W Maxto ITS łączymy technologie, ludzi, procesy
i systemy w spójną oraz bezpieczną całość.
Tworzymy rozwiązania IT, które rozwijają biznes
i wzmacniają konkurencyjność firm.

MAXTOITS
Future is Possible

Cybersecurity

MAXTO ITS
Future is Possible

Maxto ITS

W Maxto ITS łączymy technologie, ludzi, procesy i systemy w spójną oraz bezpieczną całość. Tworzymy rozwiązania IT, które rozwijają biznes i wzmacniają konkurencyjność firm.

Czy wiesz, że:

x250

Polskie firmy są celem ataków hakerskich ponad 250 razy dziennie

Źródło: Dane Check Point Software Technologies

+126%

W pierwszym kwartale 2025 roku, liczba ataków ransomware wzrosła o 126% w stosunku do roku ubiegłego

Źródło: Dane Ministerstwa Cyfryzacji

58%

W Polsce w 2024 roku odnotowano 58% wzrost liczby incydentów bezpieczeństwa w sektorze publicznym

Źródło: Dane Ministerstwa Cyfryzacji

Oferta cyberbezpieczeństwa od Maxto ITS

Od fundamentów po najbardziej zaawansowane rozwiązania.
Zabezpiecz firmę przed zagrożeniami cyfrowymi dzięki zaawansowanym rozwiązaniom IT

05 Dojrzałe cyberbezpieczeństwo

- Resilience & Compliance (NIS2, DORA, KSC)
- Integracja wszystkich warstw w spójną architekturę IT/OT
- Business Continuity (BCP)

04 Proaktywna obrona i ciągłość biznesu

- Testy odporności
- Incident Response
- Digital Forensic
- Bezpieczeństwo OT (Claroty)
- SOC / MDR

03 Widoczność i kontrola

- Zarządzanie podatnościami
- SIEM / SOAR
- Monitoring sieci (NDR)
- Log Management

02 Ochrona danych i użytkowników

- Backup & „Cyfrowy bunkier”
- Bezpieczeństwo poczty e-mail
- Endpoint Security (EDR & XDR)
- PAM

01 Fundamenty bezpieczeństwa

- NGFW
- Segmentacja sieci
- NAC (Network Access Control)
- Active Directory
- HA (High Availability)

01 FUNDAMENT BEZPIECZEŃSTWA

NGFW (Next Generation Firewall)
Zaawansowany firewall łączący tradycyjną kontrolę ruchu z inspekcją aplikacji, wykrywaniem zagrożeń i integracją z systemami bezpieczeństwa w celu skutecznej ochrony sieci.

Segmentacja sieci
Podział infrastruktury LAN na strefy bezpieczeństwa i separację z siecią SAN, realizowany w architekturze Two-Tier z kontrolą dostępu przez 802.1x/NAC.

NAC
Oprogramowanie pozwalające na zabezpieczenie dostępu do sieci korporacyjnej. Głównymi zadaniami są uwierzytelnienie, autoryzacja i monitorowanie. W wyniku weryfikacji urządzenia znajdujące się w sieci LAN uzyskują zgodę lub odmowę dostępu do sieci, przy jednoczesnym wymuszeniu polityk bezpieczeństwa.

Active Directory
Centralny system zarządzania tożsamościami i uprawnieniami użytkowników, kluczowy dla kontroli dostępu i ochrony zasobów w środowisku IT.

HA (High Availability)
Wysoka dostępność systemu oparta na klastrach HA i redundancji, zapewniająca minimalizację przestojów dzięki automatycznemu przełączaniu usług. FT (Fault Tolerance) – odporność na awarie, realizowana m.in. przez Metro Cluster, umożliwiająca nieprzerwane działanie systemów i dostęp do danych.

02 OCHRONA DANYCH I UŻYTKOWNIKÓW

Backup & cyfrowy bunkier
Backup umożliwia odzyskanie danych utraconych na skutek awarii, nieumyślnej modyfikacji, nieautoryzowanego dostępu itp. Cyfrowy bunkier to system ochrony danych oparty na izolowanej, zabezpieczonej infrastrukturze tworzenia i przechowywania kopii zapasowych w trzeciej, niezależnej lokalizacji (cyfrowym bunkrze), zapewniający ciągłość działania i odtworzenie środowiska po awarii lub ataku

Bezpieczeństwo poczty e-mail
Ochrona systemu komunikacji przed złośliwym oprogramowaniem i phishingiem poprzez zaawansowane filtrowanie SPAMu, skanowanie załączników i wielopoziomową analizę wiadomości.

Endpoint Security (EDR&XDR)
Systemy wykrywania i reagowania na zagrożenia: EDR chroni urządzenia końcowe w czasie rzeczywistym, a XDR rozszerza monitoring na całą infrastrukturę IT/OT, integrując dane z sieci, serwerów i chmury dla kompleksowej ochrony i szybkiego reagowania na incydenty.

PAM
System kontroli i monitorowania dostępu uprzywilejowanego, który zabezpiecza konta administracyjne, minimalizuje ryzyko nadużyć i umożliwia ścisłą kontrolę działań użytkowników z najwyższymi uprawnieniami.

03 ZARZĄDZANIE PODATNOŚCIAMI

Zarządzanie podatnościami
Proces identyfikacji, oceny i eliminacji luk w systemach IT/OT, pozwalający minimalizować ryzyko ataków i utrzymanie środowiska w stanie bezpiecznym.

SIEM/SOAR
Zintegrowane systemy bezpieczeństwa: SIEM zbiera i analizuje logi w czasie rzeczywistym w celu wykrywania zagrożeń, a SOAR automatyzuje reagowanie na incydenty, usprawniając procesy ochrony infrastruktury IT/OT.

Monitoring sieci (NDR)
Monitoruje ruch sieciowy w czasie rzeczywistym, wykrywa anomalie oraz zagrożenia i koreluje je z innymi źródłami bezpieczeństwa. Umożliwia także analizę incydentów i automatyczne reakcje, pomagając szybko wykrywać i ograniczać skutki ataków.

Log Management
Proces centralnego zbierania, normalizacji, przechowywania i analizy logów z systemów IT/OT, aplikacji oraz urządzeń sieciowych w celu wykrywania incydentów bezpieczeństwa. Umożliwia on korelację zdarzeń, szybkie reagowanie na zagrożenia oraz spełnienie wymagań audytowych i regulacyjnych.

04 PROAKTYWNA OBRONA I CIĄGŁOŚĆ BIZNESU

Testy odporności

Systematyczne sprawdzanie bezpieczeństwa infrastruktury poprzez symulowanie ataków i analizę podatności.

Incident Response

Ustrukturyzowany proces wykrywania, analizy, ograniczania i usuwania skutków incydentów cyberbezpieczeństwa w celu szybkiego przywrócenia ciągłości działania systemów.

Digital Forensic

Specjalistyczny obszar cyberbezpieczeństwa obejmujący zabezpieczanie i analizę danych cyfrowych w celu odtworzenia przebiegu incydentu oraz identyfikacji jego źródła.

Bezpieczeństwo OT (Claroty)

Rozwiązania firmy Claroty monitorujące i chroniące sieci przemysłowe, wykrywające zagrożenia w systemach sterowania i automatyki (ICS/SCADA) oraz umożliwiające bezpieczne zarządzanie urządzeniami OT.

SOC/MDR

SOC (Security Operations Center) to centrum monitorowania i analizy zagrożeń w czasie rzeczywistym, a MDR (Managed Detection & Response) to usługa zarządzanego wykrywania i reagowania na incydenty (potocznie nazywanego wirtualnym SOC), zapewniająca kompleksową ochronę i wsparcie eksperckie w reagowaniu na incydenty

05 DOJRZAŁE CYBERBEZPIECZEŃSTWO

Resilience & Compliance (NIS2, DORA, KSC)

Działania zapewniające odporność infrastruktury i zgodność z regulacjami prawnymi, takimi jak NIS2, DORA czy KSC, poprzez wdrażanie standardów bezpieczeństwa, procedur ciągłości działania i mechanizmów raportowania.

Integracja wszystkich warstw w spójną architekturę IT/OT

Łączenie wszystkich warstw infrastruktury IT i OT w spójną architekturę, umożliwiające centralne zarządzanie, monitorowanie i ochronę całego środowiska technologicznego.

Business Continuity (BCP)

Proces planowania i wdrażania procedur oraz mechanizmów, które zapewniają nieprzerwane działanie kluczowych systemów i procesów IT w przypadku incydentów cyberbezpieczeństwa, ataków lub awarii infrastruktury.

Korzyści dla Twojej firmy

- Bezpieczeństwo i ciągłość działania
- Skalowalność i elastyczność
- Kompleksowość
- Optymalizacja kosztów
- Ciągłość monitorowania
- Bezpieczeństwo danych
- Wydajność i niezawodność
- Pełna kontrola
- Redukcja ryzyka

Gwarantujemy usługi na wysokim poziomie

Jakość naszej pracy jest potwierdzona certyfikatami.

IQNet Certified Management System · ISO 9001 · ISO 14001 · ISO 22301 · ISO 27001

Nasi partnerzy technologiczni

Jesteśmy Tytanowym Partnerem Dell Technologies

DELL Technologies Titanium Partner

Lenovo · Huawei · Veeam · Cisco · Alcatel-Lucent · HP · Aruba · Energy Logserver · Ascom · Fortinet · Sophos · Microsoft · Lexmark · Zebra · VMware by Broadcom · Fujitsu · Intel · Claroty

Zapraszamy do kontaktu

maxtoits.pl

Maxto ITS Sp. z o.o.
+48 12 266 39 69
info@maxtoits.pl