



How to harden access to your cloud infrastructure and resources

Vladimir Stefanović



Thank you to our wonderful sponsors











































Who am I

- Vladimir Stefanović
- System Engineer @SuperAdmins
- Technical Trainer @ATC
- MCSA, MCSE, MCT, IAMCT Regional Lead, Speaker
- SysAdmin UG and Azure UG Serbia leader
- stefanovic.vladimir@hotmail.com
- www.tech-trainer.info
- https://github.com/Wladinho/Presentations

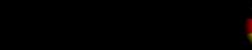


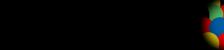


Work smarter, not harder

And try to avoid situation on picture . . .







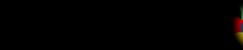


What is a goal of hardening?

- Your infrastracture and resources are more resistant
- Your client is happier
- You sleep more peacefully
- In case of emergency, you have more time to react











What need to be hardened?

- Access to tenant
- User management & Password Policy
- MFA (Multi-factor Authentication)
- Conditional Access
- Resources
- IAM (Identity Access Management)
- Network
- NSG (Network Security Group)
- Firewall











Tenant (Cloup App) Access

- User management & Password Policy
- Try to avoid so many Global Admins
- MFA (Multi-factor Authentication)
- Force "critical" users and Global Admins to use MFA
- Easy to configure, not expensive
- Conditional Access
- Buy licenses and play ©











Resources and Network Access

- IAM (Identity Access Management)
- Role Based Access Control
- Carefully select appropriate role
- Can be placed on so many "levels", from subscription to single resource
- Network Access can be protected with
- NSG (Network Security Group)
- Firewall





Demo

Text



Thank you to our wonderful sponsors

























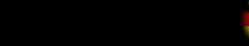


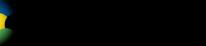






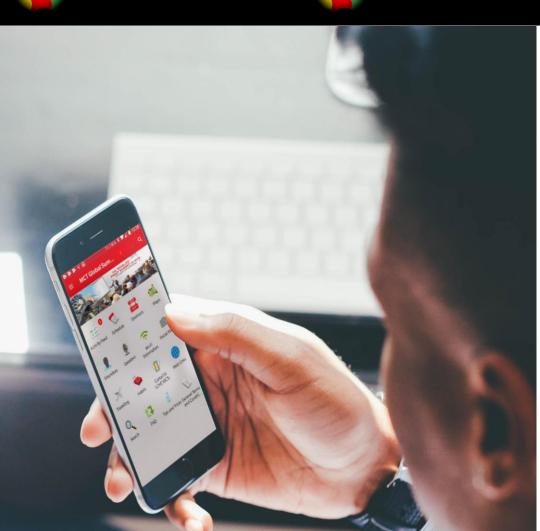












Please evaluate this session

Your feedback is important to us!

Please evaluate this session through MyEvaluations on the mobile app or website.

Download the app:

https://l.ead.me/mct-mobileapp

Go to the website:

https://events.crowdcompass.com/mctsummit



