glomex
THE GLOBAL MEDIA EXCHANGE

HOW TO MANAGE A MULTI AWS ACCOUNT INFRASTRUCTURE

A short introduction: Why, how and dodging bullets

amazon web services
Munich AWS User Group

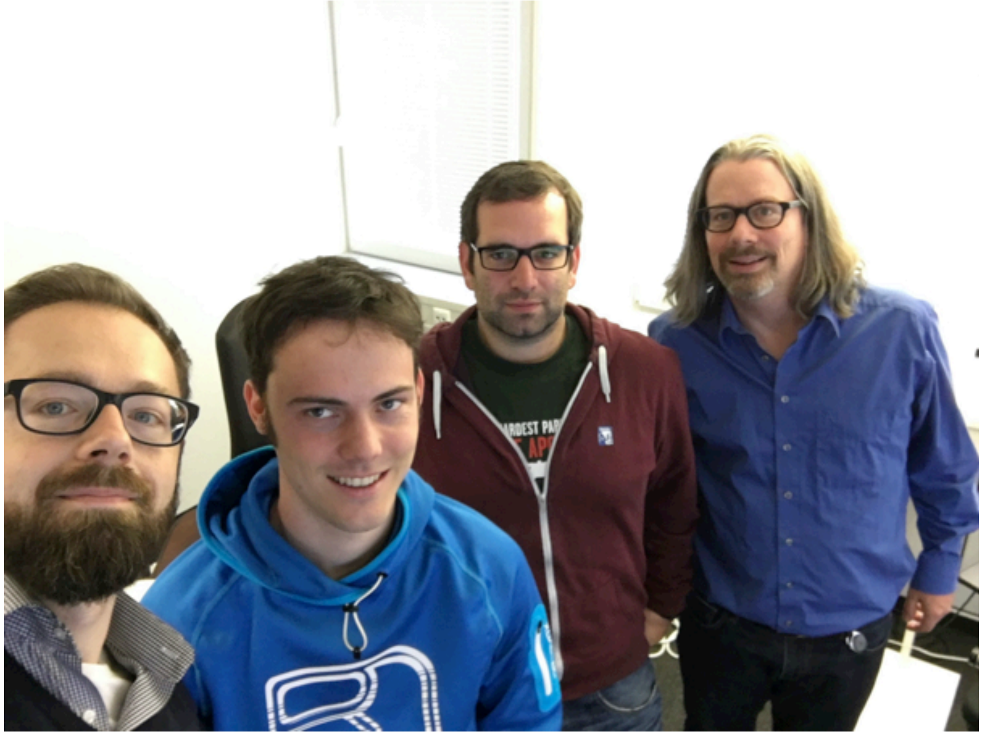
Andreas Sieferlinger
Unterföhring, 17.10.2016

INTRO

Andreas Sieferlinger

Team OPS tasks:

- base architecture
- AWS base setup
- tools and frameworks for teams
- AWS consulting for internal teams



AGENDA

WHY
would I want a multi account setup?

HOW have we implemented this?

WHICH pitfalls did we experience?

WHICH tools do we use?

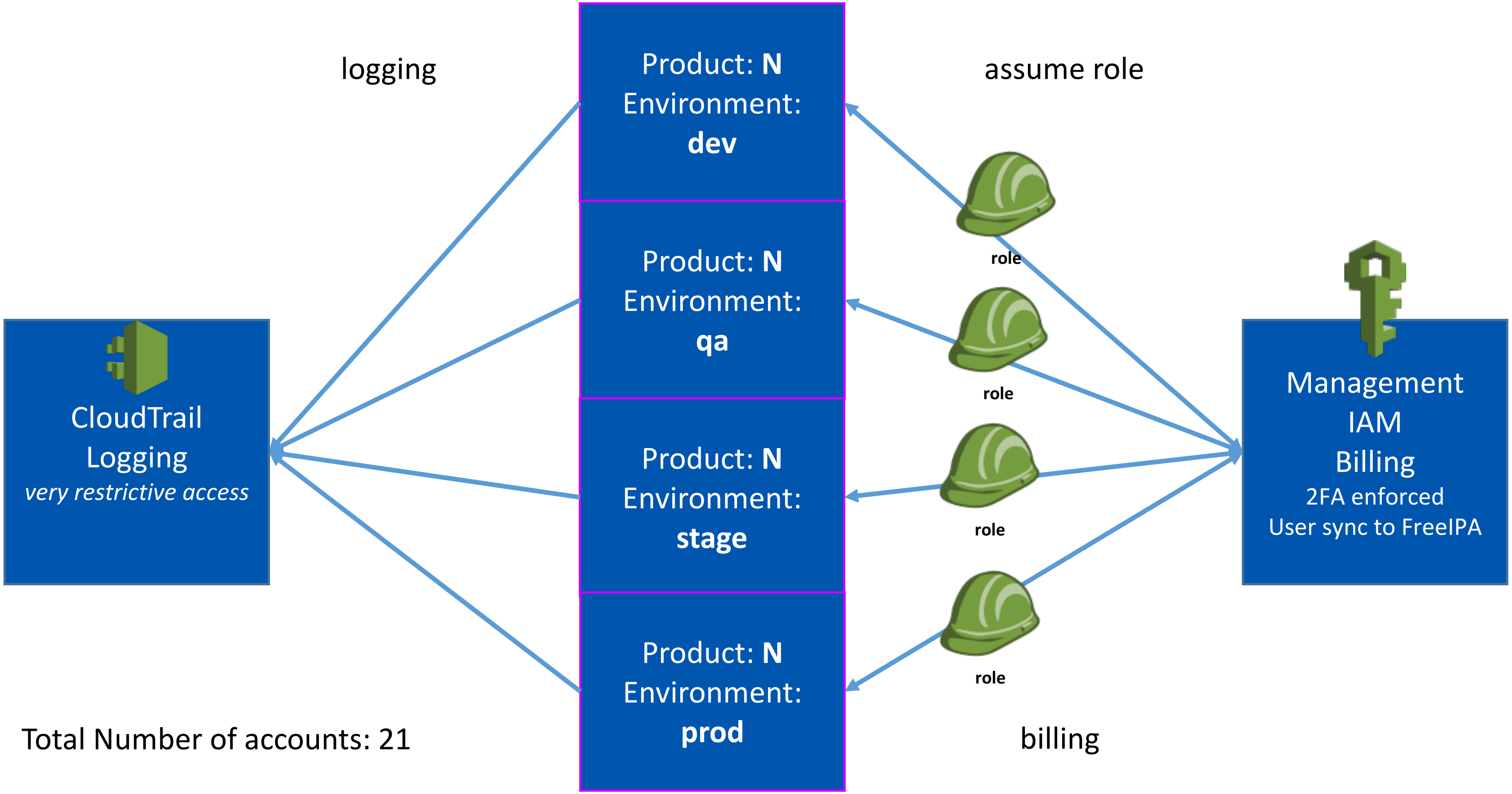
WHY?

- AWS recommendation (depending on your setup)
- separate billing
- fine grain access control / security
- mimic organization setup
- separate stages / environments
- → minimize blast radius

WHY A SINGLE ACCOUNT IS BAD

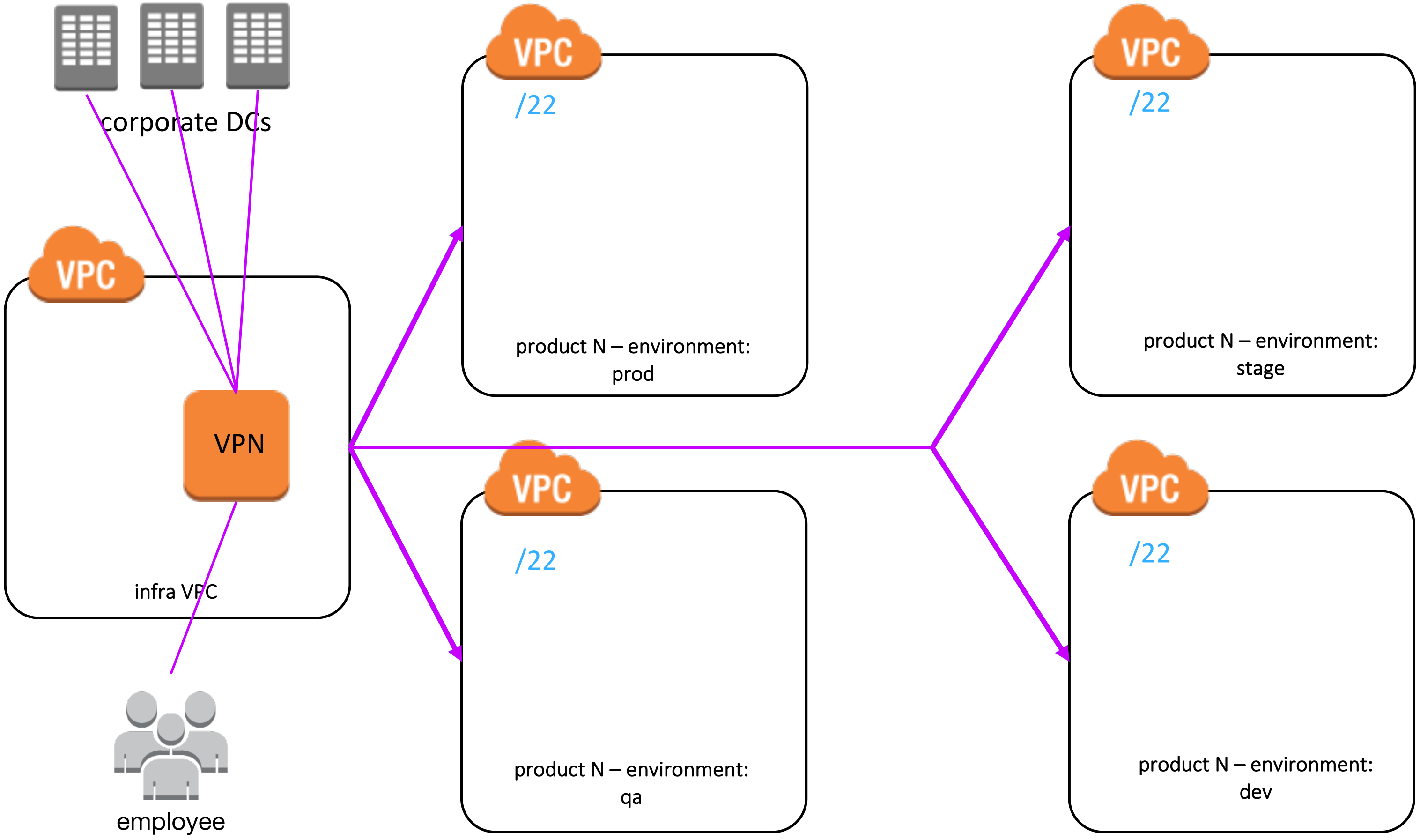
- account limits / capacity planning
- API rate limits
- complicated access control for certain resources (ec2)
- complicated deprovisioning of complete products

ACCOUNT STRUCTURE



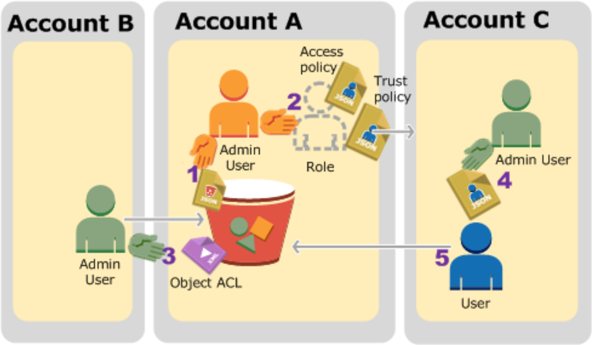
Total Number of accounts: 21

NETWORK STRUCTURE (WITHIN A SINGLE REGION)



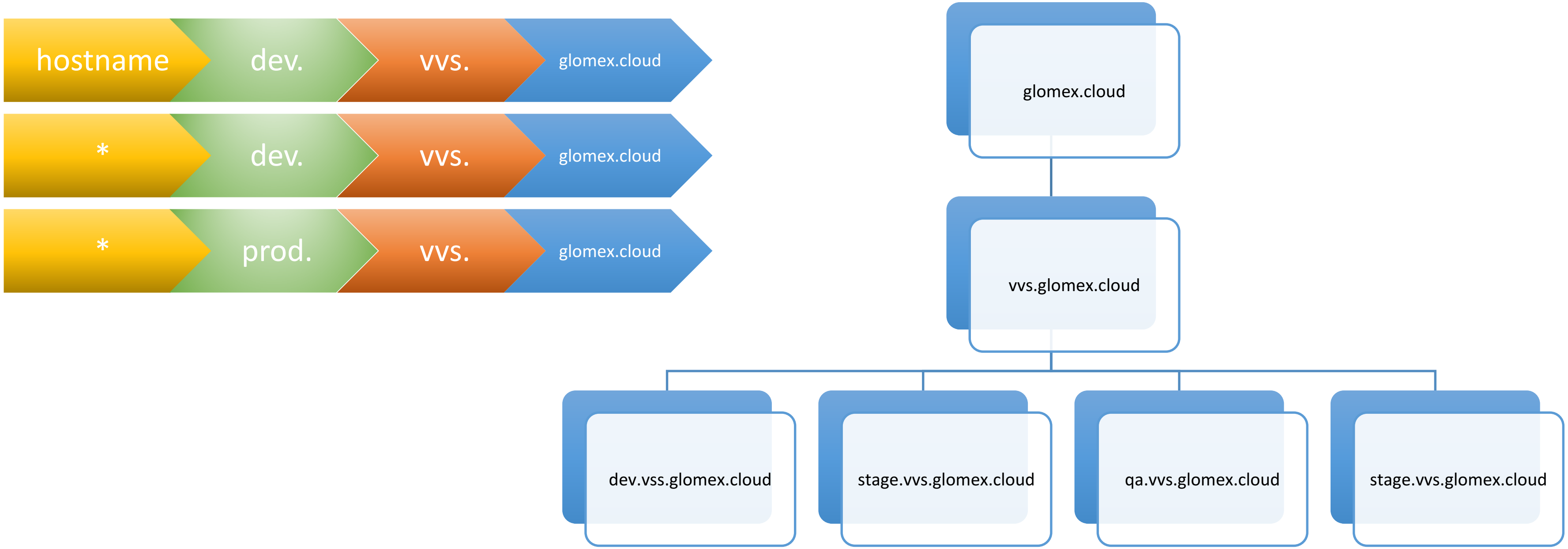
PAIN

- Tool support for cross-account access is meh…
  - kinesis agent (since 16.09.2016, IAM roles are supported!)
  - many tools do not (easily) support profiles / roles → aws-mfa
  - cli with many accounts and MFA will slow you down
- AWS support for cross account access could be better ...
  - public VPC security groups
  - complex trust relationships
  - S3 Buckets 3+ account relationships



DNS ZONE DELEGATION

- DNS Zone separation
  - cross account DNS for corporate domain too complicated -> complex DNS
  - many SSL certificates required (ACM not available for all services)



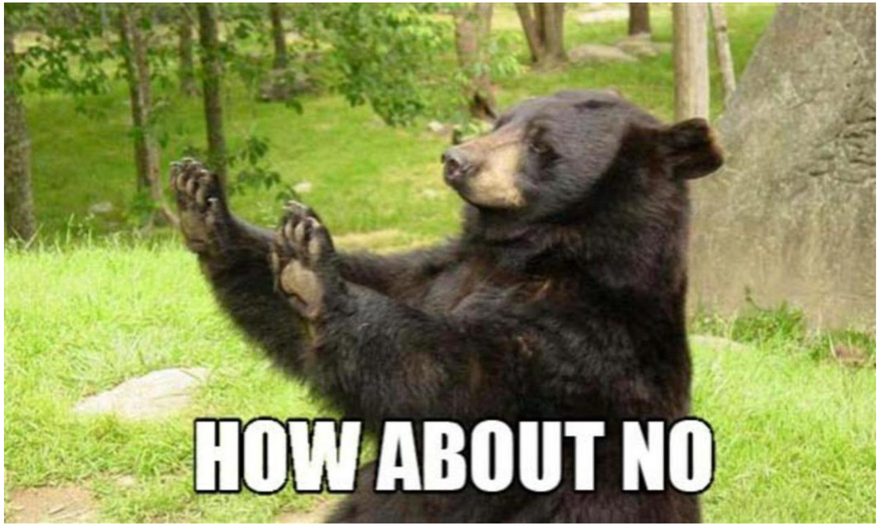
PAIN 2

- complex networking setup
  - peering / routing easily gets out of hand
  - try to keep it simple!
- No single point of view over all accounts/metrics/monitoring with AWS services/tools
  - tools like datadog and security monkey help
- Costs and effort may multiply per account (config rules, support, vpn connections, management, ssl certs).
  About $70 per account in our environment
- User support and education more demanding
- **Everything solved or found feasible workarounds!**

EDUCATE YOUR USERS

Request from developer: „We extended the instance base policy, but cannot enable it, please roll out for all“

```
{
            "Effect": "Allow",
            "Action": "autoscaling:*",
            "Resource": "*"
},
{
            "Effect": "Allow",
            "Action": "elasticloadbalancing:*",
            "Resource": "*“
}
```



Users are unaware of potential problems they create. Educate!

TOOLS

- FreeIPA is source of authentication
- FreeIPA to AWS IAM sync tool (no SAML)
- FreeIPA SSH Key User Management on instances
- aws-mfa
- Account / environment detection on instances to avoid bad things
- security monkey
- DataDog
- Base setup tool: “kiso”: manages all accounts
  - (CloudFormation / tropossphere + config + tooling)
  - Account creation automation (about 80%)
- custom application rollout tools: glomex cloud deployment tools (gcdt)
  - Kumo (cloudformation)
  - Tenkai (codedeploy)
  - Yugen (API gateway)
  - Ramuda (lambda)

LINKS

When to use AWS Multi Account Setups

https://aws.amazon.com/de/answers/account-management/aws-multi-account-security-strategy

S3 configuration for use with 3 accounts

http://docs.aws.amazon.com/AmazonS3/latest/dev/example-walkthroughs-managing-access-example4.html

aws-mfa tool

https://github.com/broamski/aws-mfa

Security Monkey

https://github.com/Netflix/security_monkey

Slides

https://speakerdeck.com/andreassieferlinger

glomex techblog

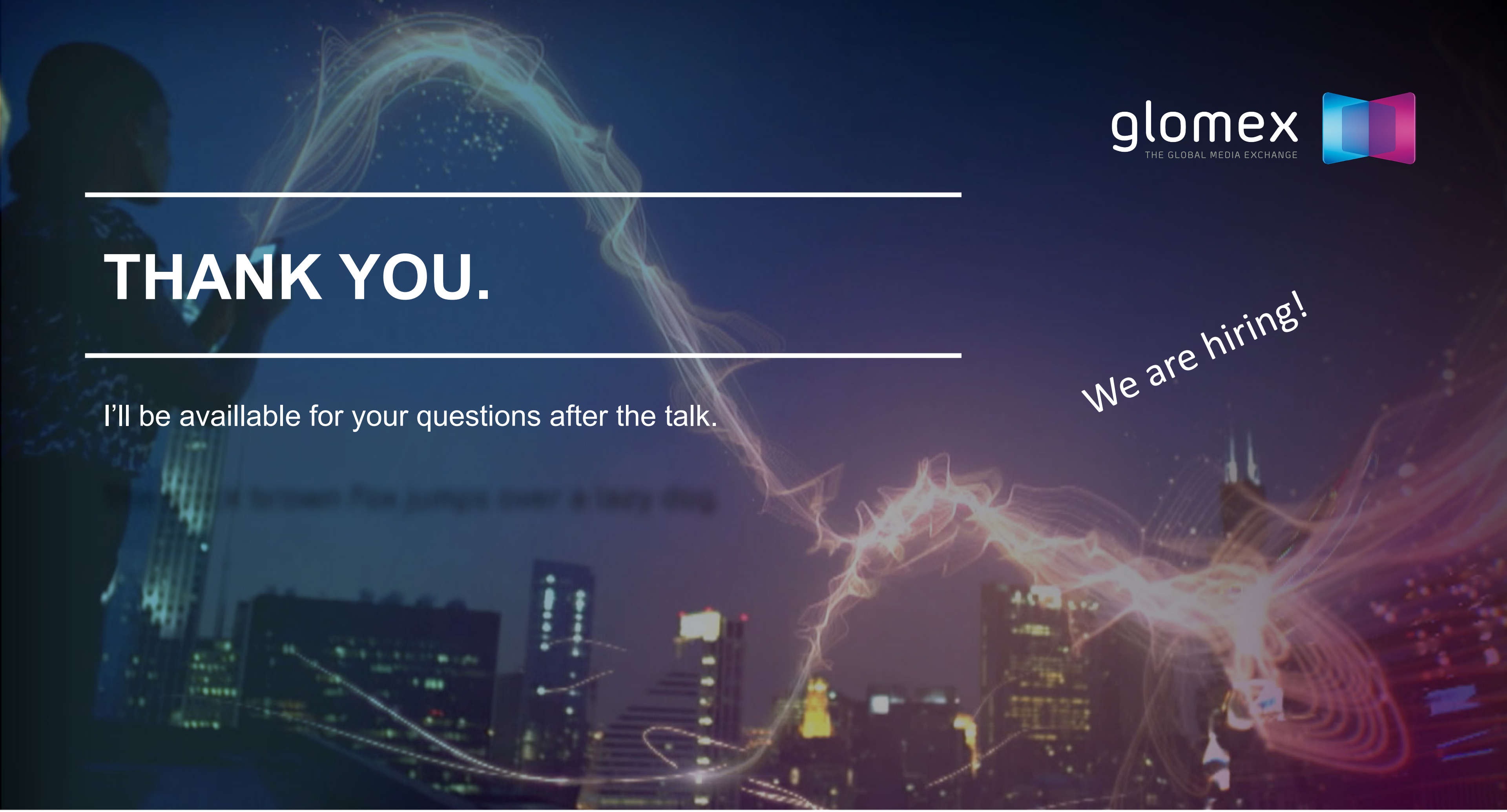
coming soon

glomex
THE GLOBAL MEDIA EXCHANGE

Q & A

Short questions regarding the presentation
More time after the talk!

Andreas Sieferlinger
Unterföhring, 17.10.2016



glomex
THE GLOBAL MEDIA EXCHANGE

THANK YOU.

I’ll be availlable for your questions after the talk.

We are hiring!

Andreas Sieferlinger
Unterföhring, 17.10.2016