ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Zarządzanie ryzykiem w chmurze

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Marcin Fronczak

Prowadzi szkolenia z zakresu bezpieczeństwa chmur m.in. przygotowujące do egzaminu Certified Cloud Security Knowledge (CCSK). Certyfikowany audytor systemów informatycznych oraz ekspert w zarządzaniu ryzykiem i bezpieczeństwem informacji - CISA, CIA, CRISC.

ZAUFANA TRZECIA STRONA.PL

Agenda

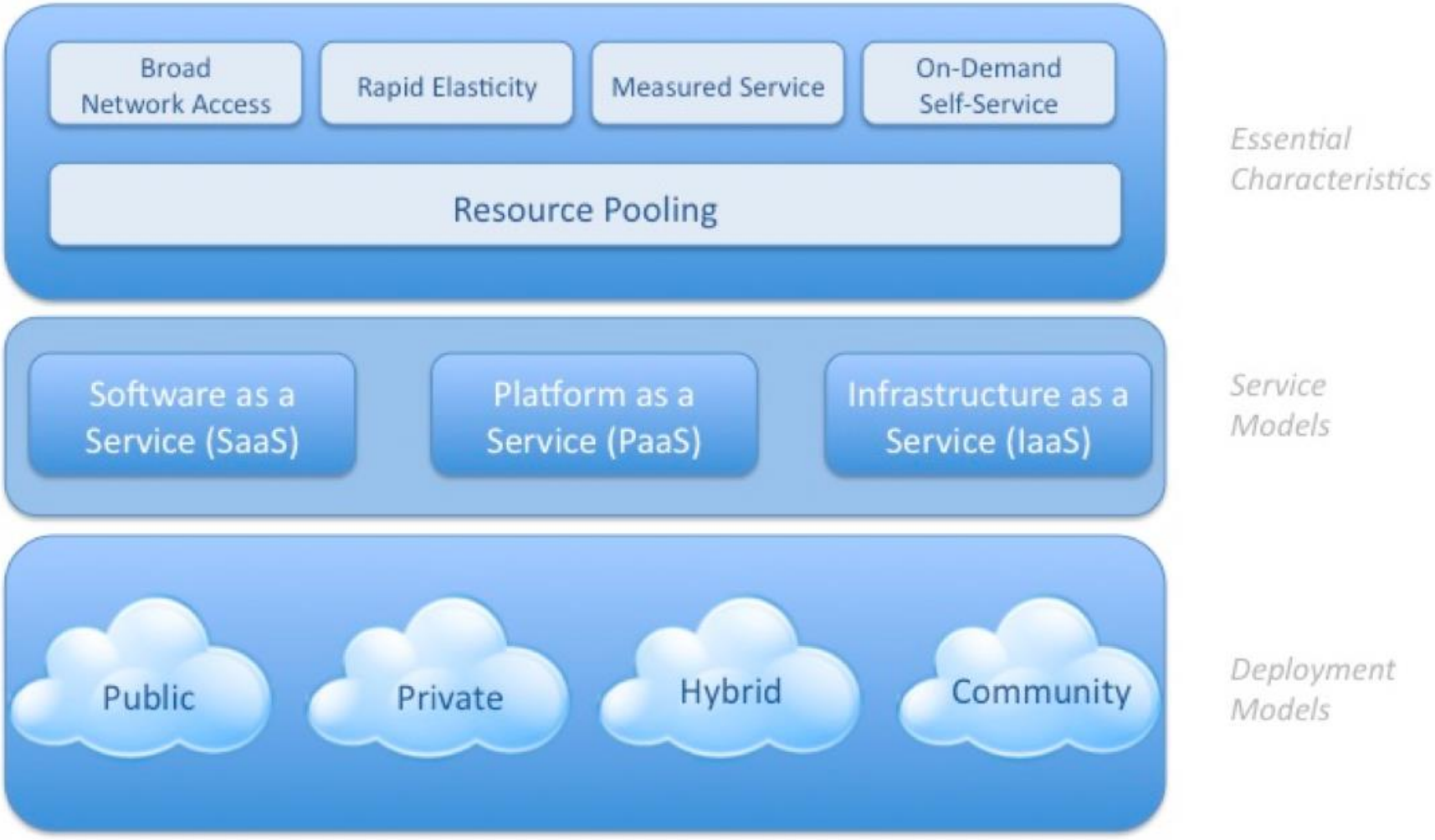
aruba CLOUD

1. Podsumowanie zagadnień poruszanych w poprzednich artykułach
2. Wprowadzenie do zarządzania ryzykiem
3. Odpowiedzialność za zabezpieczanie poszczególnych komponentów i warstw
4. Ryzyka i zagrożenia w chmurze - specyficzne i tradycyjne
5. Podsumowanie
6. Sesja pytań od uczestników

ZAUFANA TRZECIA STRONA.PL

Model chmury wg NIST

aruba CLOUD

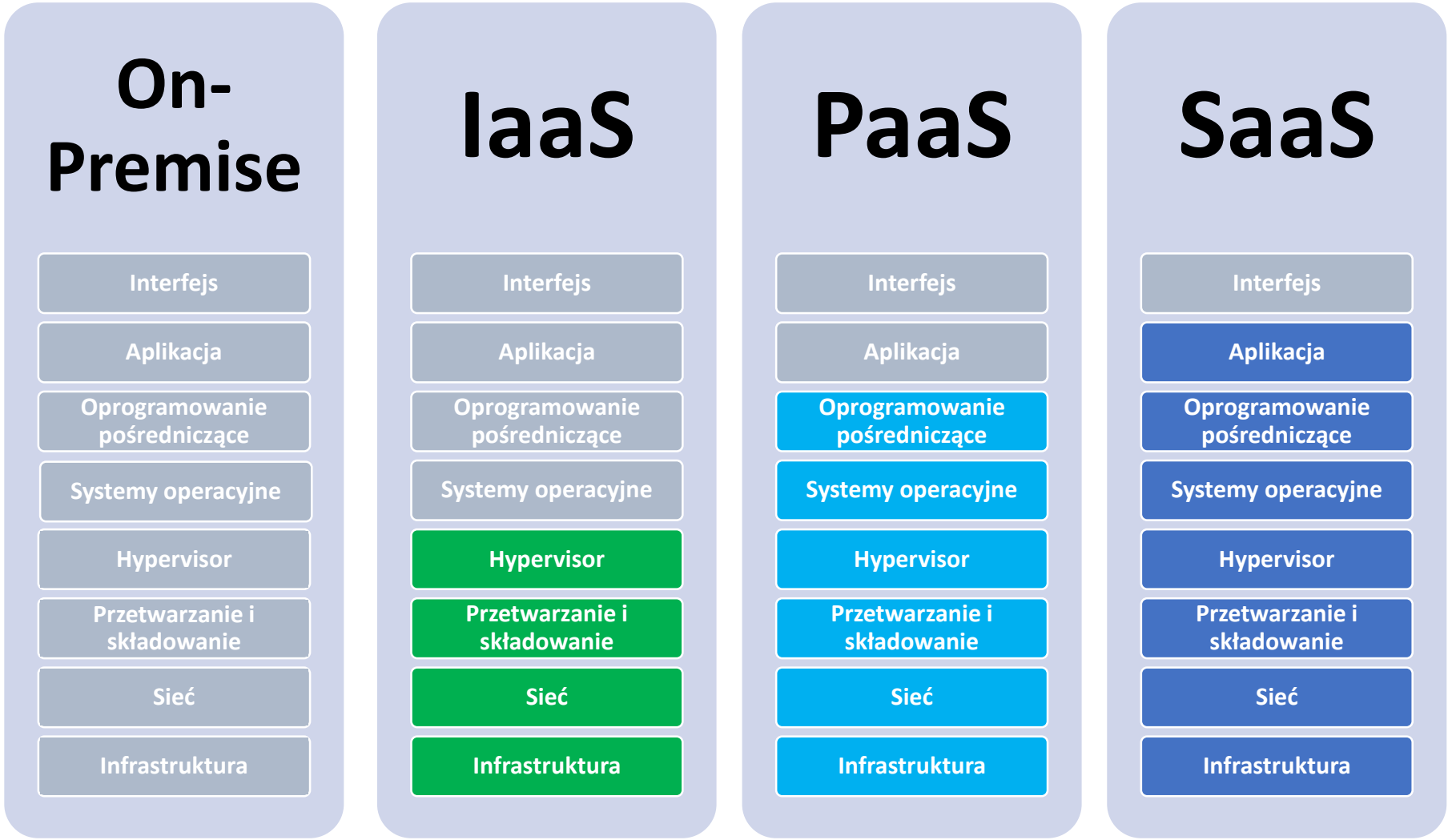


Model chmury wg NIST – *źródło: Cloud Security Alliance*

ZAUFANA TRZECIA STRONA.PL

Stos SPI

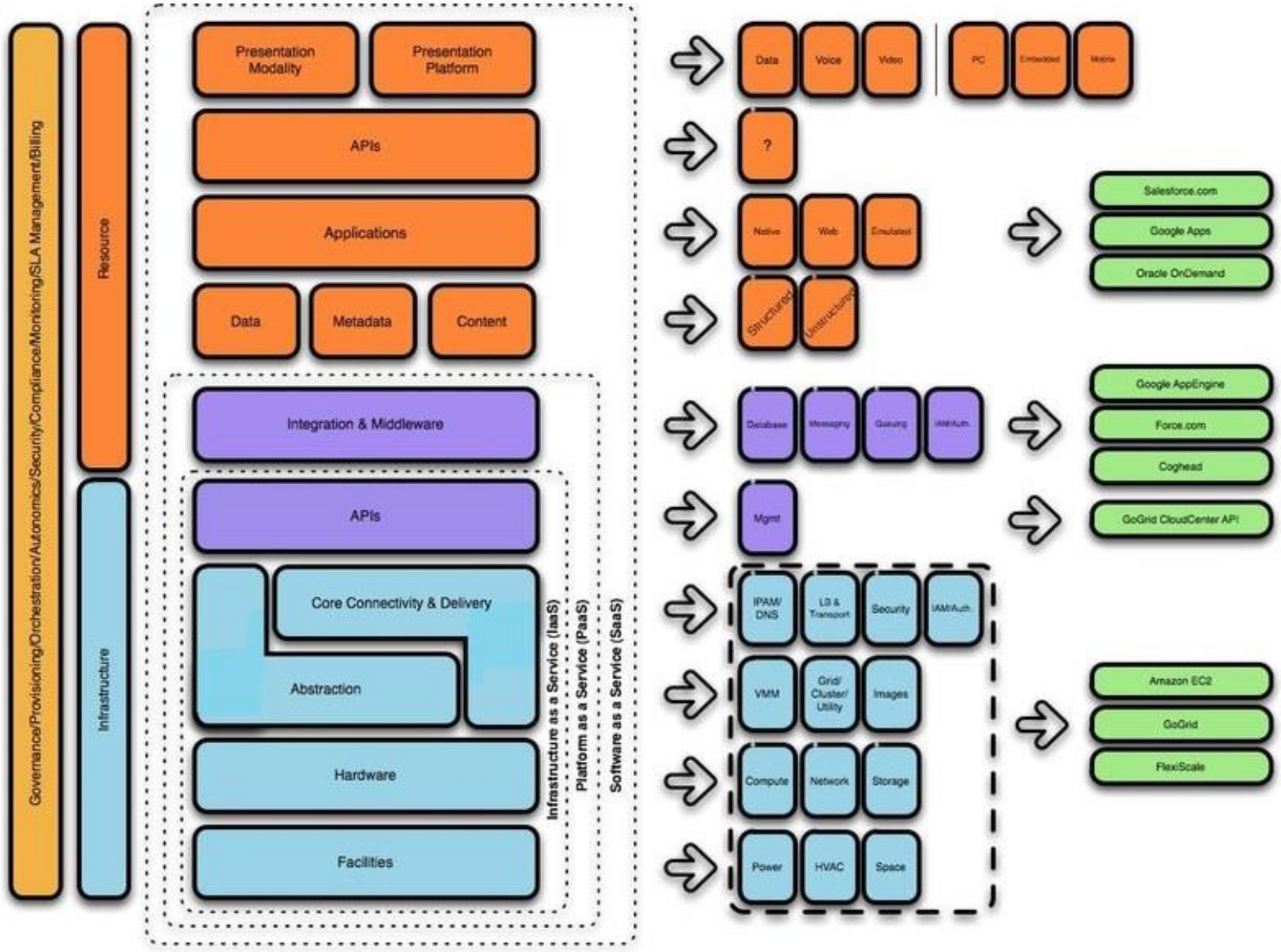
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Stos SPI

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Stos SPI

aruba CLOUD

ZAUFANA TRZECIA STRONA.PL

On Premise

aruba CLOUD

On-Premise

- Interfejs
- Aplikacja
- Oprogramowanie pośredniczące
- Systemy operacyjne
- Hypervisor
- Przetwarzanie i składowanie
- Sieć
- Infrastruktura

ZAUFANA TRZECIA STRONA.PL

Infrastructure as a Service

aruba CLOUD

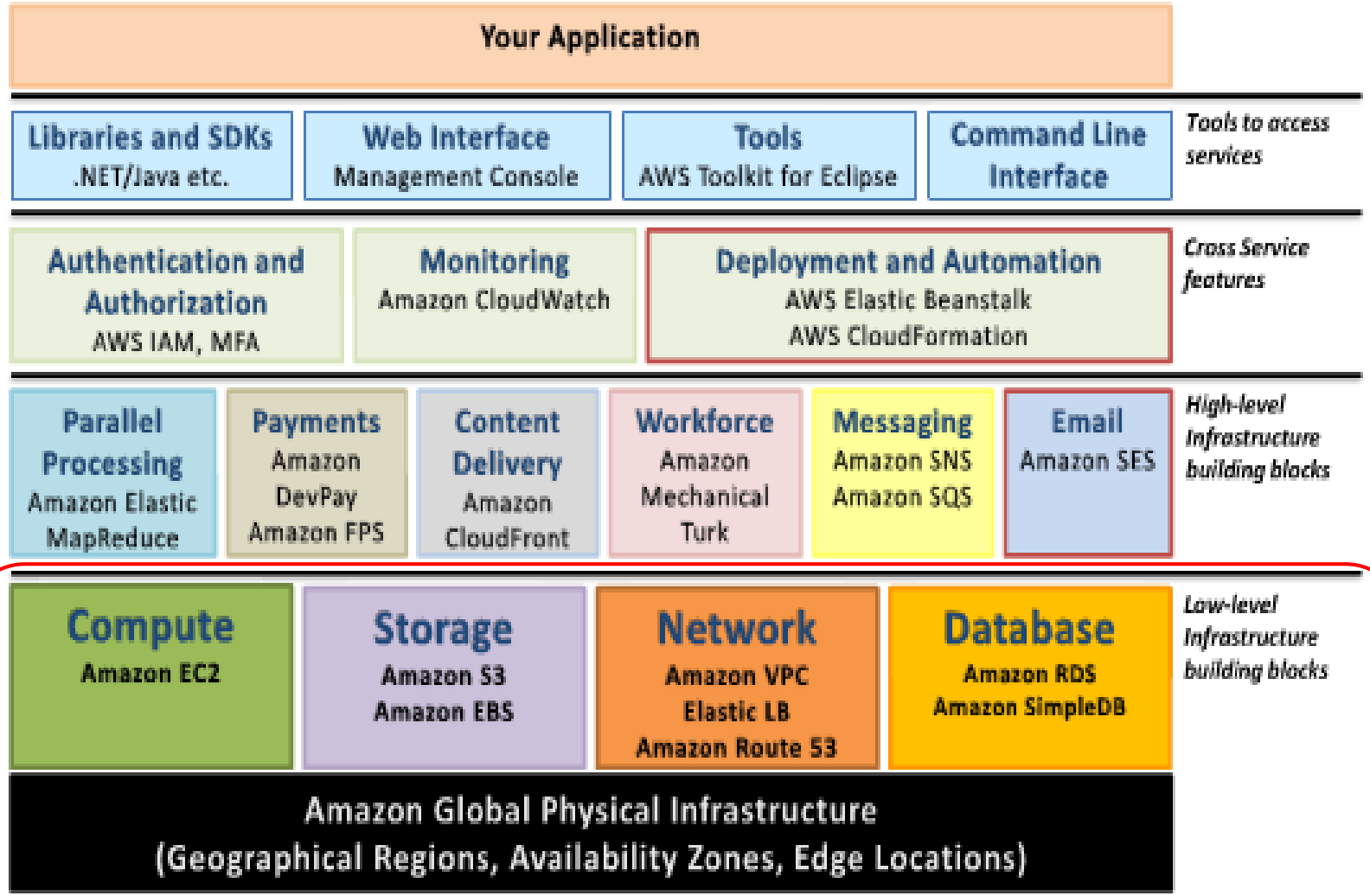
IaaS

- Interfejs
- Aplikacja
- Oprogramowanie pośredniczące
- Systemy operacyjne
- Hypervisor
- Przetwarzanie i składowanie
- Sieć
- Infrastruktura

ZAUFANA TRZECIA STRONA.PL

Infrastructure as a Service

aruba CLOUD



IaaS

- Interfejs
- Aplikacja
- Oprogramowanie pośredniczące
- Systemy operacyjne
- Hypervisor
- Przetwarzanie i składowanie
- Sieć
- Infrastruktura

- AWS
- Digital Ocean
- Google (GCE)
- Azure
- RackSpace
- OVH
- Aruba Cloud
- Oktawave
- e24cloud

ZAUFANA TRZECIA STRONA.PL

Platform as a Service

aruba CLOUD

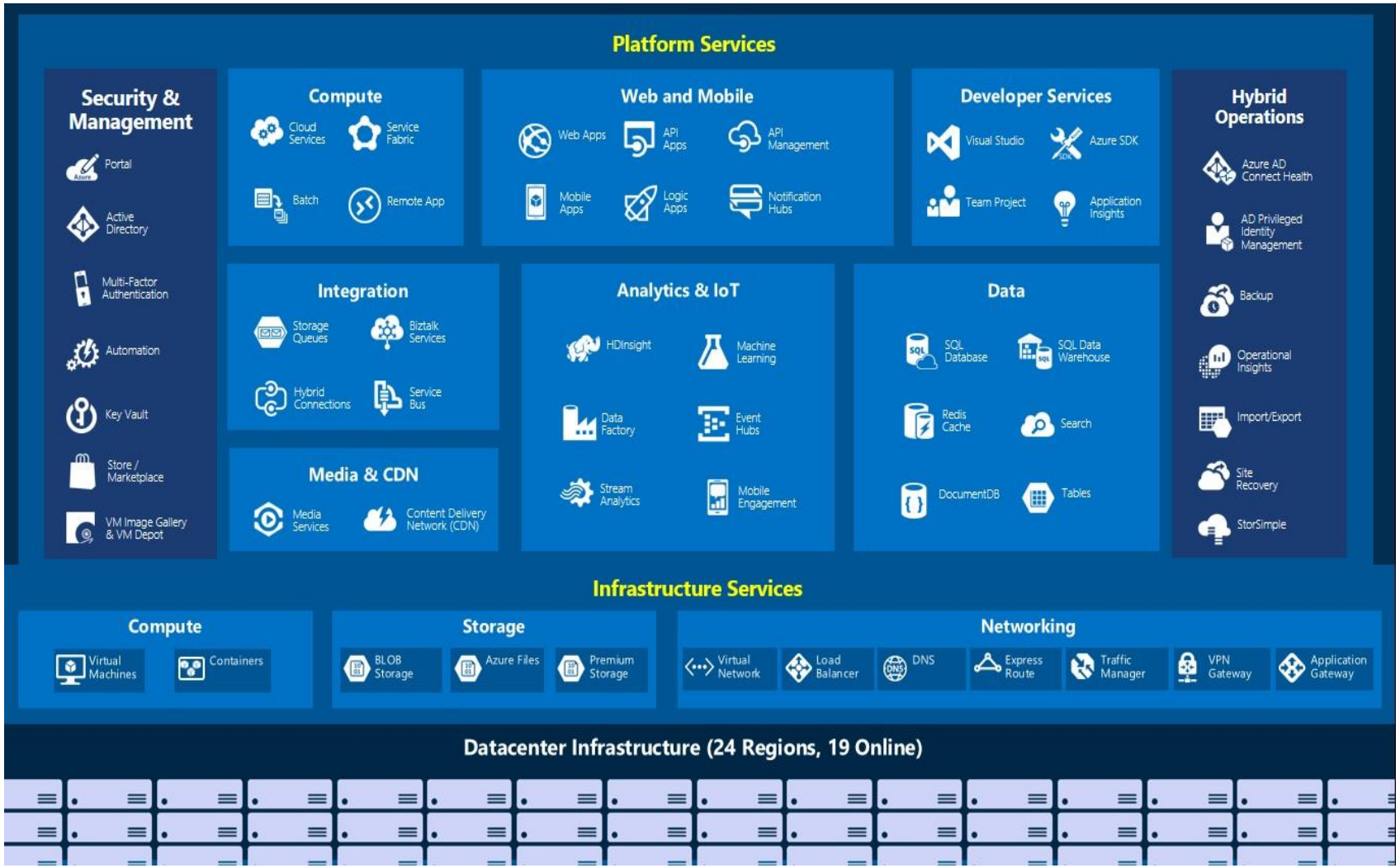
PaaS

- Interfejs
- Aplikacja
- Oprogramowanie pośredniczące
- Systemy operacyjne
- Hypervisor
- Przetwarzanie i składowanie
- Sieć
- Infrastruktura

ZAUFANA TRZECIA STRONA.PL

Platform as a Service

aruba CLOUD



PaaS

- Interfejs
- Aplikacja
- Oprogramowanie pośredniczące
- Systemy operacyjne
- Hypervisor
- Przetwarzanie i składowanie
- Sieć
- Infrastruktura

- AWS
- Azure
- App Cloud
- Force.com
- Google App Engine
- Oracle Cloud Platform
- SAP Hana Platform

ZAUFANA TRZECIA STRONA.PL

Software as a service

aruba CLOUD

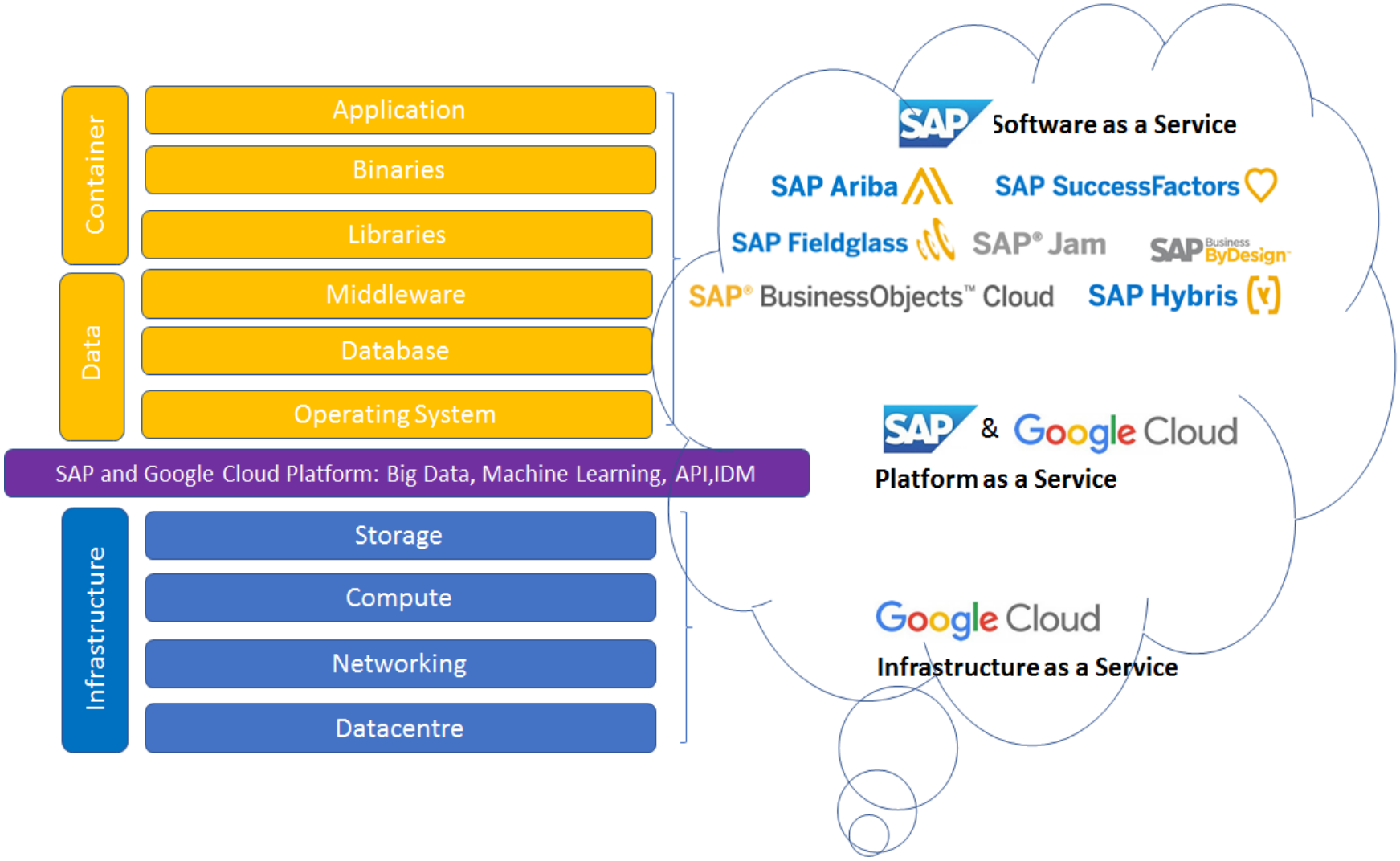
SaaS

- Interfejs
- Aplikacja
- Oprogramowanie pośredniczące
- Systemy operacyjne
- Hypervisor
- Przetwarzanie i składowanie
- Sieć
- Infrastruktura

ZAUFANA TRZECIA STRONA.PL

Software as a service

aruba CLOUD



SaaS

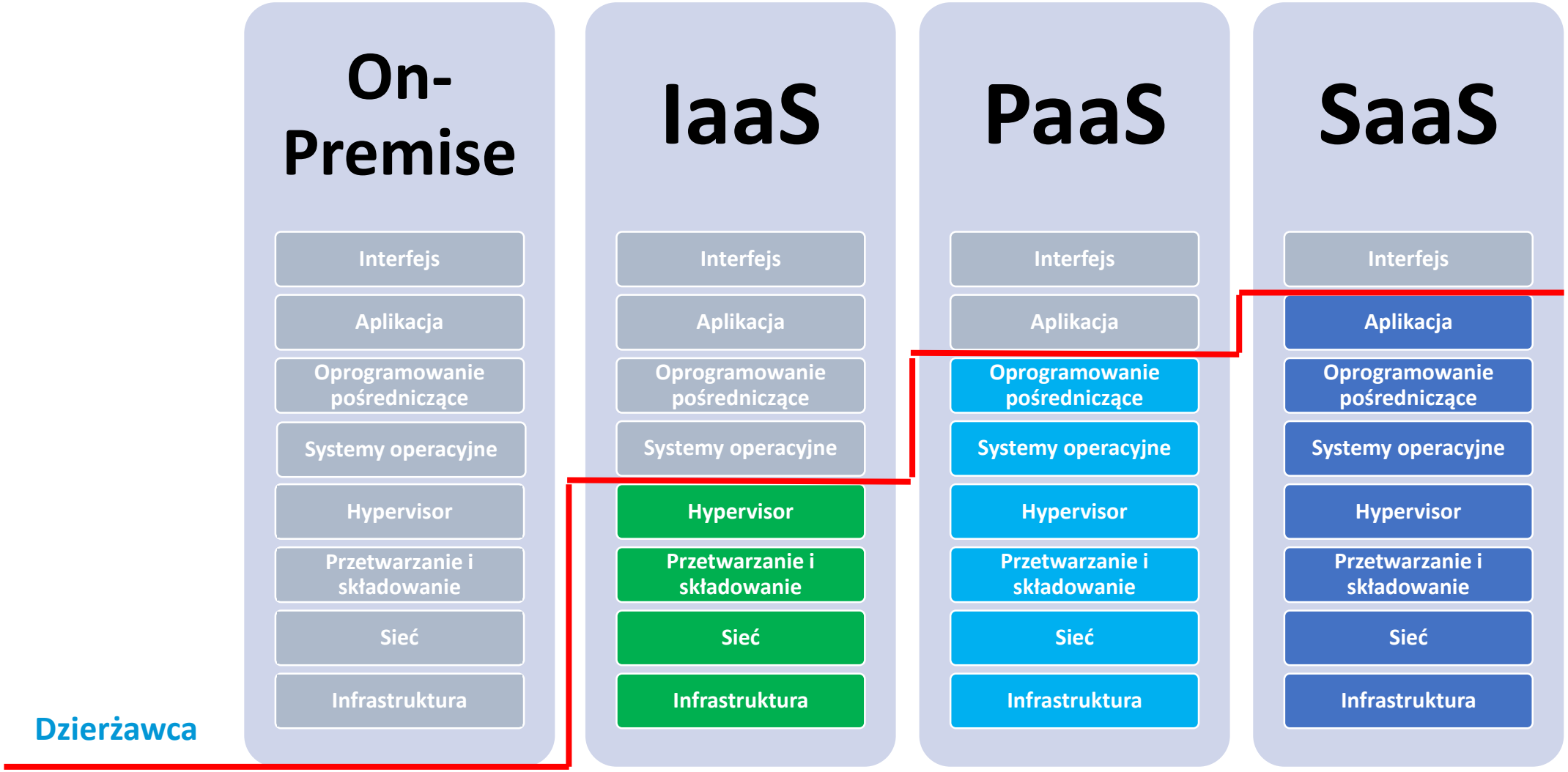
- Interfejs
- Aplikacja
- Oprogramowanie pośredniczące
- Systemy operacyjne
- Hypervisor
- Przetwarzanie i składowanie
- Sieć
- Infrastruktura

- DropBox
- Office 365
- Salesforce
- Jira

ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność

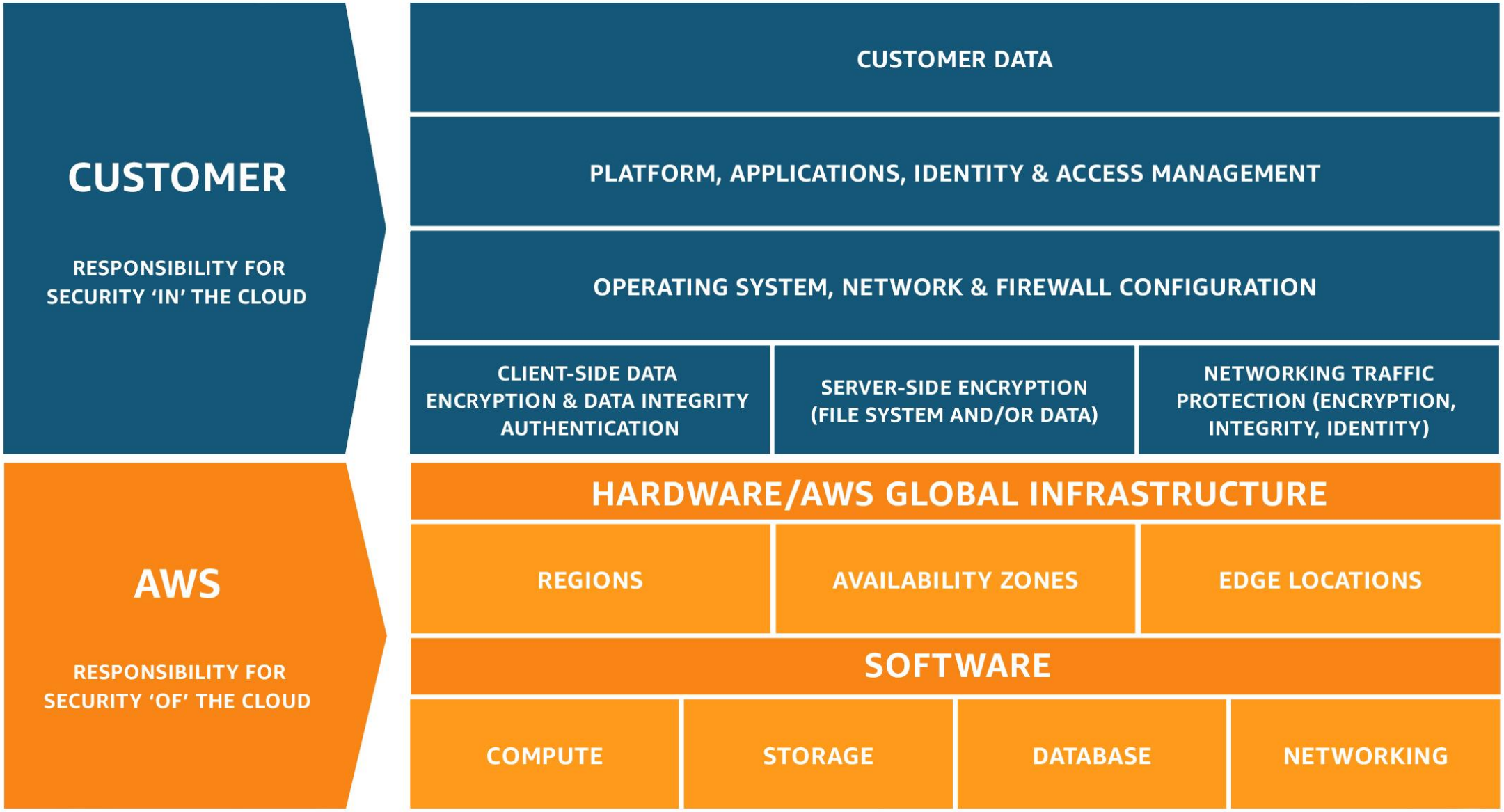
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

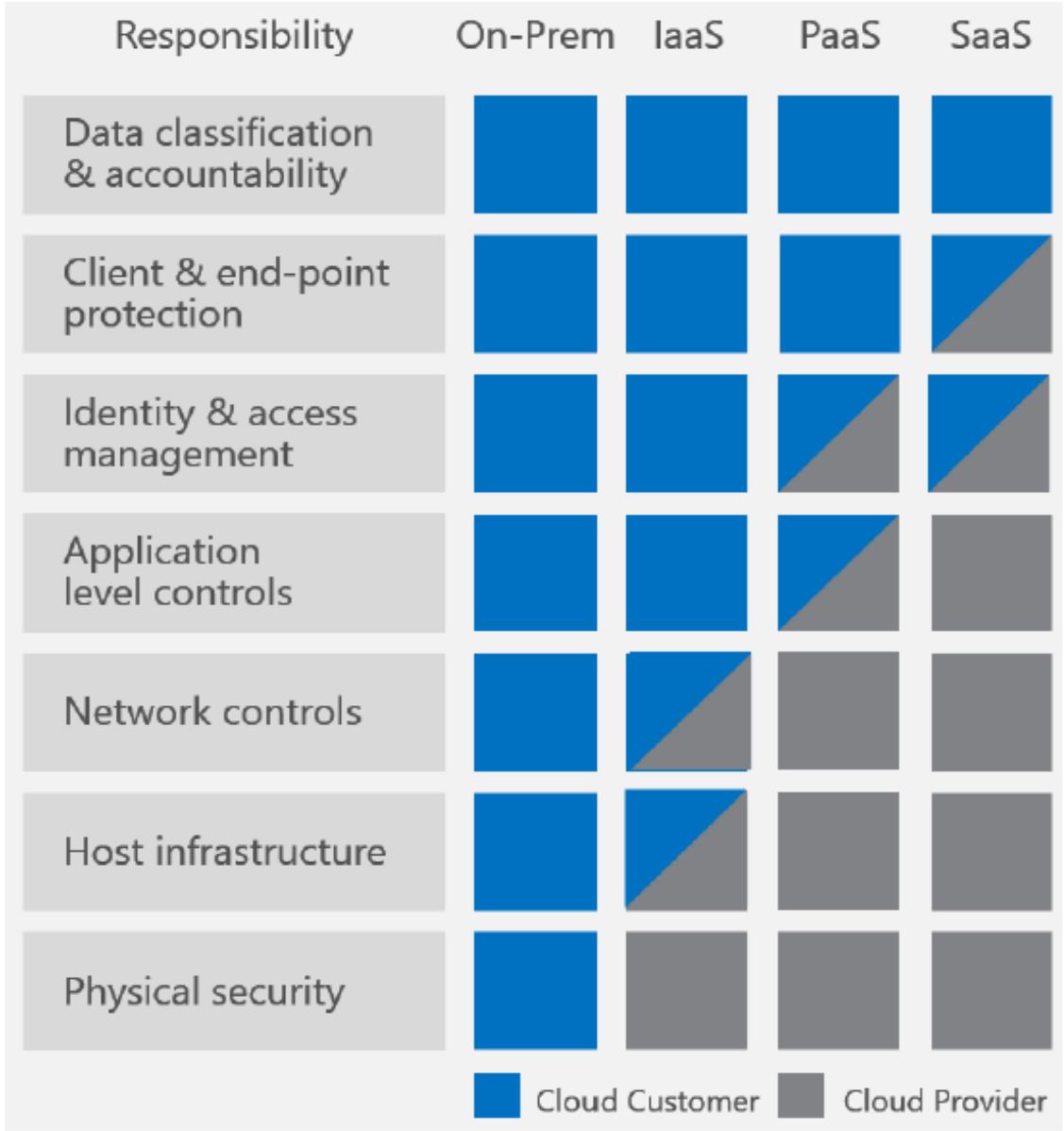
Odpowiedzialność

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność



aruba CLOUD

ZAUFANA TRZECIA STRONA.PL

Chmura publiczna

aruba CLOUD

	Infrastruktura zarządzana przez:	Infrastruktura w posiadaniu:	Infrastruktura umieszczona:	Dostępna i wykorzystywana przez:
Publiczna	Dostawca (Third Party Provider)	Dostawca (Third Party Provider)	Na zewnątrz (Off-Premise)	Niezaufana strona
Prywatna/ Współdzielona	Organizacja Lub Dostawca	Organizacja Dostawca	Wewnątrz (On-Premise) Na zewnątrz	Zaufana strona
Hybrydowa	Zarówno Organizacja jak i Dostawca	Zarówno Organizacja jak i Dostawca	Zarówno Wewnątrz jak i Na zewnątrz	Zarówno Zaufana i Niezaufana strona

ZAUFANA TRZECIA STRONA.PL

Chmura prywatna/współdzielona

aruba CLOUD

	Infrastruktura w posiadaniu:	Infrastruktura umieszczona:	Infrastruktura zarządzana przez:	Dostępna i wykorzystywana przez:
Publiczna	Dostawca (Third Party Provider)	Na zewnątrz (Off-Premise)	Dostawca (Third Party Provider)	Niezaufana strona
Prywatna/ Współdzielona	Organizacja Lub Dostawca	Wewnątrz (On-Premise) Na zewnątrz	Organizacja Dostawca	Zaufana strona
Hybrydowa	Zarówno Organizacja jak i Dostawca	Zarówno Wewnątrz jak i Na zewnątrz	Zarówno Organizacja jak i Dostawca	Zarówno Zaufana i Niezaufana strona

ZAUFANA TRZECIA STRONA.PL

Chmura hybrydowa

aruba CLOUD

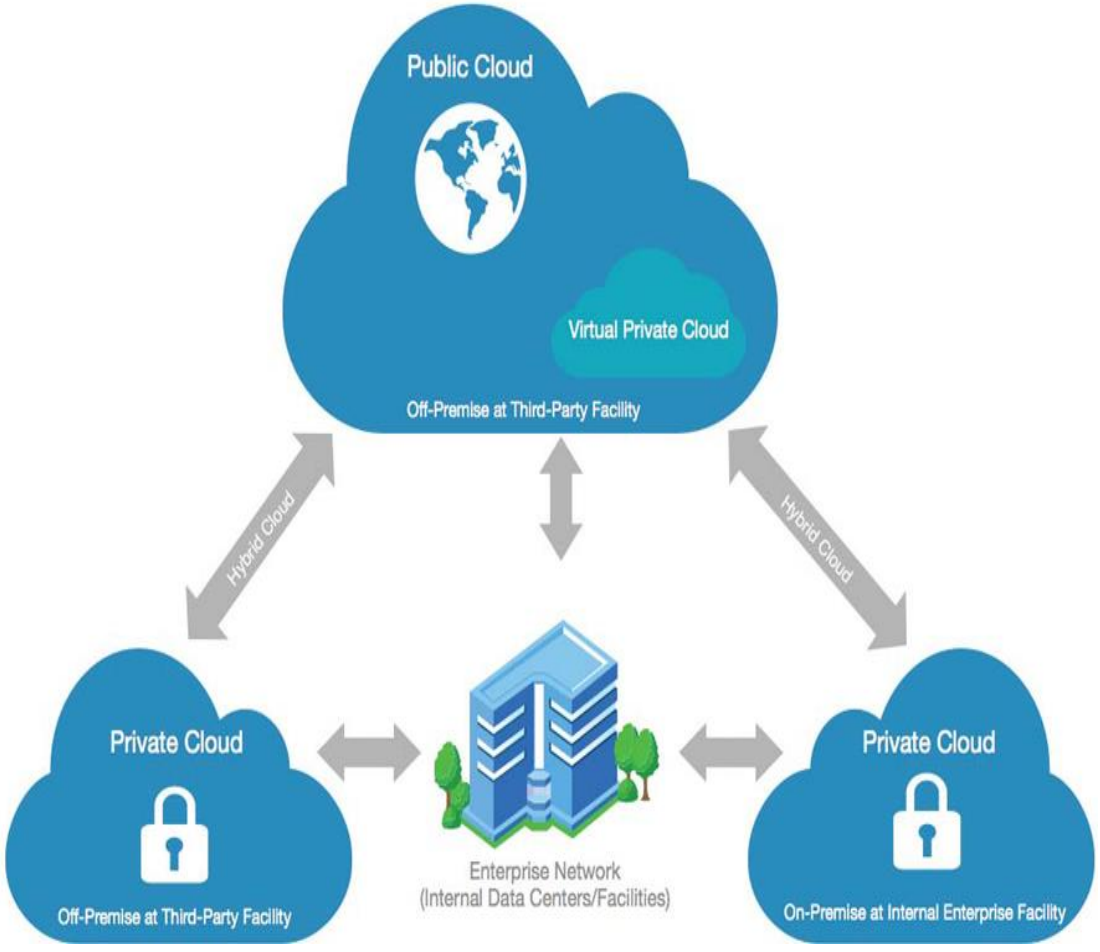
	Infrastruktura zarządzana przez:	Infrastruktura w posiadaniu:	Infrastruktura umieszczona:	Dostępna i wykorzystywana przez:
Publiczna	Dostawca (Third Party Provider)	Dostawca (Third Party Provider)	Na zewnątrz (Off-Premise)	Niezaufana strona
Prywatna/ Współdzielona	Organizacja Lub Dostawca	Organizacja Dostawca	Wewnątrz (On-Premise) Na zewnątrz	Zaufana strona
Hybrydowa	Zarówno Organizacja jak i Dostawca	Zarówno Organizacja jak i Dostawca	Zarówno Wewnątrz jak i Na zewnątrz	Zarówno Zaufana i Niezaufana strona

ZAUFANA TRZECIA STRONA.PL

Chmura hybrydowa

aruba CLOUD

	Infrastruktura zarządzana przez:	Infrastruktura w posiadaniu:	Infrastruktura umieszczona:	Dostępna i wykorzystywana przez:
Publiczna	Dostawca (Third Party Provider)	Dostawca (Third Party Provider)	Na zewnątrz (Off-Premise)	Niezaufana strona
Prywatna/ Współdzielona	Organizacja Lub Dostawca	Organizacja Dostawca	Wewnątrz (On-Premise) Na zewnątrz	Zaufana strona
Hybrydowa	Zarówno Organizacja jak i Dostawca	Zarówno Organizacja jak i Dostawca	Zarówno Wewnątrz jak i Na zewnątrz	Zarówno Zaufana i Niezaufana strona



ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność

aruba CLOUD

Bezpieczeństwo	Interfejs	Prywatna (On-Premise)	Prywatna (Off-Premise)	Public		
				IaaS	PaaS	SaaS
Personel	Odbiorca	Odbiorca	Wspólna	Wspólna	Wspólna	Dostawca
Bezpieczeństwo aplikacji	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Zarządzanie dostępem i tożsamością	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Zarządzanie logami	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Szyfrowanie danych	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Host intrusion Detection	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca	Dostawca
System monitoring	Odbiorca	Odbiorca	Odbiorca	Wspólna	Dostawca	Dostawca
OS Hardening	Odbiorca	Odbiorca	Odbiorca	Wspólna	Dostawca	Dostawca
Network intrusion Detection	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca
Bezpieczeństwo sieci	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca
Polityki bezpieczeństwa	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca
Bezpieczeństwo fizyczne/środ.	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

CSA Security Guidance ver.4

Top Threats

STRIDE

Działania operacyjne

- Architektura chmury
- Nadzór i zarządzanie ryzykiem
- Prawo i informatyka śledcza
- Zgodność i audyt
- Zarządzanie informacją i ochrona danych
- Przenaszalność i interoperacyjność
- Zarządzanie ciągłością i plany awaryjne
- Centrum danych i zarządzanie operacjami
- Zarządzanie incydentami
- Bezpieczeństwo aplikacji
- Szyfrowanie i zarządzanie kluczami
- Zarządzanie własnością, tożsamością i dostępem
- Wirtualizacja
- Security as a Service

Zarządzanie w chmurze

CCM

HIPAA Health Insurance Portability and Accountability Act

enisa European Network and Information Security Agency

COBIT 5 AN ISACA® FRAMEWORK

GDPR EU General Data Protection Regulation

ISO 27001 27002 27017 27018

NIST SP 800-53 R3/R4

PCI DSS COMPLIANT

Bundesamt für Sicherheit in der Informationstechnik

IaaS	PaaS	SaaS
Public		Private
Physical	Network	Compute
Storage	Application	Data
Service/Provider		Tenant/Consumer

cloudsecurityalliance.org/guidance

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Cloud Control Matrix ver.3.0.1

1. **AIS**: Application & Interface Security (4)
2. **AAC**: Audit Assurance & Compliance (3)
3. **BCR**: Business Continuity Management & Operational Resilience (11)
4. **CCC**: Change Control & Configuration Management (5)
5. **DSI**: Data Security & Information Lifecycle Management (7)
6. **DCS**: Datacenter Security (9)
7. **EKM**: Encryption & Key Management (4)
8. **GRM**: Governance and Risk Management (11)
9. **HRS**: Human Resources (11)
10. **IAM**: Identity & Access Management (13)
11. **IVS**: Infrastructure & Virtualization Security (13)
12. **IPY**: Interoperability & Portability (5)
13. **MOS**: Mobile Security (20)
14. **SEF**: Security Incident Management, E-Discovery & Cloud Forensics (5)
15. **STA**: Supply Chain Management, Transparency and Accountability (9)
16. **TVM**: Threat and Vulnerability Management (3)

16 domen

133 zabezpieczenia

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Cloud Control Matrix ver.3.0.1

Application & Interface Security (AIS)

- AIS-01: Application Security
- AIS-02: Customer Access Requirements
- AIS-03: Data Integrity
- AIS-04: Data Security / Integrity

Audit Assurance & Compliance (AAC)

- AAC-01: Audit Planning
- AAC-02: Independent Audits
- AAC-03: Information System Regulatory Mapping

Business Continuity Management & Operational Resilience (BCR)

- BCR-01: Business Continuity Planning
- BCR-02: Business Continuity Testing
- BCR-03: Datacenter Utilities / Environmental Conditions
- BCR-04: Documentation
- BCR-05: Environmental Risks
- BCR-06: Equipment Location
- BCR-07: Equipment Maintenance
- BCR-08: Equipment Power Failures
- BCR-09: Impact Analysis
- BCR-10: Policy
- BCR-11: Retention Policy

Change Control & Configuration Management (CCC)

- CCC-01: New Development / Acquisition
- CCC-02: Outsourced Development
- CCC-03: Quality Testing
- CCC-04: Unauthorized Software Installations
- CCC-05: Production Changes

Data Security & Information Lifecycle Management (DSI)

- DSI-01: Classification
- DSI-02: Data Inventory / Flows
- DSI-03: eCommerce Transactions
- DSI-04: Handling / Labeling / Security Policy
- DSI-05: Non-Production Data
- DSI-06: Ownership / Stewardship
- DSI-07: Secure Disposal

16 domen

133 zabezpieczenia

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Naruszenie, wyciek danych

- British Telecom TalkTalk (2014, 2015) – 4 miliony danych osobowych (400k£)
- Yahoo – wyciek kont -1 miliard (2013), 500 mln (2014), 3 mld zaraportowane w 2017 r.

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(IAM) Kontrola dostępu	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie tożsamością	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(CCC) Zarządzanie zmianą	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(EKM) Szyfrowanie danych	Odbiorca
IaaS/PaaS/SaaS	(TVM) Zarządzanie podatnościami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Zarządzanie incydentami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Informatyka śledcza	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Separacja i segmentacja sieci	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Hardening	Dostawca

Klasyfikacja zagrożeń (STRIDE)

☒ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☒ Manipulowanie danymi (Tampering with Data)
☒ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☒ Ataki odmowy usługi (Denial of Service)
☒ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Zarządzanie tożsamością, dostępem i danymi uwierzytelniającymi

- LinkedIn – 6,5 mln hashy (2012), 167 mln profili (2016)
- Instagram – reset hasła umożliwiał logowanie bez danych uwierzytelniających

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(IAM) Kontrola dostępu	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie tożsamością	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie kluczami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(HRS) Zarządzanie zasobami ludzkimi	Dostawca/Odbiorca

Klasyfikacja zagrożeń (STRIDE)

☑ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☑ Manipulowanie danymi (Tampering with Data)
☑ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☑ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Niezabezpieczone interfejsy i API

- US Internal Revenue Service – 300 tys. rekordów
- Moonpig (2015) – Dane osobowe 3 mln użytkowników.

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(AIS) Bezpieczeństwo interfejsu	Dostawca
IaaS/PaaS/SaaS	(IAM) Zarządzanie tożsamością	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Kontrola dostępu	Dostawca/Odbiorca

Klasyfikacja zagrożeń (STRIDE)

☑ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☒ Manipulowanie danymi (Tampering with Data)
☒ Zaprzeczanie autorstwu operacji (Repudiation)
☒ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☒ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Luki w systemach

- Dirty Cow Linux – eskalacja uprawnień
- CloudFlare – ClouBleed (2017)

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(AIS) Bezpieczeństwo aplikacji	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(BCR) Zarządzanie ciągłością działania	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(CCC) Zarządzanie zmianą	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS, TVM) Zarządzanie podatnościami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Zarządzanie incydentami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Informatyka śledcza	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Separacja i segmentacja sieci	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Hardening	Dostawca

Klasyfikacja zagrożeń (STRIDE)

☑ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☑ Manipulowanie danymi (Tampering with Data)
☑ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☑ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Przejmowanie kont (account hijacking)

- Amazon – Botnet Zeus (2009), przejęcie danych uwierzytelniających (XSS, 2010)
- Code Space – przejęcie kontroli na panelem Amazon EC2 (DDos 2014)

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(IAM) Kontrola dostępu	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie tożsamością	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(BCR) Zarządzanie ciągłością działania	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(CCC) Zarządzanie zmianą	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(TVM) Zarządzanie podatnościami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Zarządzanie incydentami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Informatyka śledcza	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Hardening	Dostawca

Klasyfikacja zagrożeń (STRIDE)

☑ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☑ Manipulowanie danymi (Tampering with Data)
☑ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☑ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Malicious Insiders

- Zynga – kradzież poufnych danych przez pracowników przechodzących do konkurencji
- T-Mobile – dane 1,5 miliona klientów (2016

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(IAM) Kontrola dostępu	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie tożsamością	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(DCS) Bezpieczeństwo Centrum Danych	Dostawca
IaaS/PaaS/SaaS	(EKM) Szyfrowanie danych	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(HRS) Zarządzanie zasobami ludzkimi	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Zarządzanie incydentami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Informatyka śledcza	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Separacja i segmentacja sieci	Dostawca/Odbiorca
IaaS/PaaS/SaaS	STA (Zarządzanie łańcuchem dostaw)	Dostawca/Odbiorca

Klasyfikacja zagrożeń (STRIDE)

☑ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☑ Manipulowanie danymi (Tampering with Data)
☒ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☒ Ataki odmowy usługi (Denial of Service)
☒ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Advanced Persistent Threats

- NetTraveller – 40 krajów, 350 osób z wysokiego kierownictwa
- Kampania Carbanak - 1 mld $

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(IAM) Kontrola dostępu	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie tożsamością	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(CCC) Zarządzanie zmianą	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(EKM) Szyfrowanie danych	Odbiorca
IaaS/PaaS/SaaS	(TVM) Zarządzanie podatnościami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Zarządzanie incydentami	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Informatyka śledcza	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Separacja i segmentacja sieci	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Hardening	Dostawca

Klasyfikacja zagrożeń (STRIDE)

☒ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☒ Manipulowanie danymi (Tampering with Data)
☒ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☒ Ataki odmowy usługi (Denial of Service)
☑ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Utrata danych

- Sony – straty wycenione na 15 mln$
- Google 03.2011, Amazon 04.2011

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(GRM) Nadzór i zarządzanie ryzykiem	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(BCR) Zarządzanie ciągłością działania	Dostawca/Odbiorca

Klasyfikacja zagrożeń (STRIDE)

☒ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☒ Manipulowanie danymi (Tampering with Data)
☑ Zaprzeczanie autorstwu operacji (Repudiation)
☒ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☒ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Należyta staranność (Due Dilligence)

- Funkcjonalne
- Jurysdykcyjne (United States v. Microsoft Corp.-"Microsoft Ireland„)
- Kontraktowe

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(AAC) Audyt i zgodność	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(GRM) Nadzór i zarządzanie ryzykiem	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(HRS) Zarządzanie zasobami ludzkimi	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(BCR) Zarządzanie ciągłością działania	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(TVM) Działania operacyjne	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Zarządzanie incydentami	Dostawca/Odbiorca

Klasyfikacja zagrożeń (STRIDE)

☑ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☑ Manipulowanie danymi (Tampering with Data)
☑ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☑ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Wykorzystanie chmury do nadużyć

- Amazon Ddos backdoor
- Inception Framework 2014

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(HRS) Zarządzanie zasobami ludzkimi	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Informatyka śledcza	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(SEF) Zarządzanie incydentami	Dostawca/Odbiorca

Klasyfikacja zagrożeń (STRIDE)

☒ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☒ Manipulowanie danymi (Tampering with Data)
☒ Zaprzeczanie autorstwu operacji (Repudiation)
☒ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☒ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Odmowa usługi (Denial of Service)

- Dyn (2016) - Twitter, Github, SoundCloud, Spotify, Shopify
- GiftHub

Warstwa stosu SPI	Zabezpieczenie	Odpowiedzialność
IaaS/PaaS/SaaS	(AIS) Bezpieczeństwo aplikacji	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(GRM) Nadzór i zarządzanie ryzykiem	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(BCR) Zarządzanie ciągłością działania	Dostawca/Odbiorca

Klasyfikacja zagrożeń (STRIDE)

☒ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☒ Manipulowanie danymi (Tampering with Data)
☒ Zaprzeczanie autorstwu operacji (Repudiation)
☒ Ujawnienie informacji (Information Disclosure)
☑ Ataki odmowy usługi (Denial of Service)
☒ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Luki we współdzielonych zasobach

- Venom - virtualized environment neglected operations manipulation
- Vmware Directory traversal, Oracle VirtualBox – 3d accelertion

IaaS/PaaS/SaaS	(IAM) Kontrola dostępu	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie tożsamością	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IAM) Zarządzanie dostępem	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(EKM) Szyfrowanie danych	Odbiorca
IaaS/PaaS/SaaS	(GRM) Nadzór i zarządzanie ryzykiem	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Logowanie i wykrywanie intruzów	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(IVS) Separacja i segmentacja sieci	Dostawca/Odbiorca
IaaS/PaaS/SaaS	(TVM) Zarządzanie podatnościami	Dostawca

Klasyfikacja zagrożeń (STRIDE)

☒ Przejęcie i podszycie się pod czyjąś tożsamość (Spoofing Identity)
☒ Manipulowanie danymi (Tampering with Data)
☒ Zaprzeczanie autorstwu operacji (Repudiation)
☑ Ujawnienie informacji (Information Disclosure)
☒ Ataki odmowy usługi (Denial of Service)
☑ Podniesienie poziomu uprawnień (Elevation of Privilege)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Podsumowanie

Krok 1 – co przenosimy

Usługi, procesy, dane, aplikacje

Krok 2 – co chronimy

Poufność, dostępność, integralność

Krok 3 – zgodność

Normy, regulacje, standardy

Krok 4 – jak chronimy

Ludzie, procesy, technologia

Krok 5 – ocena ryzyka

Krok 6 - architektura

Analiza modelu chmury i dostawcy

Krok 7 - Środowisko

Konfiguracja, kopie zapasowe

Krok 8 - testy

Wydajność, bezpieczeństwo, funkcjonalność

Krok 9 - umowa

Komunikacja, prawo do audytu, odpowiedzialność

Krok 10 - uruchomienie

Uruchomienie usług w wersji produkcyjnej

Krok 11 - współpraca

Komunikacja, rozwiązywanie problemów, reagowanie na incydenty