SANS

Nills Franssens

Microsoft

Summit Talk

Automating Network Firewall Rule Creation Using Powershell and CI/CD

Cloud Security
Summit & Training

San Jose, CA
April 29-30

Nills Franssens

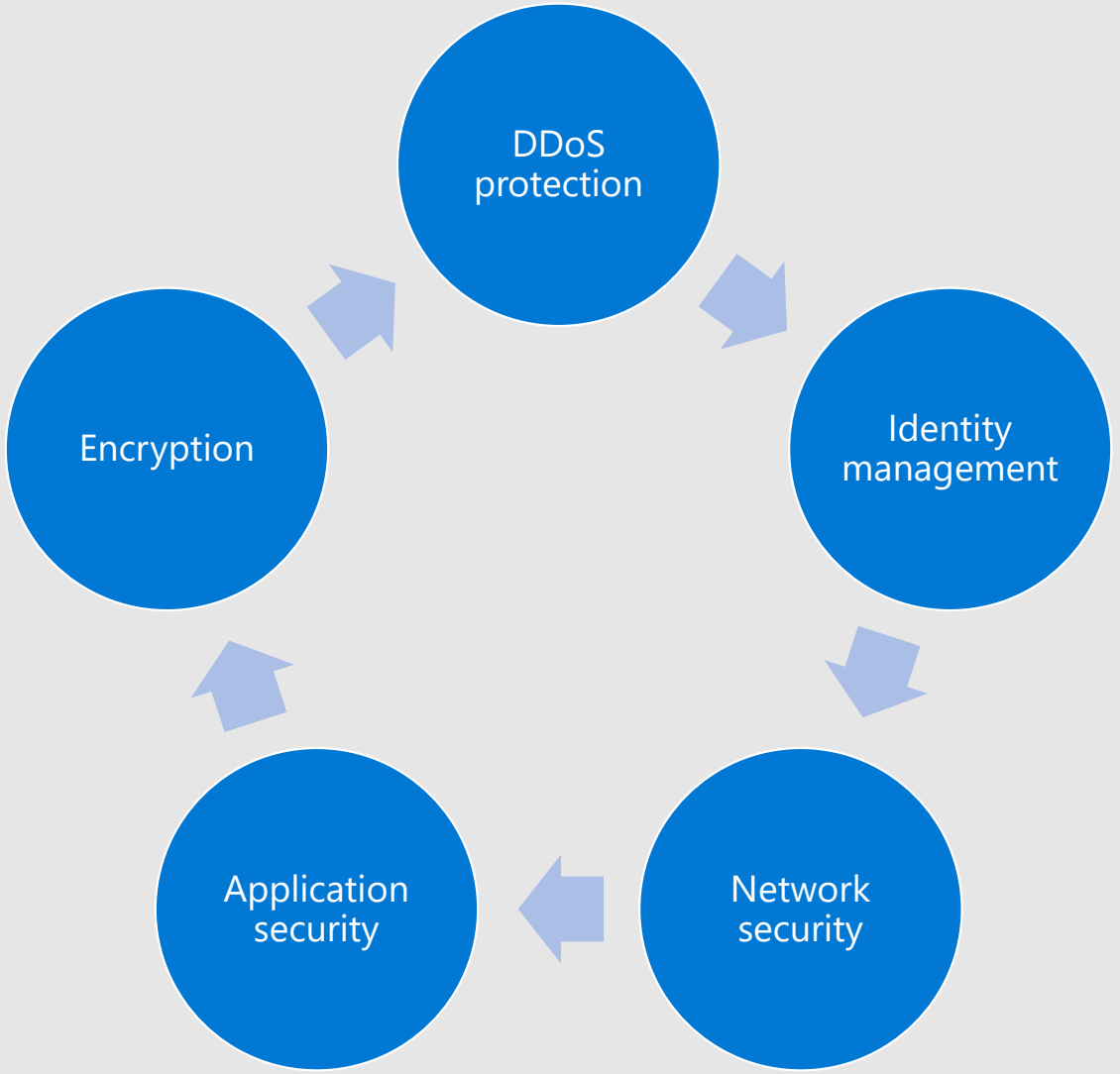
Runner

Belgian in the US

Cloud Solution Architect @ Microsoft

- Infrastructure
- Networking
- Open Source

Setting the context: Cloud Security



Cloud Network Security on L3/L4 - Implementation

All major cloud providers offer a native L3/L4 firewall capability (Security Group)

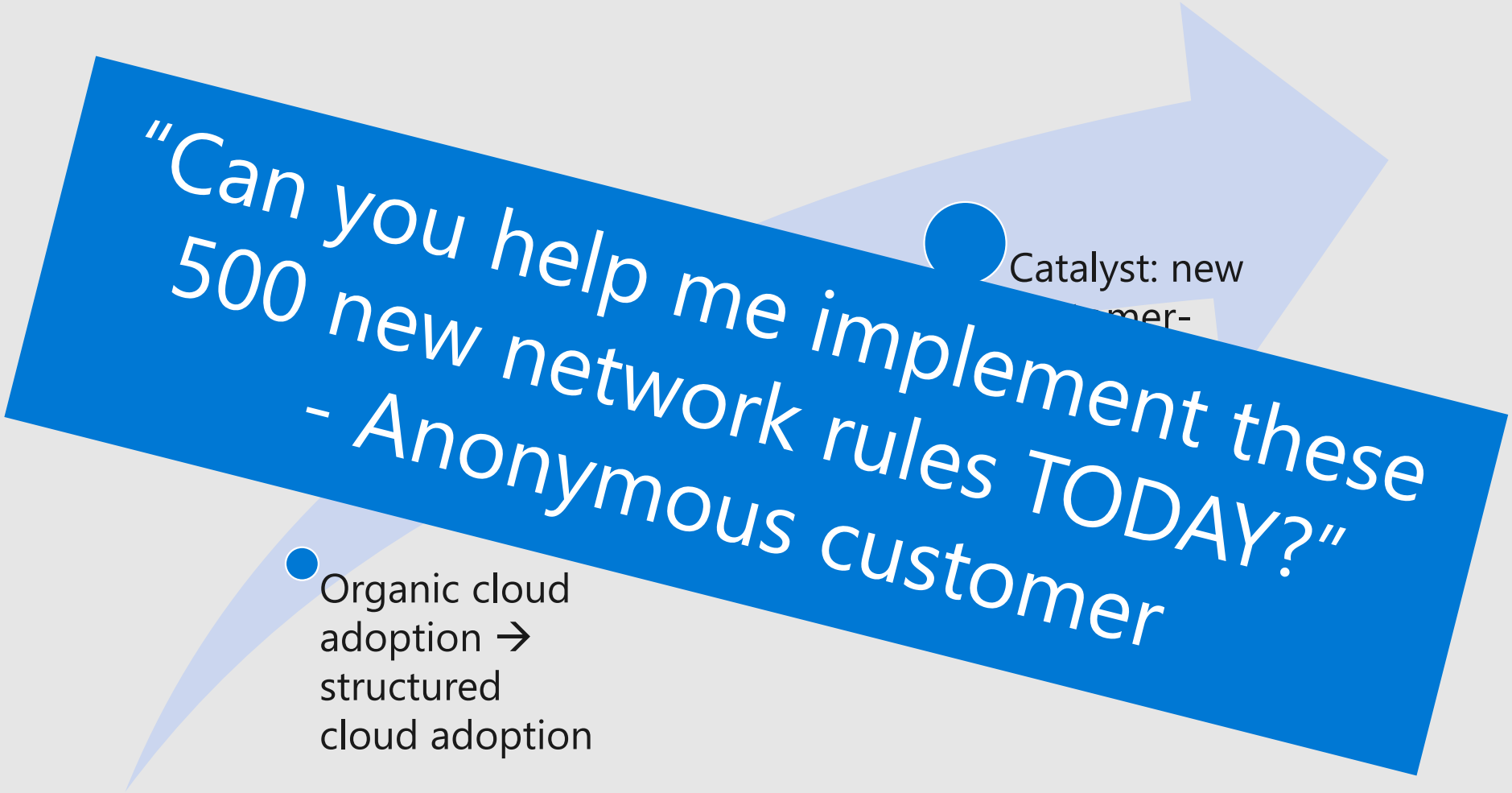
Common elements

- ~Like ACLs
- Instance tagging – security groups
- Stateful
- An object

Differences

- AWS has 2 implementations: security groups and network ACL
- Azure allows IP-based and security group based rules mixed
- Assigned to different levels: AWS is instance level, Azure is instance or subnet level, GCP is VPC level

Customer use case driving this solution.



This called for an automated solution.

Human error.

What if we needed to do it all over again?

What if this needs to repeated for a second region?

We only had half a day to do this right.

imperative

or

declarative

Highly parallel

Single API call

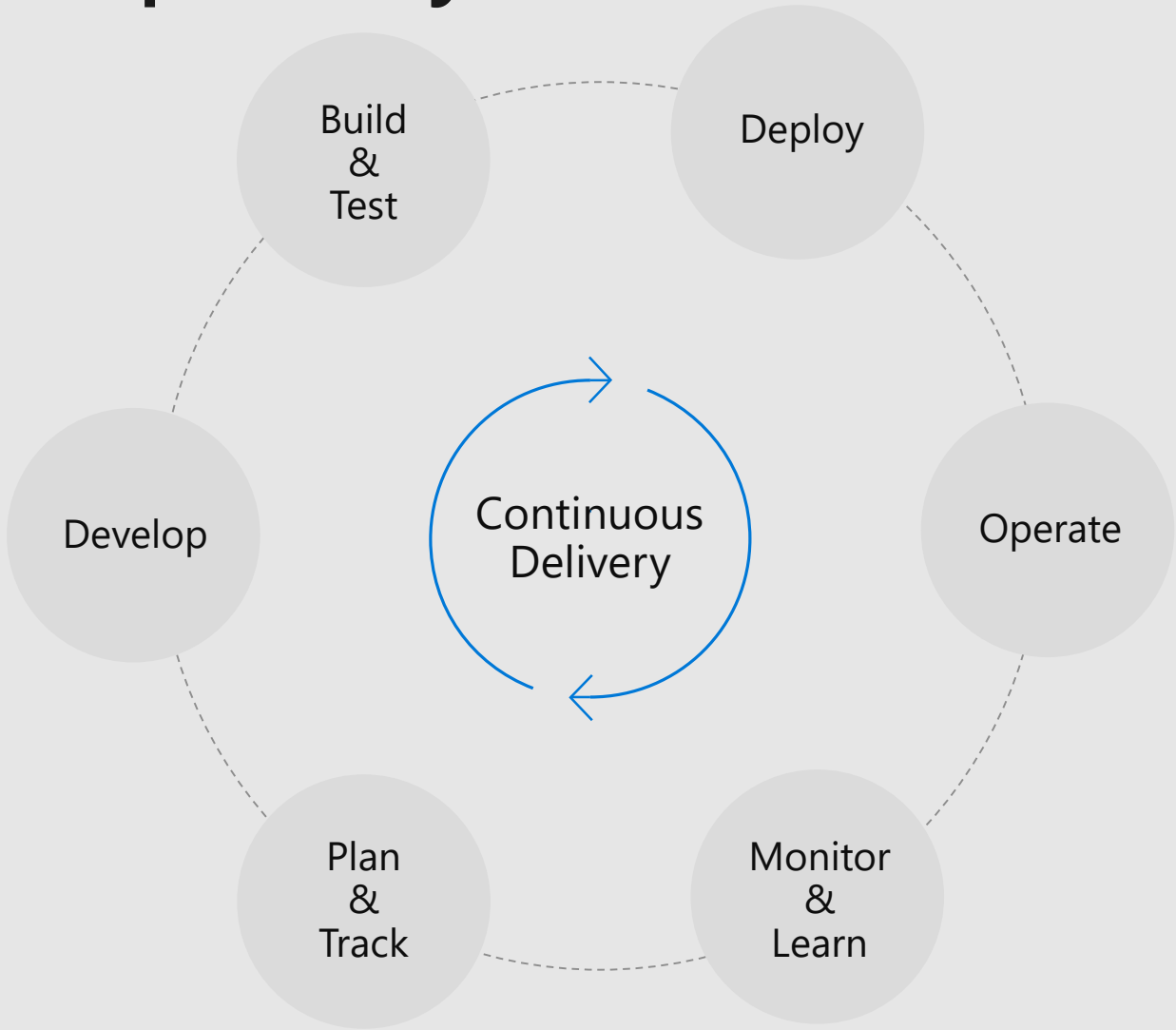
Source code

"contentVersion": "1.0.0.0",

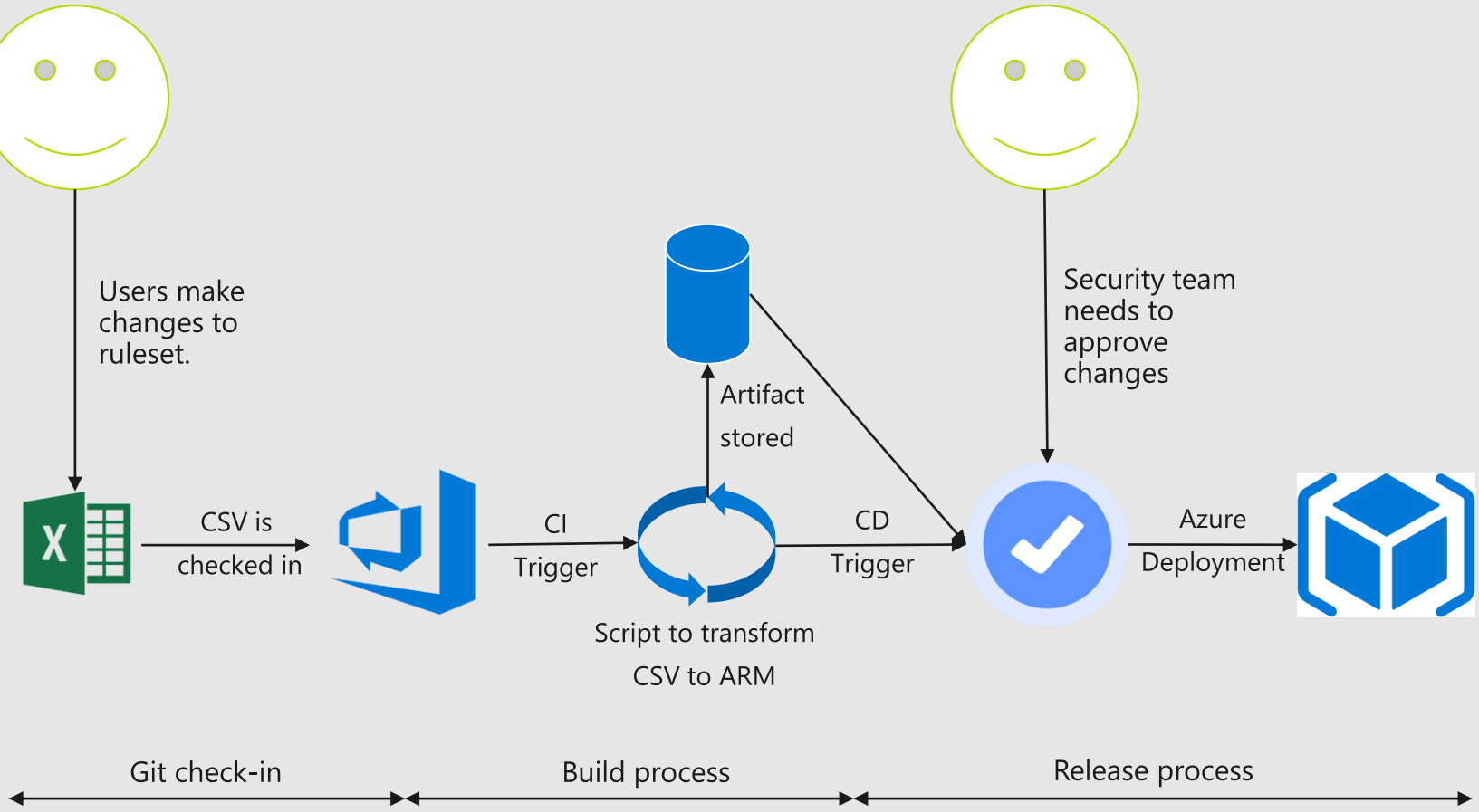
We needed to decide

Automation in step 1 in a DevOps Lifecycle.

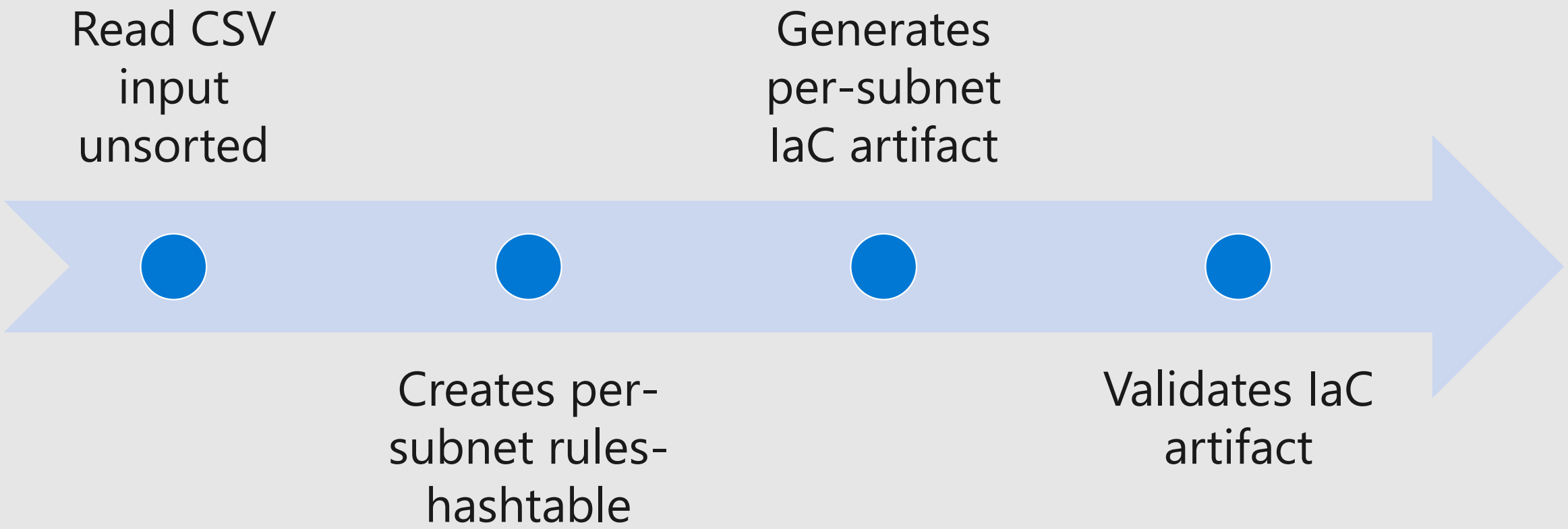
“DevOps is the union of **people**, **process**, and **products** to enable continuous delivery of value to your end users.”



End-to-end solution overview



Script walkthrough



Demo

Outcomes / Benefits

- Implemented 500 firewall rules in half a day
- Flexible way to adapt firewall rules afterwards
- Security review built-in to process
- Standard format for developers to request firewall changes
- Happy customer