2024, a następnie przejdziemy z obecnego systemu AXIS OS 11 na AXIS OS 12.



Cyberbezpieczeństwo w centrum uwagi

W systemie AXIS OS kwestie bezpieczeństwa są uwzględniane już na etapie prac projektowych. Model rozwoju zabezpieczeń Axis (Axis Security Development Model — ASDM) określa procesy i narzędzia, które ograniczają ryzyko powstawania luk w zabezpieczeniach podczas prac nad oprogramowaniem i na dalszych etapach.

Nasza sprzętowa platforma cyberbezpieczeństwa Axis Edge Vault zapewnia bezpieczny start i chronione przed ingerencją środowisko przechowywania załadowanych przez klienta kluczy kryptograficznych. Podstawowe oprogramowanie systemu AXIS OS składa się ze starannie przetestowanych komponentów open source. Natomiast każdemu wydaniu towarzyszy programowy wykaz materiałów, który dowodzi, że system AXIS OS jest aktualny i zawiera poprawki znanych luk.

AXIS OS ma także certyfikat zgodności ze standardem ETSI EN 303 645, który koncentruje się na bezpieczeństwie urządzeń brzegowych. Zgodność ze standardem FIPS 140 daje gwarancje, że AXIS OS spełnia wymogi najnowszych norm kryptograficznych określonych przez National Institutes of Technologies (NIST). I wreszcie jako zatwierdzony organ numeracji CVE przestrzegamy najlepszych praktyk z zakresu identyfikowania luk, zarządzania nimi oraz ich ujawniania.

Na kolejnych stronach bardziej szczegółowo opisano model rozwoju zabezpieczeń Axis, platformę Axis Edge Vault, zarządzanie lukami w zabezpieczeniach i koncepcję zunifikowanych zabezpieczeń.

Stworzony z myślą o bezpieczeństwie

Model rozwoju zabezpieczeń Axis (Axis Security Development Model — ASDM) zapewnia integrację cyberzabezpieczeń z całym cyklem prac nad oprogramowaniem. Opisuje on działania z zakresu bezpieczeństwa, które należy uwzględnić na poszczególnych etapach tworzenia oprogramowania. Celem tych działań jest ograniczenie luk — a także obniżenie kosztów — przez określenie bazowego poziomu cyberzabezpieczeń i zapewnienie niezbędnych wskazówek.

ASDM: autorski model Axis
Model rozwoju zabezpieczeń Axis nie jest standardową, gotową strukturą. Opracowaliśmy go samodzielnie po zapoznaniu się z wieloma standardami i platformami cyberbezpieczeństwa, takimi jak ISO 27001, IEC 62443, NIST, BSIMM i CMMC. Ich cechą wspólną jest uwzględnienie zabezpieczeń we wszystkich fazach prac rozwojowych. Wychodząc z tego założenia, dostosowaliśmy nasz model do naszej firmowej kultury, praktyk z zakresu tworzenia programowania i rodzaju dostarczanych produktów.

Zestaw narzędzi ASDM
Zestaw narzędzi ASDM zaleca szereg działań, które odpowiadają różnym problemom z zakresu bezpieczeństwa. Są to na przykład: ocena ryzyka, modelowanie zagrożeń, testowanie modelu zagrożeń, statyczna analiza kodu, skanowanie luk i ocena dostawców. Udział zespołów programistycznych w konkretnych działaniach zależy od rodzaju tworzonego oprogramowania. Nadrzędnym celem jest zapewnienie cyberbezpieczeństwa, a nie tylko zgodności z określonym procesem.

Zalety wiedzy pochodzącej z zewnątrz
Za większość kluczowych prac związanych z bezpiecznym tworzeniem oprogramowania odpowiada dział badawczo-rozwojowy Axis i nasi inżynierowie oprogramowania. Mamy jednak świadomość, że może się nam przydać wiedza i doświadczenie innych podmiotów. Dlatego testy penetracyjne zlecamy wyspecjalizowanym firmom. Uruchomiliśmy także program nagród za wykryte błędy związany z systemem AXIS OS, w ramach którego oferujemy badaczom zabezpieczeń nagrody finansowe za pomoc w identyfikacji luk.

Nadzór | **Szkolenie** | **Spotkanie nt. ASDM** | **Ocena ASDM** | **Standardy bezpieczeństwa i zapewnianie zgodności**

Wymagania	Projektowanie	Wdrożenie	Weryfikacja	Wdrożenie
Ocena ryzyka	Modelowanie zagrożeń	Statyczna analiza kodu	Test modelu zagrożeń	Zarządzanie lukami
Ocena dostawców		Analiza składu oprogramowania	Zewnętrzny test penetracyjny	Zarządzanie incydentami
Prywatność danych			Skanowanie luk	Status zabezpieczeń produktu/rozwiązania
Ocena bezpieczeństwa komponentów open source			Wewnętrzna ocena zabezpieczeń	Program nagród za wykryte błędy

Wbudowane cyberzabezpieczenia

Ochrona od wewnątrz
Axis Edge Vault to nasza sprzętowa platforma cyberbezpieczeństwa. Stanowi ona solidny fundament, dzięki któremu urządzenia Axis są wiarygodną i niezawodną częścią sieci klientów. Ale ta zaawansowana platforma sprzętowa byłaby bezużyteczna bez systemu operacyjnego pozwalającego w pełni wykorzystać jej potencjał. System AXIS OS przy użyciu platformy Edge Vault zapewnia wzmocnione zabezpieczenia urządzeń brzegowych w każdych zastosowaniach.

Edge Vault obejmuje następujące funkcje:

Bezpieczne przechowywanie kluczy
Bezpieczny magazyn kluczy obejmuje kryptograficzne moduły obliczeniowe służące do bezpiecznego przechowywania kluczy kryptograficznych i wykonywania związanych z nimi obliczeń. Moduły te chronią tożsamość urządzenia i inne wrażliwe informacje przed nieautoryzowanym dostępem — nawet w przypadku naruszenia zabezpieczeń urządzenia. Kryptograficzne moduły obliczeniowe obejmują środowisko TEE (Trusted Execution Environment) wbudowane w procesor SoC (system-on-chip) oraz specjalny bezpieczny element lub moduł TPM 2.0 (Trusted Platform Module), które są odrębnymi układami umieszczonymi na płytce drukowanej.

Podpisany system operacyjny i bezpieczny start
Podpisany system operacyjny oznacza, że podpisujemy cyfrowo kod obrazu oprogramowania urządzenia. Połączenie funkcji podpisanego systemu operacyjnego i bezpiecznego startu sprawia, że urządzenia mogą pobierać i uruchamiać wyłącznie oryginalny system operacyjny AXIS OS. Wprowadza to dodatkową warstwę ochrony przed ingerencją w łańcuchach dostaw oprogramowania i sprzętu.

Identyfikator urządzenia Axis
Funkcja identyfikatora urządzenia Axis jest zgodna ze standardem IEEE 802.1AR oraz umożliwia bezpieczne identyfikowanie urządzeń i ich dodawanie do sieci. Identyfikator ten jest swego rodzaju certyfikatem oryginalności każdego wyprodukowanego urządzenia Axis.

Zaszyfrowany system plików
Szyfrowanie systemu plików chroni dane systemu plików przed ekstrakcją i ingerencją, gdy urządzenie nie jest używane, na przykład podczas transportu od integratora systemu do klienta.

Podpisany materiał wizyjny
Funkcja podpisanego materiału wizyjnego umożliwia weryfikację autentyczności zarejestrowanego materiału i daje pewność, że nie został on zmanipulowany.

Platforma cyberbezpieczeństwa Axis Edge Vault

Kryptograficzne moduły obliczeniowe	Cechy	Zastosowania
Bezpieczny element TPM 2.0	Bezpieczny start	Wiarygodna tożsamość urządzenia
Zabezpieczenia procesora SoC (TEE)	Podpisany system operacyjny	Bezpieczne przechowywanie kluczy
	Identyfikator urządzenia Axis	Wykrywanie ingerencji w materiał wizyjny
	Bezpieczny magazyn kluczy	Ochrona łańcucha dostaw
	Podpisany materiał wizyjny	
	Zaszyfrowany system plików	

*Uwaga: nie wszystkie modele urządzeń obsługują pełen zestaw funkcji platformy Axis Edge Vault. Aby sprawdzić funkcje obsługiwane przez określony produkt, należy się zapoznać z kartą jego danych technicznych lub skorzystać z selektora produktów Axis.

Zarządzanie lukami

Aby zminimalizować ryzyko, na które są narażeni klienci, przestrzegamy najlepszych praktyk branżowych z zakresu przejrzystego zarządzania lukami w zabezpieczeniach i reagowania na nie.

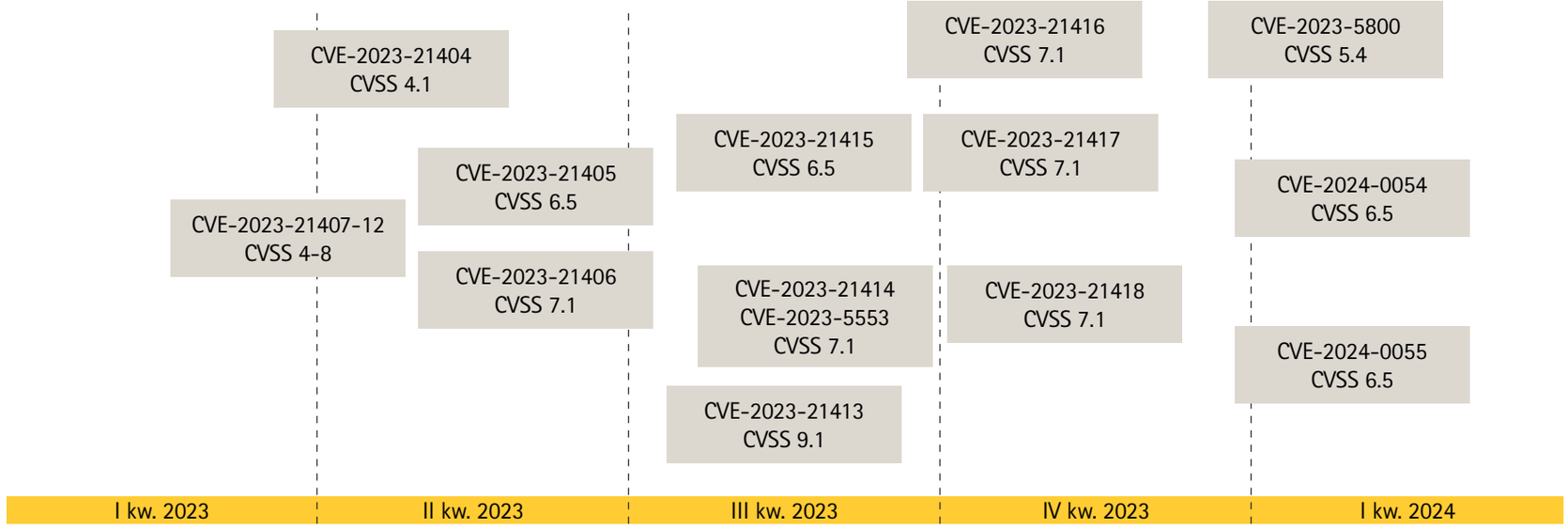
Najlepsze w swojej klasie zarządzanie lukami
Nie sposób zagwarantować, że produkty i usługi dostarczane przez Axis będą w całości wolne od luk czy słabych punktów. Nie dotyczy to jedynie naszej firmy, ale odnosi się do każdej aplikacji aplikacji i usługi. Prowadzimy jednak skoordynowane działania mające na celu identyfikację potencjalnych luk i łagodzenie ich skutków na każdym etapie prac, co ogranicza ryzyko związane z wdrażaniem produktów i usług Axis w środowisku klienta.

Organ numeracji CVE
Axis jest organem numeracji CVE. Przystąpiliśmy do programu CVE, aby współpracować z podobnie rozumującymi firmami na rzecz lepszego zarządzania lukami w zabezpieczeniach. Harmonizujemy sposób obsługi, ujawniania i usuwania luk z międzynarodowymi ramami opracowanymi przez tę organizację non-profit i z naszymi ogólnodostępnymi zasadami zarządzania lukami.

Przejrzyste, rzetelne zarządzanie
Axis korzysta z dobrze znanego systemu oceny luk CVSS (Common Vulnerability Scoring System), oceniając luki związane z własnym kodem lub z kodem open source pochodzącym od podmiotów zewnętrznych. Luki w kodzie open source są oceniane na podstawie stopnia ich wpływu na produkty Axis w przypadku zastosowania zaleceń opartych na najlepszych praktykach. Subskrybując usługę Axis Security Notification Service, można otrzymywać informacje na temat luk i innych kwestii związanych z zabezpieczeniami produktów Axis.

Współpraca z badaczami i organizacjami z obszaru zabezpieczeń
Doceniamy pracę badaczy zabezpieczeń i organizacji prowadzących badania z zakresu bezpieczeństwa, które kontaktują się z nami w celu zgłoszenia wykrytych luk. Chętnie je ujawniamy i tworzymy odpowiednie poprawki. Uważamy, że niezależnie od sposobu wykrycia luk ważne jest prawidłowe i przejrzyste postępowanie z nimi, które obejmuje etyczny i odpowiedzialny proces ich ujawniania.

Luki w systemie AXIS OS



Luki ujawnione przez Axis w odniesieniu do systemu AXIS OS.

Kompleksowe środowisko zabezpieczeń

W urządzeniach sieciowych korzystających z systemu AXIS OS elementy sprzętowe i programowe współpracują ze sobą, aby umożliwić klientom bezpieczną eksploatację urządzeń, związanych z nimi usług oraz systemów, do których są podłączone. Kompleksowa, wielowarstwowa ochrona rozpoczyna się od fundamentu zabezpieczeń i sprzętowej platformy bezpieczeństwa oraz rozciąga się aż do oprogramowania. Te warstwowe, pogłębione mechanizmy obronne zapewniają ochronę urządzeń korzystających z systemu AXIS OS. Zwiększają one ogólne bezpieczeństwo danych, aplikacji i procesów.

Dlatego możesz mieć pewność, że niezależnie od funkcji, którą pełni dane urządzenie Axis, dostępne są ochrona i bezpieczna łączność, które umożliwiają prawidłową i bezpieczną integrację z systemami innych producentów.

Kontrola dostępu

Zarządzanie kontrolą dostępu
Zarządzanie urządzeniami na poziomie użytkownika lokalnego ze wskaźnikiem złożoności hasła
Zarządzanie urządzeniami na poziomie użytkownika sfederowanego za pośrednictwem mechanizmu OpenID Connect (kod autoryzacji zgodnie z RFC6749, 1.3.1), który zapewnia integrację z ADFS udostępniającą takie funkcje jak wymuszanie złożoności hasła, rotacja, automatyczna blokada konta, uwierzytelnianie wieloskładnikowe, upoważnienia Microsoft AD

Prywatność
Korzystanie z danych diagnostycznych
Minimalistyczne podejście do ilości przechowywanych danych związanych z klientem

Aplikacja

Zabezpieczenia aplikacji
Zabezpieczenia aplikacji oparte na TLS (MQTT, SFTP, NTS, HTTPS, WebRTC)
Strumieniowe przesyłanie zaszyfrowanego materiału wizyjnego (RTSPS/SRTP, HTTPS), bezpieczny zdalny dziennik systemowy

System operacyjny

Szyfrowanie i ochrona danych
OpenSSL 1.1.1 i 3.0
Infrastruktura PKI i kryptografia z certyfikatem X.509
Transport Layer Security (TLS 1.2/TLS 1.3)
Szyfrowanie kart SD (AES-XTS-Plain64, 256 bitów)
Zaszyfrowany system plików (AES-XTS-Plain64, 256 bitów)
Podpisany materiał wizyjny

Zabezpieczenia domyślne
Domyślnie włączony protokół HTTPS
Ochrona przed atakami brute force
Zapora oparta na hoście
Network Time Security (NTS)
Wyłączenie niezabezpieczonych wersji TLS
Wyłączenie portu debugowania/UART

Zabezpieczenia sieci przedsiębiorstwa
IEEE 802.1X (kontrola dostępu do sieci)
IEEE 802.1AR (bezpieczna tożsamość urządzenia)
IEEE 802.1AE (zabezpieczenia MAC, MACsec)

System operacyjny AXIS OS
System operacyjny oparty na Linuksie, który zawiera ponad 95% standardowych komponentów programowych typu open source, takich jak OpenSSL, Apache, Curl i inne.
Ścieżka aktywna na potrzeby rozwoju funkcji oraz 5-letnie ścieżki wsparcia długoterminowego oferowane z myślą o integracji z produktami innych firm i zgodności wstecznej.

Zabezpieczenia na poziomie układów półprzewodnikowych

Sprzętowe źródło zaufania
Zabezpieczenia procesora SoC (system-on-chip) opartego na architekturze ARM
Trusted Execution Environment (TEE/OP-TEE)
Trusted Platform Module (TPM 2.0), bezpieczny element

Bezpieczne przechowywanie kluczy
Chronione przed ingerencją przechowywanie i stosowanie kluczy kryptograficznych, takich jak przesłane przez klienta klucze prywatne, klucze do podpisywania materiału wizyjnego i identyfikator urządzenia Axis.

Fundament zabezpieczeń

Model rozwoju zabezpieczeń Axis
Model rozwoju zabezpieczeń Axis (ASDM)
Zewnętrzne testy penetracyjne
Program nagród za wykryte błędy we współpracy z Bugcrowd
Programowy wykaz materiałów

Zgodność z przepisami
Common Criteria EAL
FIPS 140
ETSI EN 303 645

Wiarygodna tożsamość urządzenia
Platforma cyberbezpieczeństwa Axis Edge Vault
Bezpieczny start z podpisanym systemem operacyjnym (podpisywanie kodu)
Identyfikator urządzenia Axis (IEEE 802.1AR)

Integracja na światowym poziomie

Integracja jest kluczową cechą produktów Axis. Oferujemy solidne i spójne interfejsy API, które sprzyjają łatwej integracji w szerokiej gamie zastosowań.

Dzięki temu klienci mogą tworzyć kompleksowe rozwiązania, które w pełni wykorzystują potencjał urządzeń Axis.

Na kolejnych stronach bardziej szczegółowo opisano VAPIX (nasz własny interfejs API), nasze działania związane z ONVIF oraz IoT, modularyzację platformy poprzez ACAP, a także automatyzację w obszarze integracji sieci.

Atuty Axis: VAPIX, ONVIF, IoT i integracja z chmurą

W związku z dynamicznym rozwojem obszarów dozoru i łączności Axis Communications oferuje pakiet rozwiązań integracyjnych, które na nowo definiują branżowe standardy.

VAPIX: tradycja rozszerzalności
VAPIX, nasz otwarty interfejs API, jest znakomitą ilustracją naszego przywiązania do innowacji. Dzięki obsłudze wywołań HTTP GET i POST oraz formatów JSON i XML umożliwia on programistom łatwe tworzenie indywidualnych rozwiązań. Oferując najobszerniejszą i najspójniejszą bibliotekę dostępną na rynku, VAPIX jest pionierskim rozwiązaniem w zakresie otwartej integracji produktów sieciowych Axis, wcześniejszym nawet od standardu ONVIF.

ONVIF: standardy branżowe oparte na współpracy
Axis współdziała z otwartym forum branżowym ONVIF, aby pobudzać ducha współpracy, który sprzyja rozwojowi branży oraz zapewnia klientom kompleksowe i kompatybilne rozwiązania. ONVIF udostępnia i promuje znormalizowane interfejsy, które pozwalają uzyskać zgodność operacyjną różnych produktów zabezpieczających opartych na protokole IP. Upraszcza to integrację naszym partnerom, ponieważ zapewnia bezproblemową funkcjonowanie urządzeń Axis w różnego rodzaju systemach.

IoT: śmiałe spojrzenie w przyszłość
W sytuacji, gdy Internet rzeczy (IoT) zmienia oblicze łączności, urządzenia Axis stanowią ważny element ewoluującego ekosystemu. Axis obsługuje takie protokoły jak MQTT, które są stosowane w innowacyjnych rozwiązaniach IoT. Urządzenia Axis są nie tylko połączone, ale też stanowią część prężnego środowiska IoT.

Integracja z chmurą: podniebne innowacje
W dziedzinie łączności cyfrowej Axis aktywnie bada możliwości integracji z chmurą przy użyciu interfejsów API zaprojektowanych pod kątem płynnego współdziałania z takimi popularnymi platformami jak Microsoft Azure i Amazon Web Service (AWS). W miarę rozwoju technologii będziemy wprowadzać obsługę kolejnych rozwiązań chmurowych, takich jak MQTT na potrzeby przesyłania komunikatów oraz WebRTC do celów strumieniowego przesyłania materiału wizyjnego i dźwięku. Naszym celem jest umożliwienie użytkownikom jak najpełniejszego wykorzystania technologii chmurowych.

Modularyzacja platformy poprzez ACAP

Jedną z najważniejszych cech systemu AXIS OS jest umożliwienie modularyzacji za pośrednictwem platformy ACAP (AXIS Camera Application Platform). ACAP umożliwia programistom tworzenie i wdrażanie aplikacji oraz usług, takich jak narzędzia do analizy materiału wizyjnego czy dźwięku i inne specjalistyczne rozszerzenia odpowiadające wymaganiom biznesowym. Aplikacje ACAP są niezależne od podstawowych funkcji systemu AXIS OS oraz mogą być instalowane, aktualizowane i usuwane bez wpływu na pozostałe elementy systemu. Ponadto aplikacje ACAP mogą się komunikować ze sobą i z systemami zewnętrznymi za pomocą standardowych protokołów i interfejsów API.

Skalowalność i wydajność
Platforma ACAP wykorzystuje architekturę mikrousług stosowaną w systemie operacyjnym urządzeń Axis. Każdą usługę można niezależnie skalować w górę lub w dół stosownie do zapotrzebowania i obciążenia. To poprawia ogólną wydajność i dostępność systemu oraz umożliwia efektywne wykorzystywanie i alokowanie zasobów.

Adaptacja i dostosowywanie
Platforma ACAP zwiększa wszechstronność oraz możliwość adaptacji i dostosowywania urządzeń Axis, ponieważ obsługują one różne rodzaje integracji, narzędzi analitycznych i urządzeń. Ponadto ACAP ogranicza powiązanie, a zwiększa spójność platformy, ponieważ każda aplikacja jest luźno powiązana z systemem AXIS OS i bardzo spójna sama w sobie.

Łatwość konserwacji i niezawodność
Każdą usługę można testować, monitorować i debugować niezależnie oraz w sposób odizolowany. To upraszcza rozwiązywanie problemów i diagnostykę oraz zwiększa odporność systemu i jego tolerancję na błędy, a także sprawia, że AXIS OS wyróżnia się pod względem jakości oprogramowania.

AXIS OS dla zespołów IT

Określenie właściwej automatyzacji i integracji z infrastrukturą IT zapewnia odpowiednie mechanizmy kontroli bezpieczeństwa oraz może się przełożyć na oszczędności czasu i pieniędzy. Ponadto minimalizowana jest niepotrzebna złożoność systemu. Poniżej wymieniono wybrane korzyści wynikające z integracji urządzeń i oprogramowania Axis z infrastrukturą IT przedsiębiorstwa:

> Minimalizacja złożoności systemu przez usunięcie odrębnych, fizycznych sieci przygotowawczych urządzeń

> Redukcja kosztów dzięki automatyzacji procesów dodawania urządzeń i zarządzania nimi

> Możliwość korzystania z mechanizmów kontroli bezpieczeństwa sieci opartych na zerowym zaufaniu, takich jak IEEE 802.1X, IEEE 802.1AR

> Zwiększenie ogólnego bezpieczeństwa sieci dzięki wprowadzeniu szyfrowania danych na bazowym poziomie przy pomocy standardu IEEE 802.1AE MACsec; w ten sposób urządzenie Axis przyczynia się np. do poprawy bezpieczeństwa sieci

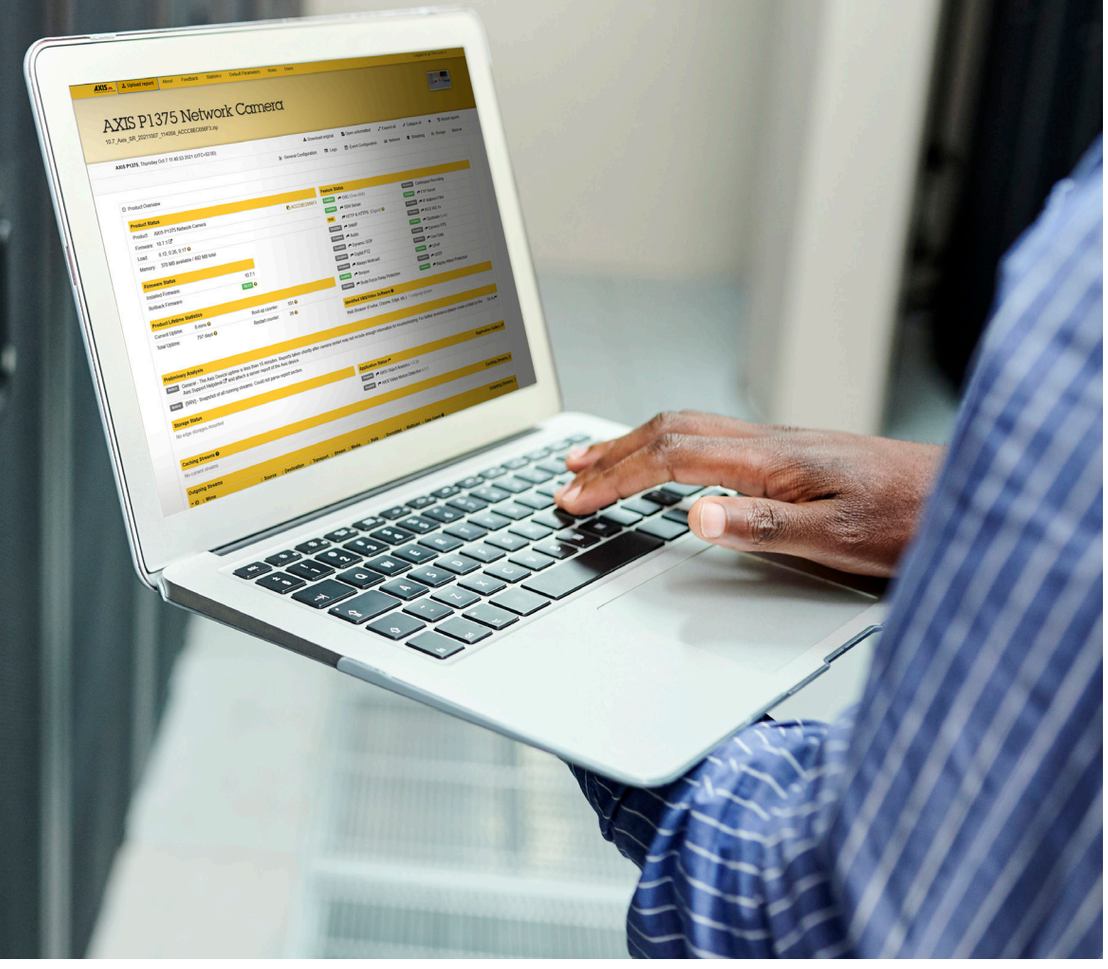
> Monitorowanie urządzenia Axis za pośrednictwem takich standardowych protokołów jak Remote Syslog, umożliwiających np. monitorowanie dziennika i stanu technicznego

Bezpieczne sieci oparte na zasadzie zerowego zaufania

Tworzenie konwergentnych, bezpiecznych sieci opartych na zasadzie zerowego zaufania jest niezbędnym warunkiem wyeliminowania odizolowanych, niezależnie działających systemów. Integracja urządzeń Axis z infrastrukturą IT przedsiębiorstwa przy użyciu dobrze zdefiniowanych, otwartych protokołów i standardów sieciowych przekłada się na wyższy poziom bezpieczeństwa, niższe koszty konfiguracji i konserwacji oraz skuteczniejsze egzekwowanie zasad IT.

Korzyści dla działów IT

Działy IT odpowiadają za zabezpieczanie sieci IT, więc urządzenia Axis są dla nich korzystną propozycją. Produkty Axis są łatwiejsze w integracji, konserwacji i użytkowaniu za sprawą swojej wszechstronności, a także podobieństwa do rozwiązań IT zdefiniowanych przez otwarte, standardowe protokoły sieciowe IEEE i IETF oraz jednolite zasady projektowe. W sieciach klientów urządzenia Axis są niczym „wiarygodni obywatele", którzy przyczyniają się do poprawy bezpieczeństwa.



Porozmawiajmy

System AXIS OS sprawia, że na urządzeniach Axis można polegać. To dzięki niemu oferują one tak znakomitą jakość obrazu i dźwięku oraz inne korzyści.

System ten został specjalnie zaprojektowany, aby spełniać najważniejsze kryteria dotyczące urządzeń sieciowych, do których należą długoterminowa wartość, wysokie standardy cyberbezpieczeństwa i łatwość integracji.

Z przyjemnością porozmawiamy z Tobą na temat tego, jak urządzenia Axis mogą wnieść nową wartość do Twojej firmy lub organizacji.

Zachęcamy do kontaktu już dziś!

Zapraszamy też zapoznania się z naszymi urządzeniami na stronie axis.com

O firmie Axis Communications

Axis wspiera rozwój inteligentnego oraz bezpiecznego świata przez tworzenie rozwiązań umożliwiających poprawę bezpieczeństwa i efektywności biznesowej. Jako firma zajmująca się technologiami sieciowymi oraz lider branży, Axis oferuje rozwiązania z zakresu dozoru wizyjnego, kontroli dostępu, systemów domofonowych i systemów audio. Ich rozszerzeniem i uzupełnieniem są inteligentne aplikacje analityczne oraz wysokiej jakości szkolenia.

Axis zatrudnia około 4000 pracowników w ponad 50 krajach oraz współpracuje z partnerami z obszaru technologii i integracji systemów na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma została założona w 1984 roku i ma swoją siedzibę w Lund w Szwecji.