

Temat 8 .

Cenzura, normy,
przetwarzanie i analiza
informacji

dr inż. Michał Malinowski

<https://www.drmalinowski.edu.pl>

BEZPIECZEŃSTWO
INFORMACJI



- Cenzura Internetu
- Norma ISO/IEC 27001:2022
- Big Data
- Usługi chmurowe
- Internet rzeczy (IoT)
- OSINT
- SIEM, SOAR

Zadanie

Treść

Prezentacja zadania podczas zajęć.

Okolo 9 osób podczas zajęć

(0-2 pkt)



Cenzura Internetu

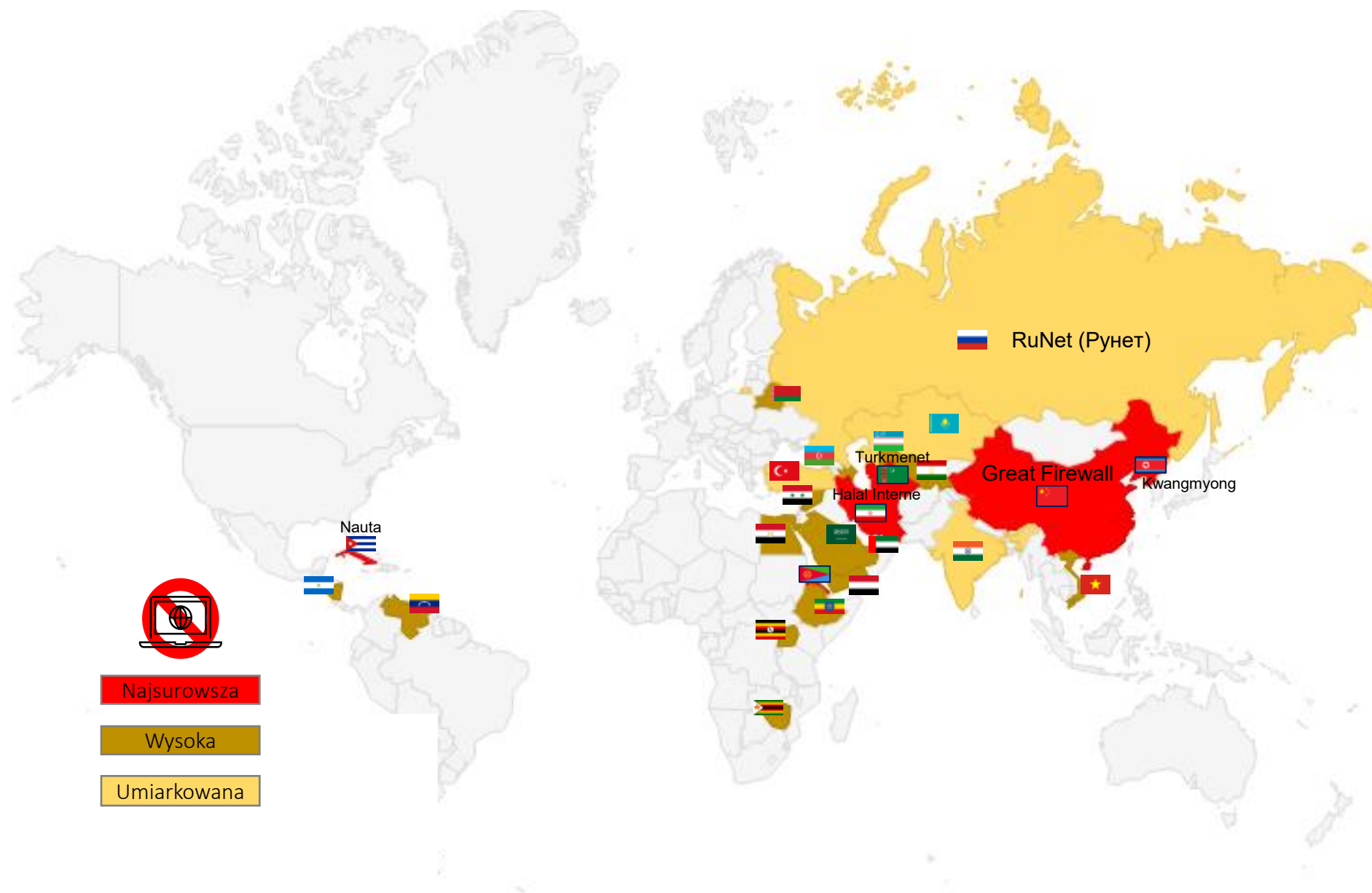
Cenzura Internetu

to kontrolowanie lub ograniczanie treści, do których użytkownicy mogą uzyskać dostęp w sieci.

Kto cenzuruje Internet?

- **Rządy państw** – Najbardziej widoczne i często krytykowane przypadki dotyczą krajów, gdzie władze ograniczają dostęp do informacji z powodów politycznych (np. blokowanie serwisów informacyjnych, mediów społecznościowych).
- **Firmy technologiczne** – Platformy takie jak Facebook, Google czy X (dawniej Twitter) stosują własne regulaminy, automatycznie usuwając treści uznane za szkodliwe lub nielegalne.
- **Dostawcy usług internetowych (ISP)** – Na żądanie państwa lub z własnej inicjatywy mogą blokować dostęp do określonych treści.
- **Instytucje prywatne** – Szkoły, uczelnie i firmy komercyjne filtrują treści dostępne przez ich sieci.

Cenzura Internetu



Cenzura Internetu

Blokowanie mediów społecznościowych

Państwo			Facebook	Platforma X	Instagram	YouTube	Snapchat	WhatsApp	TikTok	Telegram	LinkedIn
											
	Chiny	CN	X	X	X	X	X	X	X	X	X
	Korea Północna	KP	X	X	X	X	X	X	X	X	X
	Iran	IR	X	X		X	X		X	X	
	Erytrea	ER	X	X	X	X	X	X	X	X	X
	Turkmenistan	TM	X	X	X	X	X	X	X	X	X
	Kuba	CU	X	X		X					
	Uzbekistan	UZ	O	O	O	O	O	O	O	O	O
	Tadżykistan	TJ	O			O				O	
	Azerbejdżan	AZ	O	O	O	O		O	O	O	O
	Jemen	YE		O	O	O	O			O	O
	Uganda	UG	O	O							
	Etiopia	ET	O	O						O	
	Zimbabwe	ZW	O	O				O			
	Wenezuela	VE		X		O					
	Wietnam	VN								X	
	Białoruś	BY	O	O	O	O	O	O			
	Kazachstan	KZ	O	O	O	O	O	O	O		
	Rosja	RU	X	X	X			X	X		
	Indie	IN	O	O				O			
	Turcja	TR		O	O	O	O				

Cenzura Internetu

Odpowiedniki blokowanych mediów społecznościowych

Państwo		Zablokowany serwis	Krajowy odpowiednik
	Chiny Great Firewall	 Facebook	WeChat, Weibo
		 Twitter (X)	Weibo
		 Instagram	Weibo
		 YouTube	Youku Tudou
		 WhatsApp	WeChat
		 TikTok	Douyin
		 Telegram	WeChat
	Rosja RuNet (Рунет)	 Facebook	VKontakte
		 Instagram	VKontakte
		 Twitter (X)	VKontakte
		 YouTube	VK Video / RuTube
		 LinkedIn	VKontakte
	Iran Halal Internet (NIN)	 YouTube	Aparat
		 Facebook	Aparat i Cloob (dawniej Cloob)
		 Telegram	Soroush Plus
		 Instagram	Iransa
		 WhatsApp	iGap
	Wietnam	 WhatsApp	Zalo
		 Facebook	Gapo

Norma ISO/IEC 27001:2022

ISO/IEC 27001:2022 Technologia informacyjna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji - wymagania

<https://www.iso.org/standard/27001>

Cel normy:

- Zapewnienie systematycznego podejścia do identyfikacji, oceny i zarządzania ryzykiem dla informacji.
- Ustanowienie **Systemu Zarządzania Bezpieczeństwem Informacji (ISMS)**.

Zakres:

- Dotyczy wszystkich organizacji przetwarzających dane – niezależnie od wielkości i branży.



Norma ISO/IEC 27001:2022

Kluczowe elementy wdrożenia ISO/IEC 27001:2022

Analiza ryzyka:

- Zidentyfikowanie zasobów informacyjnych, zagrożeń i podatności.
- Oszacowanie ryzyka i decyzja o środkach kontrolnych.

Polityka bezpieczeństwa informacji:

- Zdefiniowanie celów, odpowiedzialności i zakresu ISMS.

Kontrole bezpieczeństwa (Załącznik A):

- Przykłady środków: kontrola dostępu, szyfrowanie, ciągłość działania, zarządzanie incydentami.

Audyty wewnętrzne i ciągłe doskonalenie:

- Koncepcja cyklu Deminga (PDCA): Plan – Działaj – Sprawdzaj – Poprawiaj.

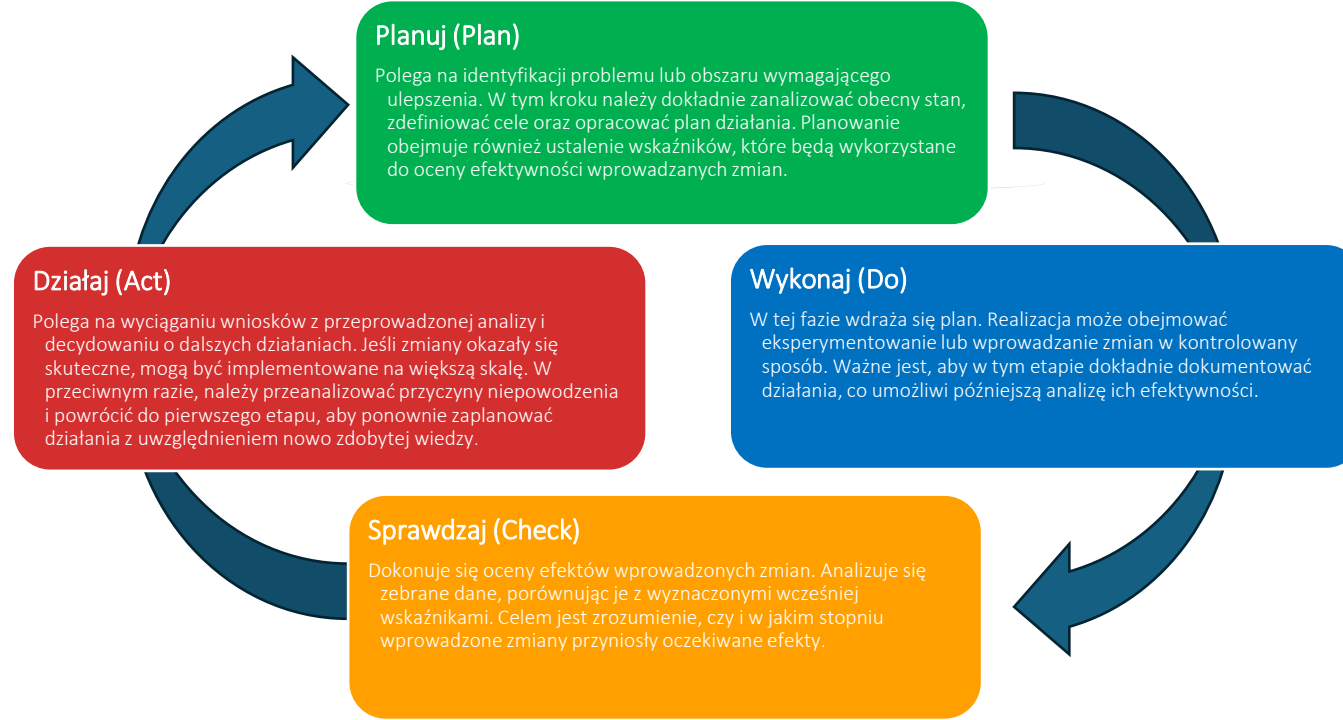
Dokumentacja i dowody zgodności:

- Rejestr ryzyk, raporty z audytów, plan ciągłości działania, dowody szkoleń.

Metodologia PDCA

Model Planuj-Wykonaj-Sprawdzaj-Działaj (PDCA) znany również jako cykl Deminga

to metodologia zarządzania ciągłym doskonaleniem procesów w organizacjach. Jego głównym celem jest systematyczne wprowadzanie zmian w celu poprawy efektywności i efektywności procesów.



Norma ISO/IEC 27001:2022

Inne powiązane normy – Rozszerzenie ISO/IEC 27001

Norma	Zakres	Kluczowe aspekty
ISO/IEC 27002:2022	Wskazówki do wdrożenia środków z 27001	Szczegółowe wytyczne dla 93 kontroli
ISO/IEC 27005	Zarządzanie ryzykiem bezpieczeństwa info.	Metodyki analizy i oceny ryzyka
ISO/IEC 27701	Zarządzanie prywatnością (PIMS)	Rozszerzenie 27001 o aspekty RODO/GDPR
ISO/IEC 27017	Bezpieczeństwo usług chmurowych	Obowiązki CSP i klienta
ISO/IEC 27018	Prywatność w chmurze (dane osobowe)	Zgodność z przepisami o ochronie danych

ISO/IEC 27001 stanowi **bazowy system zarządzania**, natomiast inne normy pozwalają na **dopasowanie go do specyfiki organizacji** – np. obsługi danych osobowych, środowisk chmurowych, sektora finansowego lub publicznego.

Big Data

Big Data

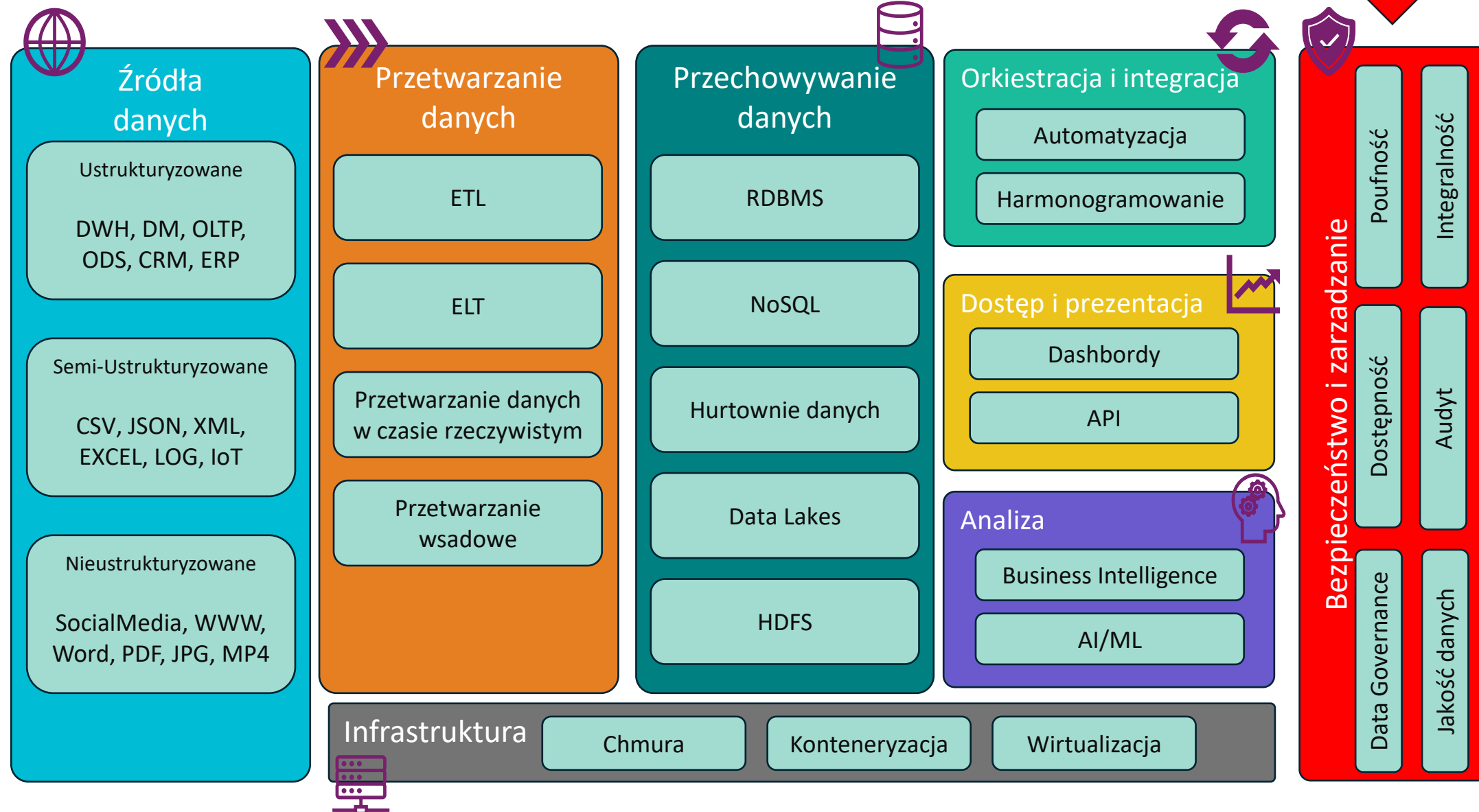
to termin określający **bardzo duże, szybko zmieniające się i różnorodne zbiory danych**, które **przekraczają możliwości tradycyjnych narzędzi do przetwarzania danych** w zakresie ich pozyskiwania, przechowywania, analizy i wizualizacji.

Wymiar (3V)	Opis
Volume	Ogromna ilość danych (terabajty, petabajty)
Velocity	Szybkość generowania i przetwarzania danych (np. dane strumieniowe)
Variety	Różnorodność formatów (strukturalne, niestukturalne, półstrukturalne)

W nowszych ujęciach dodaje się także:

- **Veracity** – wiarygodność i jakość danych,
- **Value** – wartość biznesowa wynikająca z analizy danych.

Architektura Big Data



Big Data

Zagrożenia bezpieczeństwa i prywatności

Zagrożenie	Opis
Profilowanie użytkowników	Tworzenie profili i ocen na podstawie danych behawioralnych
Naruszenie prywatności	Identyfikacja osób mimo anonimizacji lub pseudonimizacji
Luki w zabezpieczeniach infrastruktury	Brak wystarczających środków ochrony w systemach Big Data
Zautomatyzowane decyzje bez zgody użytkownika	Algorytmy podejmujące decyzje bez przejrzystości i możliwości sprzeciwu
Reidentyfikacja danych	Łączenie zbiorów danych umożliwiające odzyskanie tożsamości
Brak zgodności z przepisami (np. RODO)	Przetwarzanie danych niezgodnie z celem lub bez podstawy prawnej
Nieautoryzowany dostęp (zagrożenie wewnętrzne)	Nadużycie uprawnień przez pracowników lub osoby z dostępem
Brak kontroli nad źródłem i jakością danych	Ryzyko błędnych analiz na podstawie danych niekompletnych lub błędnych

Big Data

Metody ochrony danych

Maskowanie danych (Data Masking):

- Zastępowanie danych wrażliwych fikcyjnymi, ale realistycznymi wartościami.
- Używane w środowiskach testowych i analitycznych.

Pseudonimizacja:

- Zamiana identyfikatorów (np. PESEL, e-mail) na pseudonimy.
- Możliwość odtworzenia tożsamości przy pomocy klucza dodatkowego (zgodnie z RODO).

Anonimizacja:

- Usunięcie lub nieodwracalne przekształcenie danych osobowych.
- Trudniejsze w kontekście zbiorów powiązanych (np. dane geolokalizacyjne + czasowe).

Szyfrowanie:

- Zabezpieczenie danych w spoczynku (at-rest) i w transmisji (in-transit).
- Algorytmy: AES-256, RSA, homomorficzne szyfrowanie (dla analizy bez odszyfrowania).

Big Data

Rekomendacje

Podejście „privacy by design”:

- Prywatność uwzględniana już na etapie projektowania systemów Big Data.

Minimalizacja danych:

- Zbieraj tylko dane niezbędne do danego celu.

Audyty bezpieczeństwa i zgodność z RODO:

- Okresowa weryfikacja polityk i procedur (np. DPIA – ocena skutków dla ochrony danych).

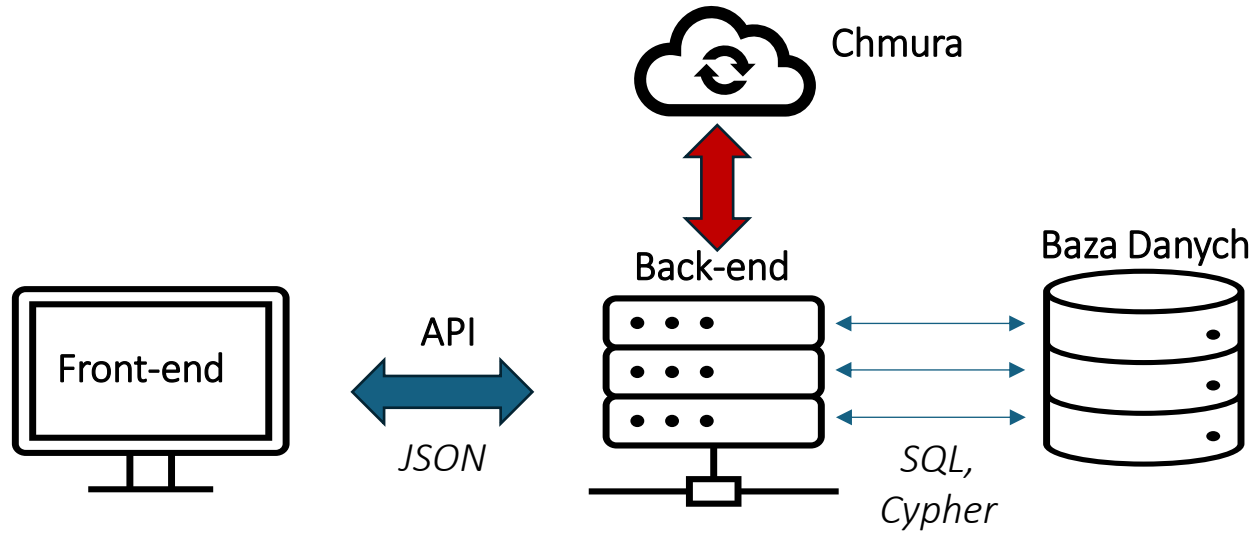
Ograniczenie dostępu:

- Kontrola ról i uprawnień (RBAC, ABAC).
- Logowanie i monitorowanie aktywności.

Usługi chmurowe

Usługi Chmurowe

to szeroka gama rozwiązań IT, które są dostarczane przez Internet. Pozwalają na elastyczne zarządzanie zasobami IT, oferując skalowalność, elastyczność i możliwość płatności na zasadzie pay-as-you-go.



Usługi chmurowe

Zastosowania

Przechowywanie i Backup Danych:

- Usługi chmurowe oferują bezpieczne i skalowalne magazyny danych, które mogą być używane do przechowywania dużych ilości informacji oraz tworzenia kopii zapasowych.

Hosting Aplikacji Webowych:

- Platformy chmurowe umożliwiają hostowanie aplikacji internetowych i mobilnych, zapewniając wysoką dostępność i skalowalność.

Analiza Danych:

- Narzędzia do analizy danych w chmurze umożliwiają przetwarzanie i analizowanie dużych zbiorów danych w celu uzyskania wartościowych wniosków.

Uczenie Maszynowe i AI:

- Usługi chmurowe oferują zaawansowane narzędzia do trenowania i wdrażania modeli uczenia maszynowego i sztucznej inteligencji.

DevOps:

- Platformy chmurowe dostarczają narzędzia do ciągłej integracji i ciągłego dostarczania (CI/CD), umożliwiając automatyzację procesów programistycznych.

Usługi chmurowe

Modele usług w chmurze

On-Premises

Organizacja samodzielnie posiada, zarządza i utrzymuje całą infrastrukturę IT, w tym serwery, sieci, systemy operacyjne, aplikacje i dane – w lokalnym centrum danych.

- Przykład: instytucje rządowe, banki, wojsko, przedsiębiorstwa o wysokich wymaganiach regulacyjnych

IaaS (Infrastructure as a Service):

Dostarcza podstawową **infrastrukturę IT**, taką jak serwery, sieci, pamięć masowa. Użytkownik ma pełną kontrolę nad systemami operacyjnymi, aplikacjami i danymi, ale fizyczny sprzęt jest zarządzany przez dostawcę usług.

- Przykład: Amazon Web Services (AWS), Microsoft Azure.

PaaS (Platform as a Service):

Oferuje **środowisko programistyczne**, które pozwala użytkownikom rozwijać, testować i zarządzać aplikacjami bez potrzeby zarządzania infrastrukturą. Użytkownicy mają dostęp do narzędzi programistycznych, a dostawca dba o zarządzanie serwerami, siecią i pamięcią.

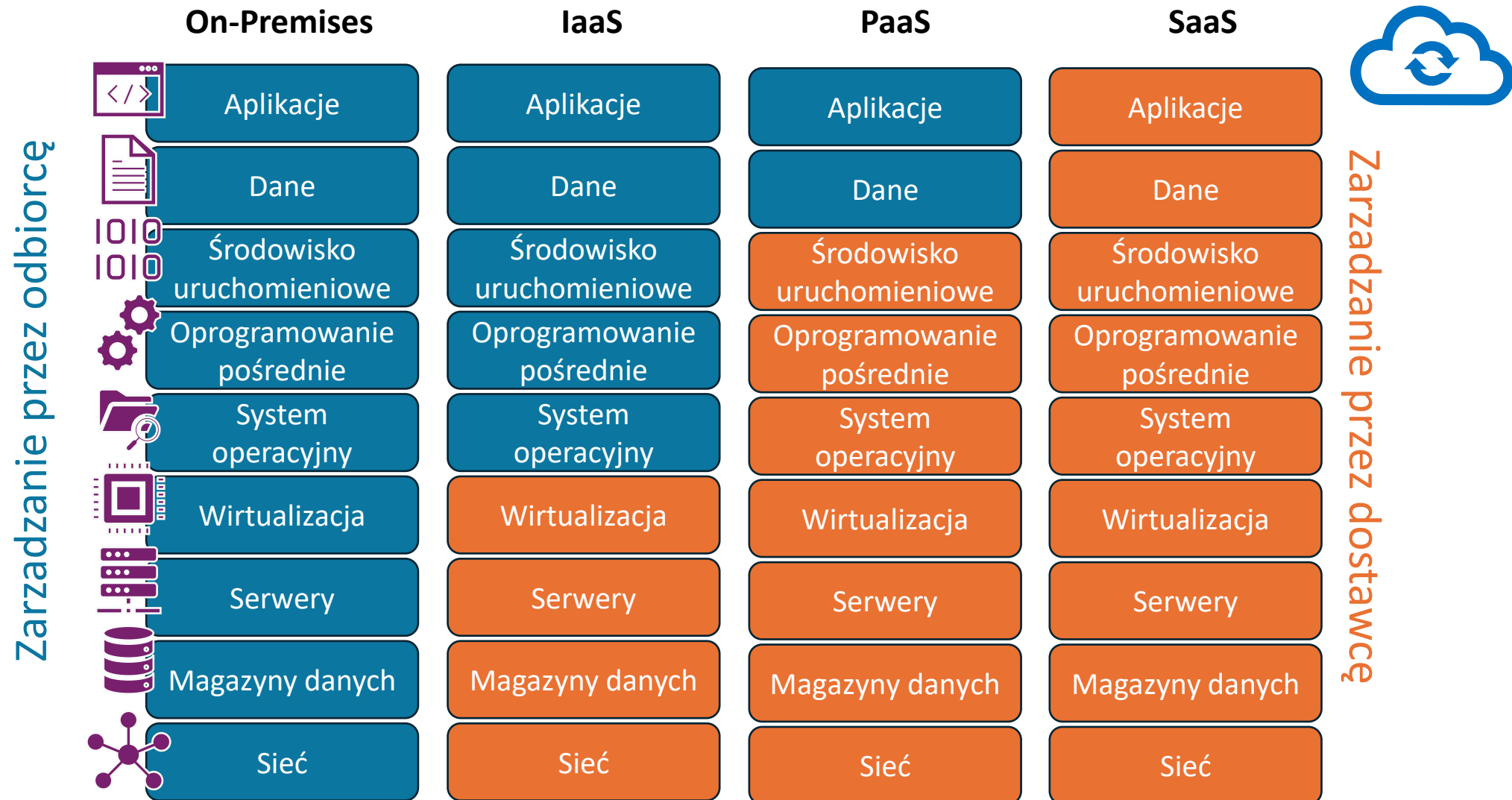
- Przykład: Google Colab, Heroku.

SaaS (Software as a Service):

Oferuje **gotowe aplikacje** dostarczane za pośrednictwem Internetu. Użytkownik ma dostęp do aplikacji przez przeglądarkę, a dostawca zarządza całą infrastrukturą, aktualizacjami i danymi.

- Przykład: Google Docs, Microsoft 365, Salesforce.

Modele dostarczania usług chmurowych



Usługi chmurowe

Zalety

Elastyczność i skalowalność:

- Można łatwo skalować w górę lub w dół, w zależności od bieżących potrzeb. Dzięki temu użytkownicy płacą tylko za to, co faktycznie wykorzystują.

Oszczędność kosztów:

- Eliminuje potrzebę inwestowania w drogi sprzęt oraz oprogramowanie. Płatności oparte są na subskrypcji lub użyciu zasobów, co zmniejsza początkowe koszty.

Dostępność i mobilność:

- Są dostępne z dowolnego miejsca z dostępem do Internetu, co umożliwia pracę zdalną i łatwy dostęp do danych z różnych urządzeń.

Bezpieczeństwo i kopie zapasowe:

- Oferuje zaawansowane zabezpieczenia danych, takie jak szyfrowanie, a także regularne tworzenie kopii zapasowych.

Praca grupowa

- Umożliwiają dzielenie zasobów i dokumentów różnym użytkownikom na różnych prawach dostępu (edycja, podgląd)

Usługi chmurowe

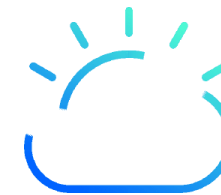
Przechowywanie danych w chmurze



Usługa	Cechy	Integracja	Pojemność darmowa	Płatne plany (przykładowo)
Google Drive	Przechowywanie dokumentów, zdjęć, filmów, możliwość współpracy w czasie rzeczywistym	Google Workspace, Android, Chrome OS	15 GB	100 GB za 8,99 PLN/mies., 2 TB za 46,99 PLN/mies.
Dropbox	Synchronizacja plików, współdzielenie folderów, dostęp do poprzednich wersji plików	Windows, macOS, Android, iOS	2 GB	2 TB za 11,99 EUR/mies.
Microsoft OneDrive	Integracja z Microsoft 365, synchronizacja plików, dostęp z urządzeń mobilnych	Microsoft 365, Windows, Office Online	5 GB	100 GB za 8,40 PLN/mies., 1 TB z subskrypcją Microsoft 365
iCloud	Automatyczna synchronizacja zdjęć, dokumentów i innych danych, dostęp do wszystkich urządzeń Apple	Apple ekosystem (iPhone, iPad, Mac)	5 GB	50 GB za 3,99 PLN/mies., 2 TB za 39,99 PLN/mies.

Usługi chmurowe

Główne platformy



Platforma	Opis	Główne Usługi
Amazon Web Services	AWS oferuje szeroki zakres usług chmurowych, od przetwarzania i magazynowania po sztuczną inteligencję i analitykę.	EC2, S3, RDS, Lambda, SageMaker
Microsoft Azure	Azure to kompleksowa platforma chmurowa Microsoftu, która oferuje usługi w zakresie przetwarzania, magazynowania, baz danych, IoT i wielu innych.	Virtual Machines, Azure SQL Database, Azure Functions, Azure DevOps
Google Cloud Platform	GCP dostarcza usługi chmurowe Google, w tym zaawansowane usługi analizy danych, uczenia maszynowego, przetwarzania i przechowywania danych.	Compute Engine, Cloud Storage, BigQuery, Cloud Functions
IBM Cloud	IBM Cloud oferuje zarówno publiczne, prywatne, jak i hybrydowe rozwiązania chmurowe, z usługami obejmującymi AI, blockchain, IoT i wiele innych.	IBM Cloud Kubernetes Service, IBM Watson, IBM Blockchain Platform
Oracle Cloud	Oracle Cloud oferuje szeroką gamę usług chmurowych, szczególnie skoncentrowanych na rozwiązaniach baz danych i aplikacjach biznesowych.	Oracle Autonomous Database, Oracle Cloud Infrastructure, Oracle Cloud Applications

Usługi chmurowe

Zagrożenia

Zagrożenie	Opis
Nieautoryzowany dostęp do danych	Brak kontroli ról, słabe hasła, brak MFA – ryzyko przejęcia konta
Błędy konfiguracji zasobów chmurowych	Publiczne zasoby, brak szyfrowania, nieprawidłowe reguły zapory
Zagrożenia wewnętrzne (insider threat)	Nadużycie uprawnień przez użytkowników lub personel usługodawcy
Ataki między tenantami (cross-tenant attacks)	Luka w izolacji danych między klientami (multi-tenancy)
Złośliwe oprogramowanie i podatności aplikacyjne	Wstrzyknięcia kodu, niezabezpieczone API, zainfekowane instancje
Utrata danych lub brak backupu	Usunięcie danych, awarie bez replikacji lub automatycznego odzysku
Brak zgodności z regulacjami	Naruszenia RODO, HIPAA, PCI – np. przez lokalizację danych lub brak zgody
Brak przejrzystości i vendor lock-in	Ograniczony wgląd w infrastrukturę, trudność zmiany usługodawcy

Usługi chmurowe

Zabezpieczenia

Zabezpieczenie	Opis
Szyfrowanie danych	Ochrona danych w spoczynku (at rest) i w transmisji (in transit); np. AES-256
Uwierzytelnianie wieloskładnikowe (MFA)	Zapobieganie przejęciu kont użytkowników przez dodanie drugiego czynnika logowania
Zarządzanie tożsamością i dostępem (IAM)	Kontrola ról i uprawnień, zasada najmniejszych przywilejów (least privilege)
Kopie zapasowe i replikacja danych	Ochrona przed utratą danych – automatyczny backup i replikacja między regionami
Monitorowanie i rejestrowanie zdarzeń (logi)	Detekcja anomalii, analiza incydentów, zgodność z politykami (SIEM, CloudTrail)
Segmentacja sieci i mikrosegmentacja	Izolowanie zasobów i ograniczanie rozprzestrzeniania się zagrożeń
Bezpieczne interfejsy API i bramy API	Kontrola dostępu do funkcji chmurowych, ograniczenie ataków typu injection
Zgodność i audyty bezpieczeństwa	Regularna weryfikacja zgodności z RODO, ISO 27001, SOC 2 i wewnętrznymi normami

Internet rzeczy (IoT)

Internet Rzeczy (IoT)

to dynamicznie rozwijająca się technologia, która łączy różnorodne urządzenia przez Internet, umożliwiając im komunikację i wymianę danych.

Ta sieć połączonych urządzeń wpływa na wiele aspektów codziennego życia oraz działalności gospodarczej.

Urządzenia IoT:

- Fizyczne obiekty wyposażone w czujniki, oprogramowanie i inne technologie umożliwiające zbieranie i wymianę danych z innymi urządzeniami przez Internet.

Czujniki i Aktory:

- Zbierają dane z otoczenia, takie jak temperatura, wilgotność, światło, ruch.

Połączenie Sieciowe:

- Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT.

Chmura i Serwery:

- Przechowywanie, przetwarzanie i analiza danych z urządzeń IoT.

Oprogramowanie i Aplikacje:

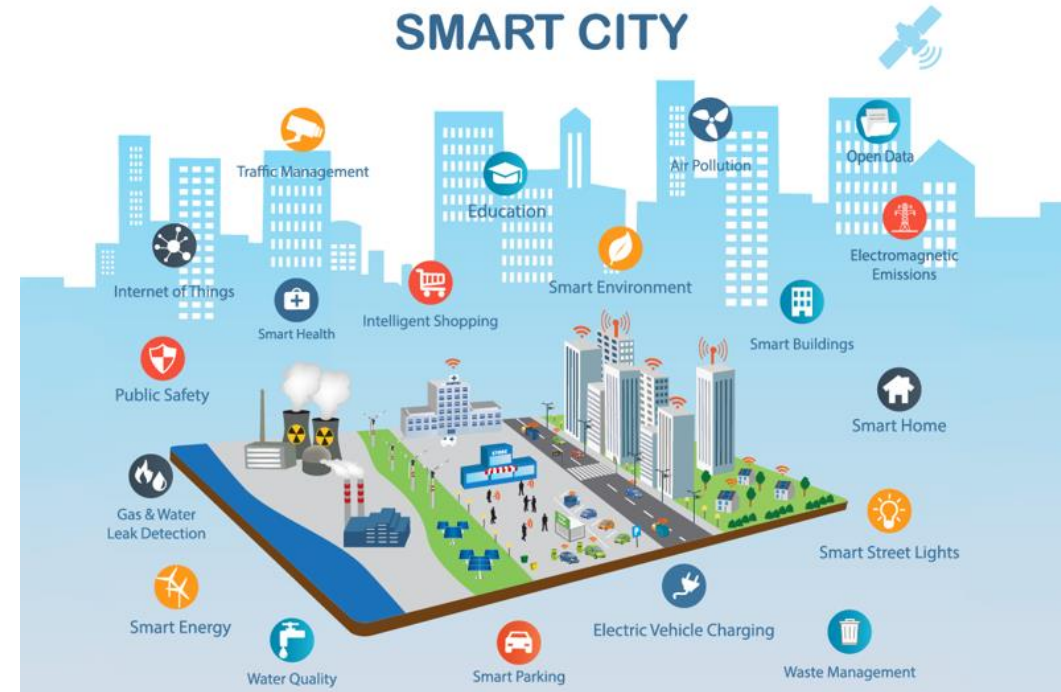
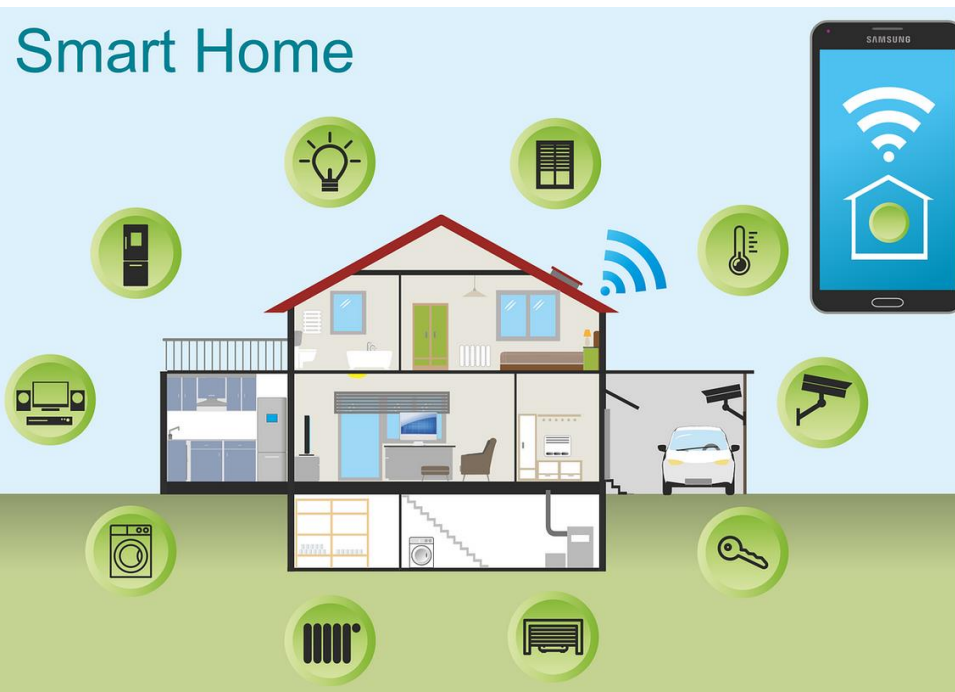
- Aplikacje mobilne do sterowania inteligentnym domem, systemy zarządzania flotą.

Internet rzeczy (IoT)

Internet rzeczy (Internet of Things, IoT)

to sieć połączonych ze sobą urządzeń, które zbierają, przesyłają i analizują dane za pomocą Internetu.

Urządzenia te działają autonomicznie, komunikują się między sobą oraz reagują na zmiany w otoczeniu zamiast



Przetwarzanie Brzegowe

Przetwarzanie Brzegowe (Edge Computing)

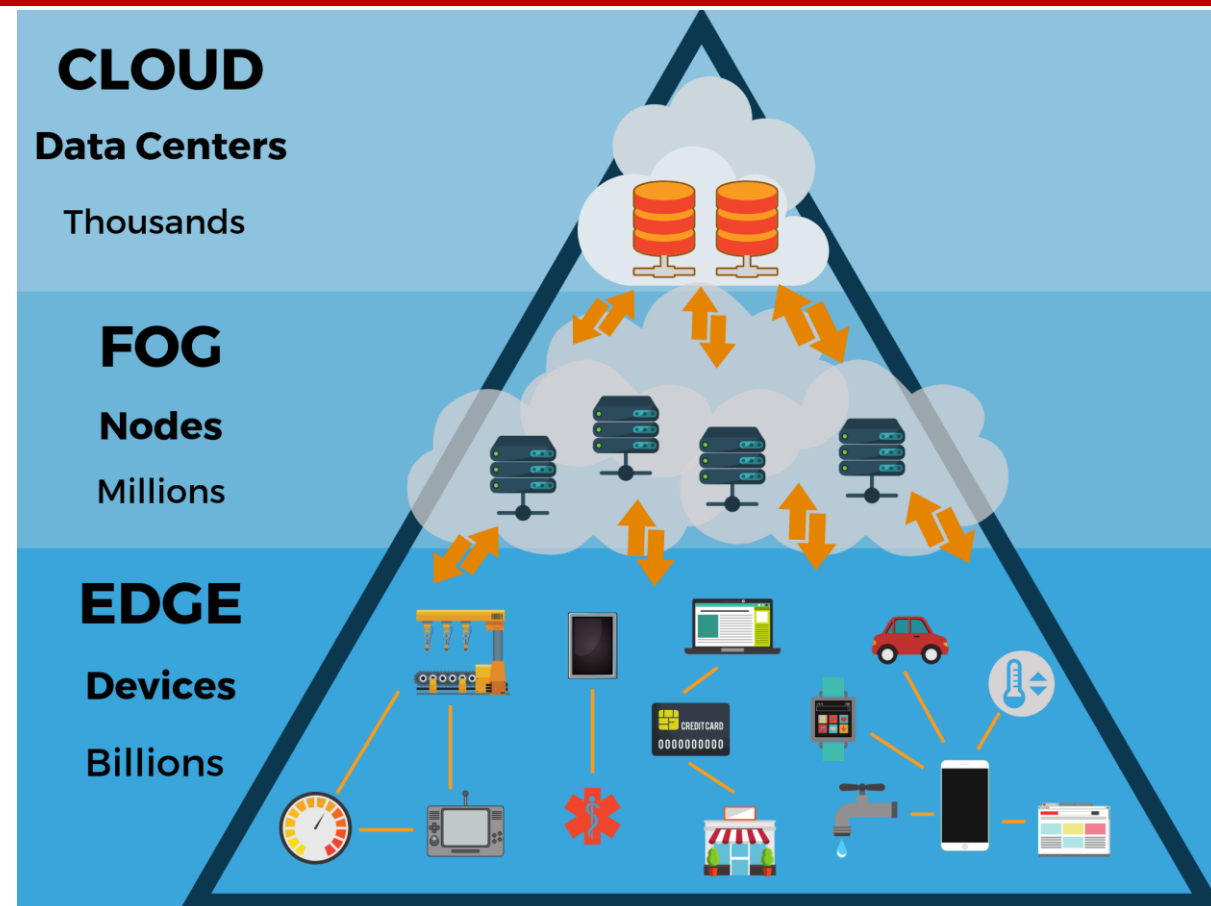
to model obliczeniowy, w którym przetwarzanie danych odbywa się **bliżej źródła ich powstawania** – na urządzeniach końcowych (np. czujnikach, kamerach, dronach) lub lokalnych serwerach brzegowych, zamiast w chmurze.

Zmniejsza to opóźnienia, oszczędza pasmo sieciowe i zwiększa bezpieczeństwo danych.

Fog Nodes (węzły mgły)

to pośrednie jednostki obliczeniowe w architekturze **Fog Computing**, które przetwarzają dane bliżej źródła ich generowania, ale dalej niż urządzenia brzegowe.

Działają jako pomost między urządzeniami IoT a chmurą, redukując opóźnienia i obciążenie sieci.



Internet rzeczy (IoT)

Zagrożenia

Zagrożenie	Opis
Brak aktualizacji oprogramowania (firmware)	Urządzenia IoT często nie otrzymują regularnych poprawek bezpieczeństwa
Domyślne lub słabe hasła dostępu	Fabryczne loginy (np. admin/admin) wykorzystywane do przejęcia kontroli
Brak szyfrowania danych	Przesył danych w postaci otwartego tekstu naraża na podsłuch i modyfikację
Niska moc obliczeniowa urządzeń	Ograniczone możliwości implementacji zaawansowanych mechanizmów kryptograficznych
Złożoność i skala środowiska	Trudność w monitorowaniu tysięcy urządzeń rozproszonych w sieci
Ataki typu botnet (np. Mirai)	Przejęcie urządzeń IoT i użycie ich do przeprowadzania ataków DDoS
Brak standaryzacji zabezpieczeń	Różne podejścia producentów powodują niespójność i luki w ochronie
Zagrożenie prywatności	Gromadzenie i przetwarzanie danych osobowych bez zgody lub kontroli użytkownika

Internet rzeczy (IoT)

Zabezpieczenia

Zabezpieczenie	Opis
Regularne aktualizacje oprogramowania (OTA)	Automatyczne i bezpieczne mechanizmy aktualizacji firmware urządzeń
Zmiana domyślnych haseł i polityka silnych haseł	Wymuszenie zmiany haseł przy pierwszym użyciu, zasada złożoności
Szyfrowanie komunikacji (TLS/DTLS)	Zabezpieczenie transmisji danych przed podsłuchem i modyfikacją
Autoryzacja i uwierzytelnianie urządzeń	Certyfikaty, tokeny, klucze publiczne i prywatne
Minimalizacja uprawnień (least privilege)	Przydzielanie tylko niezbędnych uprawnień do funkcji i zasobów
Segmentacja sieci IoT (np. VLAN, mikrosegmentacja)	Izolacja urządzeń od głównej sieci organizacji
Monitorowanie i analiza zachowania urządzeń	Wykrywanie anomalii, IDS/IPS dla IoT, integracja z SIEM
Zgodność z normami i standardami bezpieczeństwa	Wdrażanie zaleceń z ISO/IEC 27400, ETSI EN 303 645, NIST SP 800-213

OSINT

OSINT (Open Source Intelligence)

to pozyskiwanie informacji z jawnych, legalnie dostępnych źródeł, a następnie ich analiza w celu wsparcia podejmowania decyzji.

Niskokosztowy, pasywny, trudny do wykrycia.

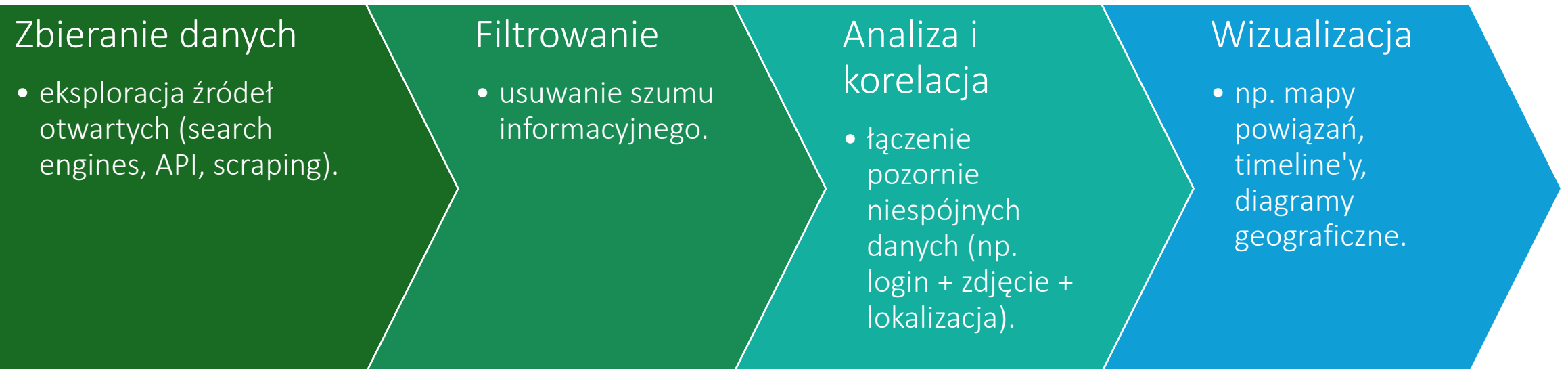
Może być zautomatyzowany
(np. z użyciem botów, crawlerów, AI)

Źródła informacji:

- Media społecznościowe (Facebook, Twitter/X, LinkedIn)
- Strony WWW i fora internetowe
- Rejestry publiczne (KRS, CEIDG, WHOIS, BIP, patenty, rejestry gruntów)
- Bazy danych i raporty (Google Scholar, SEC, EDGAR, JSTOR)
- Materiały audiowizualne i metadane

OSINT

Etapy działań



OSINT

Popularne narzędzia

Narzędzie	Zastosowanie	Oficjalna strona / repozytorium
Maltego	Mapowanie relacji i sieci powiązań	https://www.maltego.com
SpiderFoot	Automatyczna rekonesans domen	https://www.spiderfoot.net
Shodan	Wyszukiwanie urządzeń w sieci	https://www.shodan.io
Google Dorks	Zaawansowane wyszukiwanie w Google	https://www.exploit-db.com/ghdb/8444
TheHarvester	Zbieranie adresów e-mail i domen	https://github.com/laramies/theHarvester
FOCA	Wydobywanie metadanych z dokumentów	https://www.elevenpaths.com/labstools/foca/index.html

OSINT

Zastosowanie

Analiza ryzyka i testy penetracyjne:

- Identyfikacja podatności publicznie dostępnych systemów (np. niezabezpieczone domeny, e-maile pracowników).
- Uzupełnienie testów Red Team i rekonesansu pasywnego.

Walka z cyberprzestępczością:

- Namierzanie źródeł dezinformacji i ataków (np. phishing, kampanie APT).
- Weryfikacja danych wyciekowych i dark web intelligence.

Cyberhigiena organizacji:

- Monitoring obecności firmy i jej pracowników w Internecie.
- Ograniczanie ryzyka poprzez polityki prywatności i anonimizację danych.

SIEM, SOAR

Skrót	Pełna nazwa	Cel systemu
SIEM	Security Information and Event Management	Zbieranie, korelacja i analiza logów z systemów IT
SOAR	Security Orchestration, Automation and Response	Automatyzacja reakcji na incydenty i zarządzanie procesami bezpieczeństwa

Różnice funkcjonalne:

- **SIEM** koncentruje się na **widoczności zagrożeń i analizie zdarzeń**.
- **SOAR** umożliwia **reakcję i automatyzację** działań w odpowiedzi na te zagrożenia.

SIEM, SOAR

SIEM

Główne funkcje SIEM:

- Zbieranie logów z różnych źródeł (serwery, aplikacje, systemy sieciowe, IoT)
- Normalizacja i korelacja danych w czasie rzeczywistym
- Wykrywanie anomalii i wzorców ataków (np. brute-force, lateral movement)
- Tworzenie alertów i dashboardów

Korzyści:

- Centralna analiza bezpieczeństwa
- Wykrywanie incydentów wcześniej niż w przypadku ręcznych metod
- Zgodność z regulacjami (RODO, ISO 27001, PCI-DSS)

Przykłady narzędzi:

Splunk, IBM QRadar, LogPoint, ArcSight, Microsoft Sentinel

SIEM, SOAR

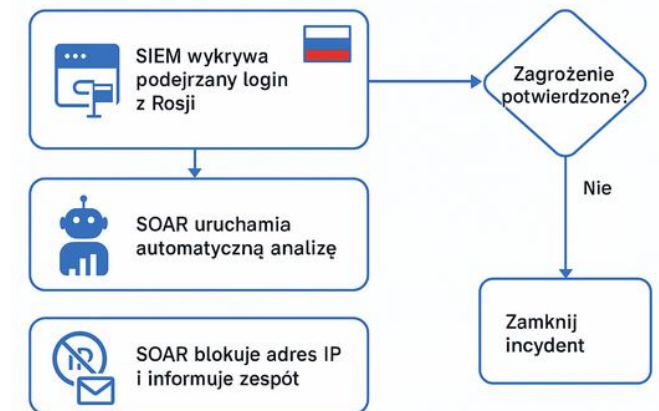
SOAR

Komponenty SOAR:

- **Orkiestracja (Orchestration):** integracja narzędzi i źródeł danych (SIEM, EDR, firewall, ticketing)
- **Automatyzacja (Automation):** wykonywanie skryptów reagujących na incydenty (np. blokada IP, reset hasła)
- **Zarządzanie przypadkami (Case Management):** dokumentacja i workflow reakcji zespołu SOC

Przykład scenariusza SOAR:

- ◆ SIEM wykrywa podejrzany login z Rosji →
- ◆ SOAR uruchamia automatyczną analizę →
- ◆ Jeśli zagrożenie się potwierdza, SOAR blokuje adres IP i informuje zespół



Przykłady narzędzi:

Palo Alto Cortex XSOAR, IBM Resilient, Splunk SOAR, Microsoft Sentinel (SOAR funkcjonalności)

SIEM, SOAR

Inne systemy

Technologia / Klasa systemu	Opis funkcjonalny
UEBA (User and Entity Behavior Analytics)	Wykrywanie anomalii w zachowaniu użytkowników i urządzeń (np. nagły wzrost dostępu do plików)
EDR (Endpoint Detection and Response)	Wykrywanie i reagowanie na zagrożenia na poziomie urządzeń końcowych (np. laptop, serwer)
XDR (Extended Detection and Response)	Rozszerzony EDR: koreluje dane z wielu źródeł (endpoint, sieć, chmura) w jeden system analizy i reakcji
NDR (Network Detection and Response)	Wykrywanie i reagowanie na zagrożenia sieciowe poprzez analizę ruchu i wykrywanie wzorców ataków
TIP (Threat Intelligence Platform)	Zbieranie i korelowanie danych z zewnętrznych źródeł o zagrożeniach (IOC, TTP, kampanie APT)
IRP (Incident Response Platform)	Platformy wspierające proces obsługi incydentów (często jako część SOAR)
Deception Technology	Wdrażanie pułapek i honeypotów w celu wykrycia intruzów przez ich nieautoryzowane działania

Ocena ryzyka

Ocena ryzyka bezpieczeństwa informacji

to proces identyfikacji, analizy i oceny ryzyka związanego z zagrożeniami dla zasobów informacyjnych organizacji. Jej głównym celem jest dostarczenie decydentom wiarygodnych danych umożliwiających:

1. Zrozumienie, jakie zagrożenia (wewnętrzne i zewnętrzne) oraz podatności mogą wpłynąć na poufność, integralność i dostępność informacji.
2. Wyznaczenie priorytetów działań zabezpieczających w oparciu o akceptowalny poziom ryzyka.
3. Optymalizację nakładów na środki ochrony, tak aby inwestycje były proporcjonalne do wielkości i istotności ryzyka.

Norma / Rama	Zakres i przeznaczenie	Kluczowe cechy
ISO/IEC 27005	Wytyczne do zarządzania ryzykiem w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z ISO/IEC 27001.	• Proces zgodny z cyklem PDCA • Identyfikacja, analiza, ocena i traktowanie ryzyka • Skoncentrowana na poufności, integralności i dostępności

Ocena ryzyka

Metody oceny ryzyka

Jakościowa

Rangi (np. niskie/średnie/wysokie) przypisywane przez ekspertów.

Zalety: szybka, niskokosztowa.

Ograniczenia: subiektywność, trudności w porównywaniu wyników.

Ilościowa

Wyrażanie ryzyka w wartościach liczbowych (np. w PLN, USD, godzinach przestoju).

Wymaga danych statystycznych i modelowania.

Zapewnia precyzyjne pomiary, ale jest pracochłonna.

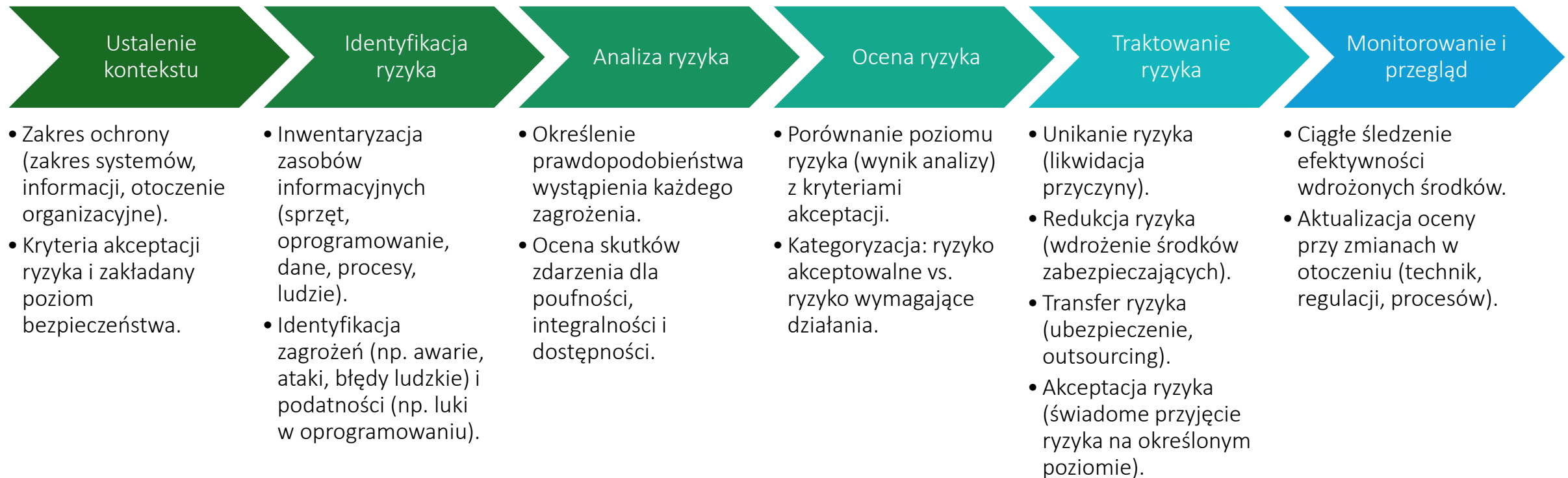
Hybrydowa

Łączy podejście jakościowe z wstępną analizą liczbową.

Umożliwia kompromis między szybkością a dokładnością.

Ocena ryzyka

Etapy procesu oceny ryzyka



Ocena ryzyka

Narzędzia i techniki

Diagram scenariuszy ataku (ang. attack trees)

- modelowanie dróg, poprzez które przeciwnik może osiągnąć cel.

Check-listy i kwestionariusze

- standaryzowane listy zagrożeń i kontroli.

Analiza FMEA (Failure Mode and Effects Analysis)

- ocena wpływu możliwych awarii na funkcjonowanie systemu.

Symulacje i testy penetracyjne

- praktyczna weryfikacja podatności.

Ocena ryzyka

Macierz oceny ryzyka

to dwuwymiarowe narzędzie służące do graficznej lub tabelarycznej prezentacji poziomu ryzyka, zdefiniowanego jako iloczyn:

$$\text{Ryzyko} = \text{Prawdopodobieństwo}(P) \times \text{Skutek}(S)$$

- **Oś pozioma (X)** reprezentuje poziomy skutku (S) zdarzenia — np. od „bardzo niskiego” do „krytycznego”.
- **Oś pionowa (Y)** reprezentuje poziomy prawdopodobieństwa (P) wystąpienia zdarzenia — od „bardzo małego” do „bardzo dużego”.

W każdej komórce macierzy umieszcza się skategoryzowany poziom ryzyka (np. niskie, umiarkowane, wysokie, krytyczne), co umożliwia szybką identyfikację obszarów wymagających uwagi i działań zaradczych.

#	Zagrożenie	P (1–5)	S (1–5)	P×S	Kategoria	Proponowane środki zaradcze
1	Awaria łącza internetowego w trakcie wysyłki	3	4	12	Wysokie	Przygotować kopię offline; wysłać plik z wyprzedzeniem; backup łącz
2	Przerwa techniczna platformy Moodle	2	5	10	Wysokie	Monitorować status Moodle; wysłać sprawozdanie przed deadline
3						

Progi kategorii ryzyka

- 1–4: **Niskie** (akceptowalne)
- 5–8: **Umiarkowane** (wymaga podstawowych środków)
- 9–16: **Wysokie** (należy wdrożyć istotne zabezpieczenia)
- 17–25: **Bardzo wysokie** (natychmiastowa interwencja)

Zadanie

(0-2 pkt)



Treść

Jesteście zespołem konsultantów ds. bezpieczeństwa informacji w fikcyjnej firmie „DataSafe sp. z o.o.” (ok. 50 pracowników). Firma przechowuje dane osobowe klientów, dokumentację finansową oraz prowadzi wewnętrzny system CRM dostępny przez sieć firmową.

Identyfikacja zagrożeń

- Wyszczególnij co najmniej 6 głównych zagrożeń dla poufności, integralności i dostępności danych w przedstawionej organizacji.

Ocena ryzyka

- Przeprowadź ocenę ryzyka dla każdego zidentyfikowanego zagrożenia, stosując prostą macierz ryzyka (Prawdopodobieństwo × Skutek).

Dobór środków ochronnych

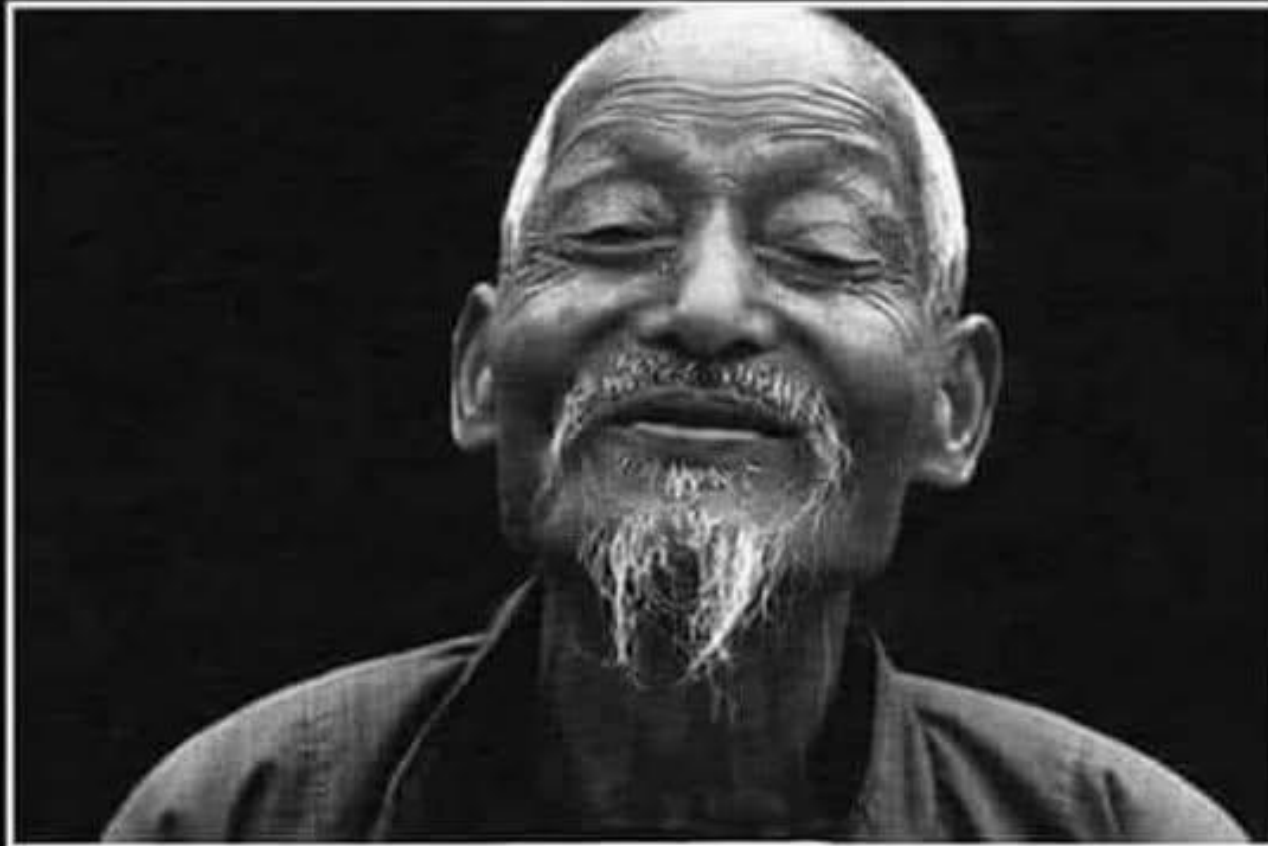
- Zaproponuj odpowiednie środki techniczne, organizacyjne i proceduralne, które zminimalizują lub wyeliminują wskazane zagrożenia.

Wnioski i rekomendacje

- Podsumuj najważniejsze wnioski i wskaż, które działania powinny być realizowane najpilniej.

Termin przesłania sprawozdania, wskazany w zadaniu w Moodle.

Tylko w chińskich samochodach...



...wszystkie części są oryginalne