Hybrid cloud infrastructure security challenges and pitfalls

2022
ALMATY
KAZAKHSTAN

TOLTARYS
KAZHACKSTAN

01 —— About me

Head of infrastructure and platform security at Yandex.

Used to play CTFs.

CTFtime.org maintainer.

Eldar Zaitov

02 —— What is hybrid cloud?

Traditional DC	IaaS	PaaS	SaaS
Data	Data	Data	Data
Applications	Applications	Applications	
Container	Container		
OS	OS		
Virtual Network	Virtual Network		
Hypervisor			
Hardware			
Physical Network			

~400B

2022 Worldwide Public Cloud Services Spending End-User Forecast (IaaS, PaaS, SaaS) by Gartner

03 —— Cloud challenges

- —— Legal
- —— Billing
- —— Authentication
- —— Authorization and Identity management
- —— Inventory
- —— Networking
- —— Logs

04 —— Legal

—— Policies

—— Certifications

- SOC 2/3

- ISO 27001

...

Questionaries help

05 —— Billing

- —— Budget
- —— Billing policy

Nice control point!

06 —— Authentication

—— Single Sign On (SSO)

- ADFS
- Okta
- ...

—— 2FA / MFA

- TOTP
- Hardware tokens
- Push OTP
- 3rd party solutions (Okta, Duo, ...)

—— Access policies

07 —— Identity management (IDM) and access controls

—— Role presets
- DevOps
- Administrator
- Network manager
- Auditor
- ...

—— Azure AD + SCIM

—— Temporary roles

IAM is your friend

07 —— Identity management (IDM) and access controls

—— Role presets
- DevOps
- Administrator
- Network manager
- Auditor
- ...

—— Azure AD + SCIM

—— Temporary roles

Роль	Описание	Тип
Автор полезных данных атаки	Может создавать полезные данные атаки, для которых адми...	Встроенное
Администратор Аналитики компьютеров	Может получать доступ к службам и средствам управления к...	Встроенное
Администратор атрибутов потоков пользователей с вн	Может создавать схему атрибутов, доступную для всех поток...	Встроенное
Администратор базы знаний	Может настраивать базы знаний, обучение и другие интелле...	Встроенное
Администратор безопасности	Может просматривать отчеты и сведения для защиты, а такж...	Встроенное
Администратор виртуальных посещений	Может просматривать сведения и метрики виртуальных пос...	Встроенное
Администратор внешнего поставщика удостоверений	Может настраивать поставщики удостоверений для использ...	Встроенное
Администратор выставления счетов	Может выполнять основные задачи по выставлению счетов, ...	Встроенное
Администратор гибридных удостоверений	Может управлять облачной синхронизацией Azure AD на баз...	Встроенное
Администратор групп	Может управлять всеми аспектами групп и параметрами гру...	Встроенное
Администратор данных соответствия	Может создавать и контролировать данные по соответствию...	Встроенное
Администратор доменных имен	Может управлять доменными именами в облаке и локально.	Встроенное
Администратор лицензий	Возможность назначать, удалять и изменять лицензии.	Встроенное
Администратор набора ключей IEF B2C	Может управлять секретами для федерации и шифрования в...	Встроенное

08 —— Service accounts and secrets management

- —— Super Power
- —— No credentials rotation by default
- —— No access policies

- —— Every cloud has its own secrets management solution

09 —— Inventory

—— Every cloud has specific resources and technologies

—— You need an inventory

- Cloudquery

—— Infrastructure as a code

- Terraform

10 —— Networking

—— IP Layout
—— Firewall
—— Load Balancing
    - TLS termination
    - DDoS protection
—— Infrastructure connectivity
    - Tunnels
    - Direct Connect
    - VPN

11 —— Logs

—— Logs
- Cloudtrails
- Azure Log Monitor
- ...

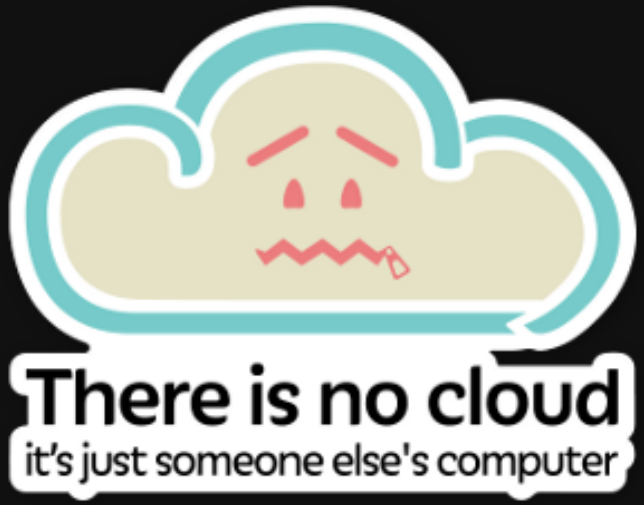
—— Custom fields and events

—— SIEM

Give your SOC a hug

12 —— Cloud security is your responsibility

Public clouds can give you powerful security tools and controls but demand your infrastructure and processes to be mature enough.



13 —— Thank you!

Questions?

@kyprizel