Microsoft Azure

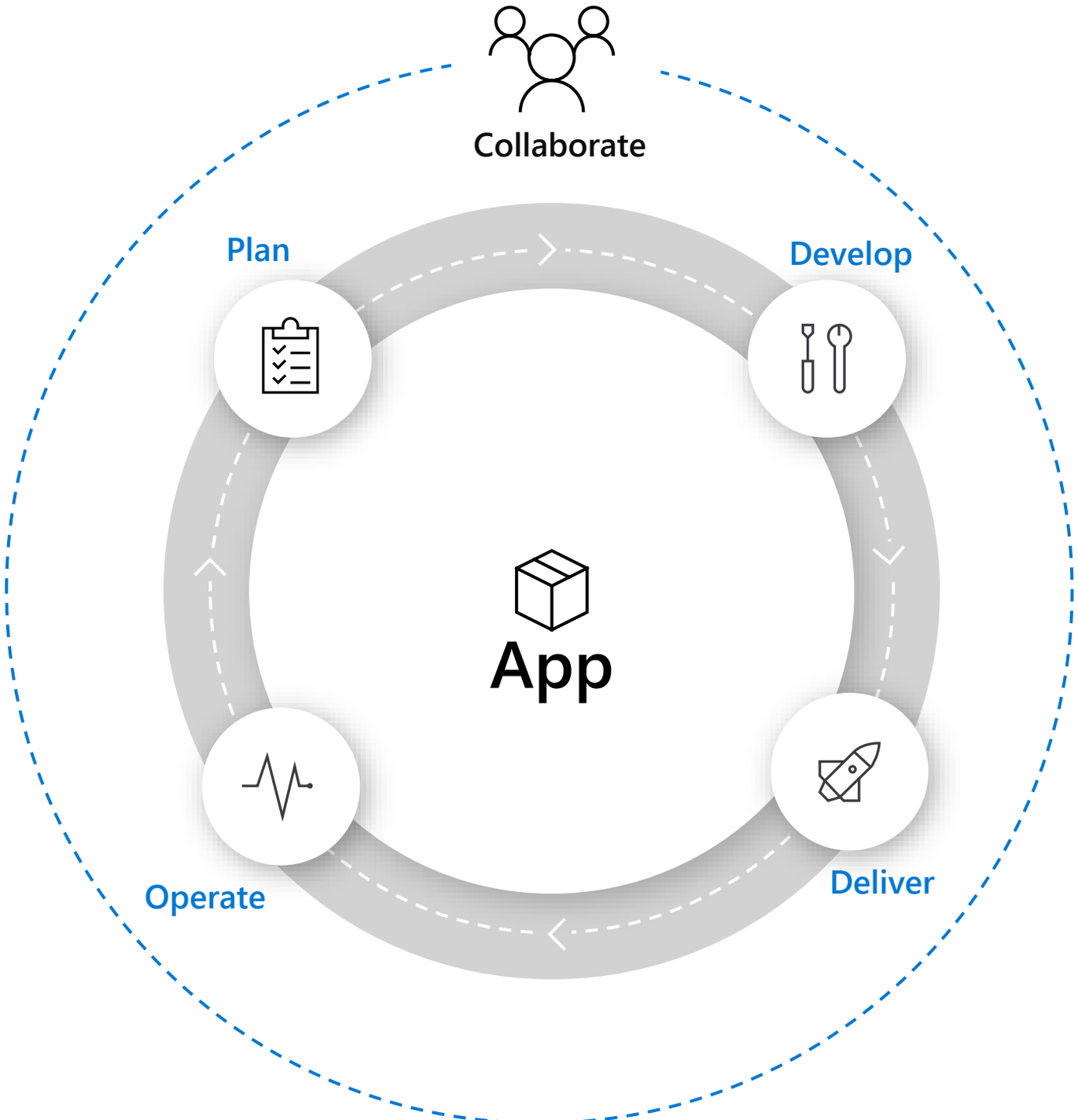
DevOps Security Best Practices with Microsoft Azure

Wai Man Hui
28 Jan 2021

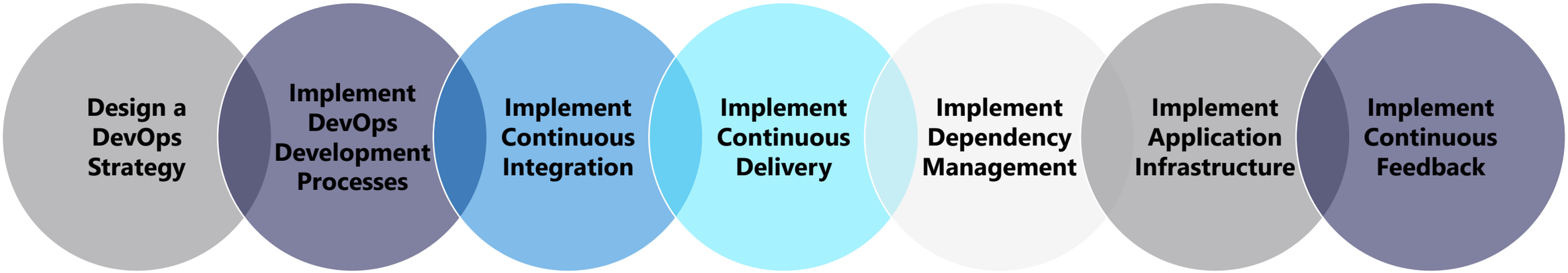
Introduction

Modern app engineering is enabled by DevOps

> DevOps is the union of people, process, and technology to enable continuous delivery of value to your end users.



Microsoft Azure DevOps Solutions Objectives



DevOps practices improve security

Proper DevOps practices make your application development more secure, technology is available to help, but don't forget about the people and the processes

PEOPLE

- Education
- Security first mindset
- Assumed breach
- Protect credentials

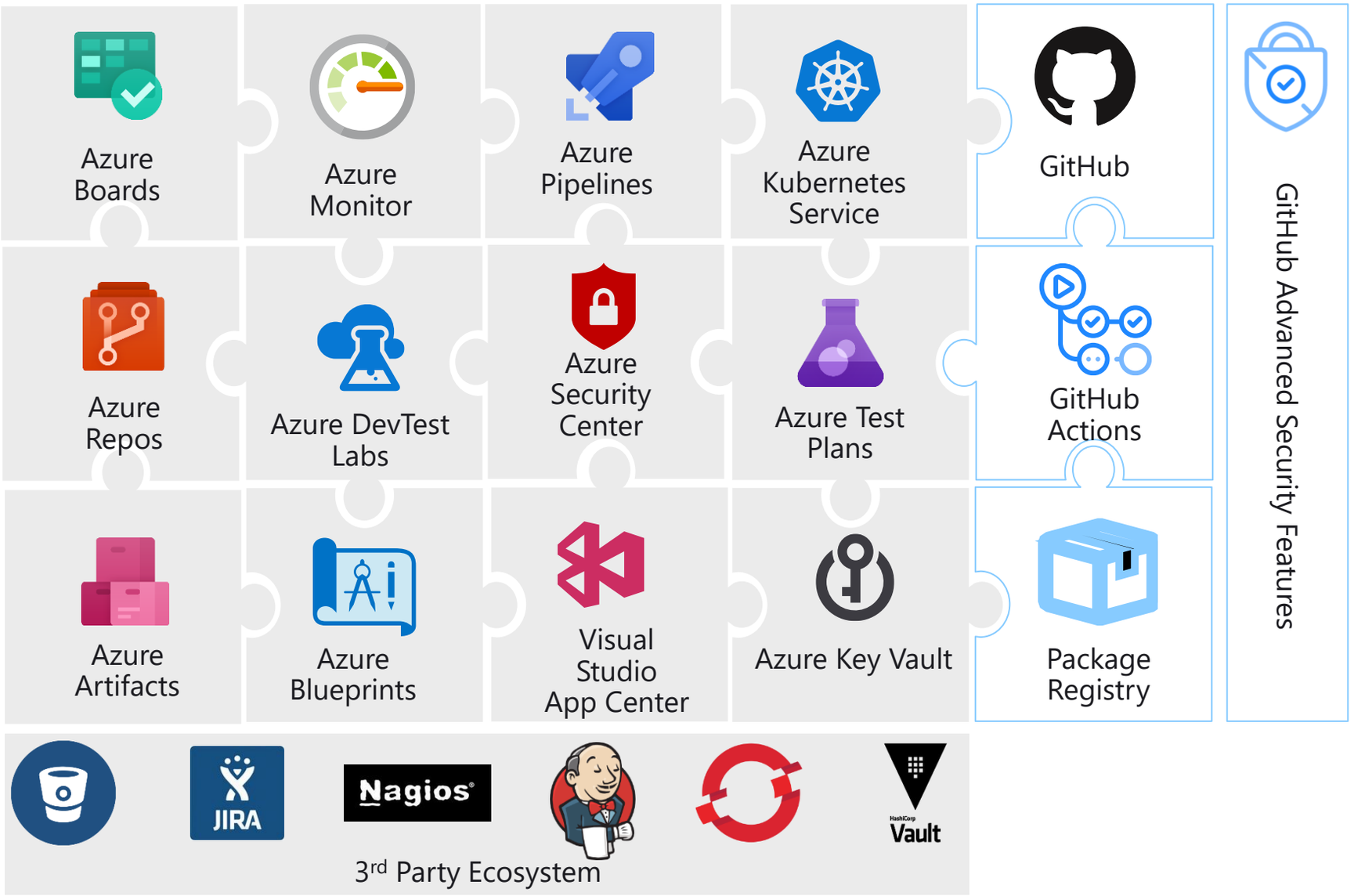
PROCESSES

- Secure development lifecycle
- Threat modeling
- Security assessments
- Red-blue team exercises (pen test)
- Code reviews
- Limited production access
- Immutable infrastructure
- Progressive exposure/ canary deployments

TECHNOLOGY

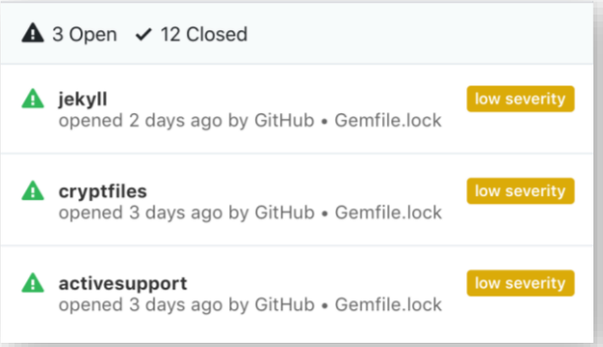
- Release automation
- Infrastructure/config as code
- Static App. Security Testing (SAST)
- Dynamic App. Security Testing (DAST)
- Credential scanning
- Secrets management
- Known vulnerabilities
- License risks

DevOps on Azure – native and third-party services ...enhanced by GitHub



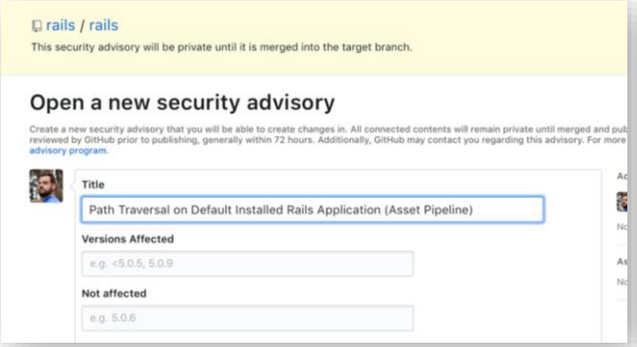
Securing your Software Supply Chain

GitHub gives your teams powerful tools to identify issues with the open source code your app depends on.



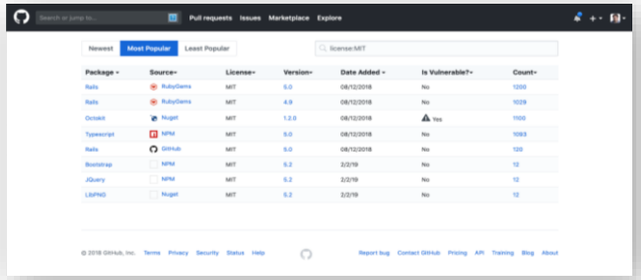
Get automatic alerts and patches with **vulnerability scanning and remediation.**

Automatic scanning and notifications for vulnerabilities; automatic pull requests to patch vulnerable code.



Investigate and fix vulnerabilities safely and privately with **security advisory workflows.**

Tools for scanning, investigation and remediation of security issues in your projects.



View and manage open source dependencies and licenses with **dependencies insights.**

Understand what your project is using, and the health, security, and license information of your software dependencies.

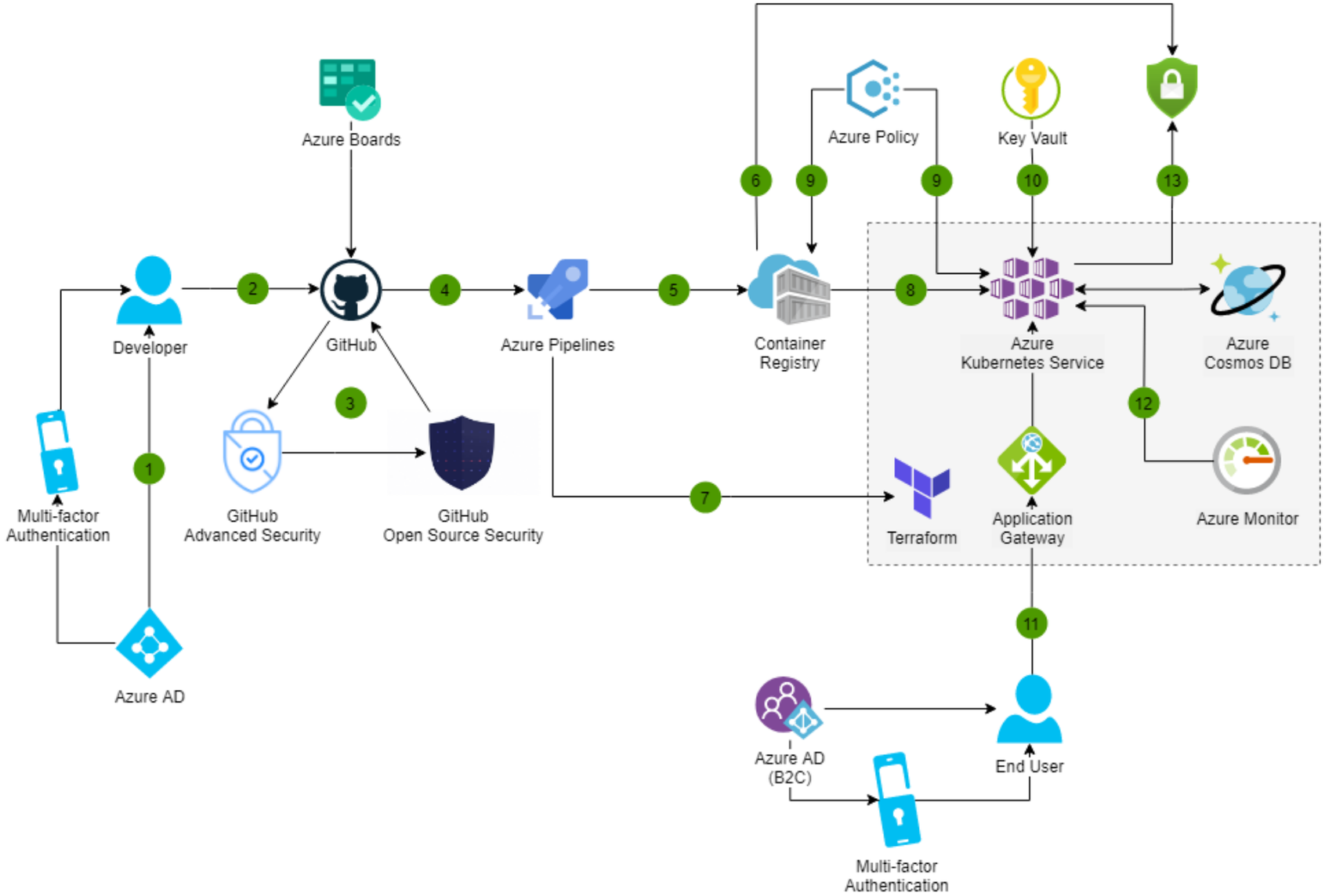
Sample Architecture

DevSecOps in Azure

1. Azure Active Directory (AD) can be configured as the identity provider for GitHub

2. GitHub Commit tracked by Azure Board

3. GitHub Enterprise can integrate automatic security and dependency scanning through GitHub Advanced Security and GitHub Open Source Security.

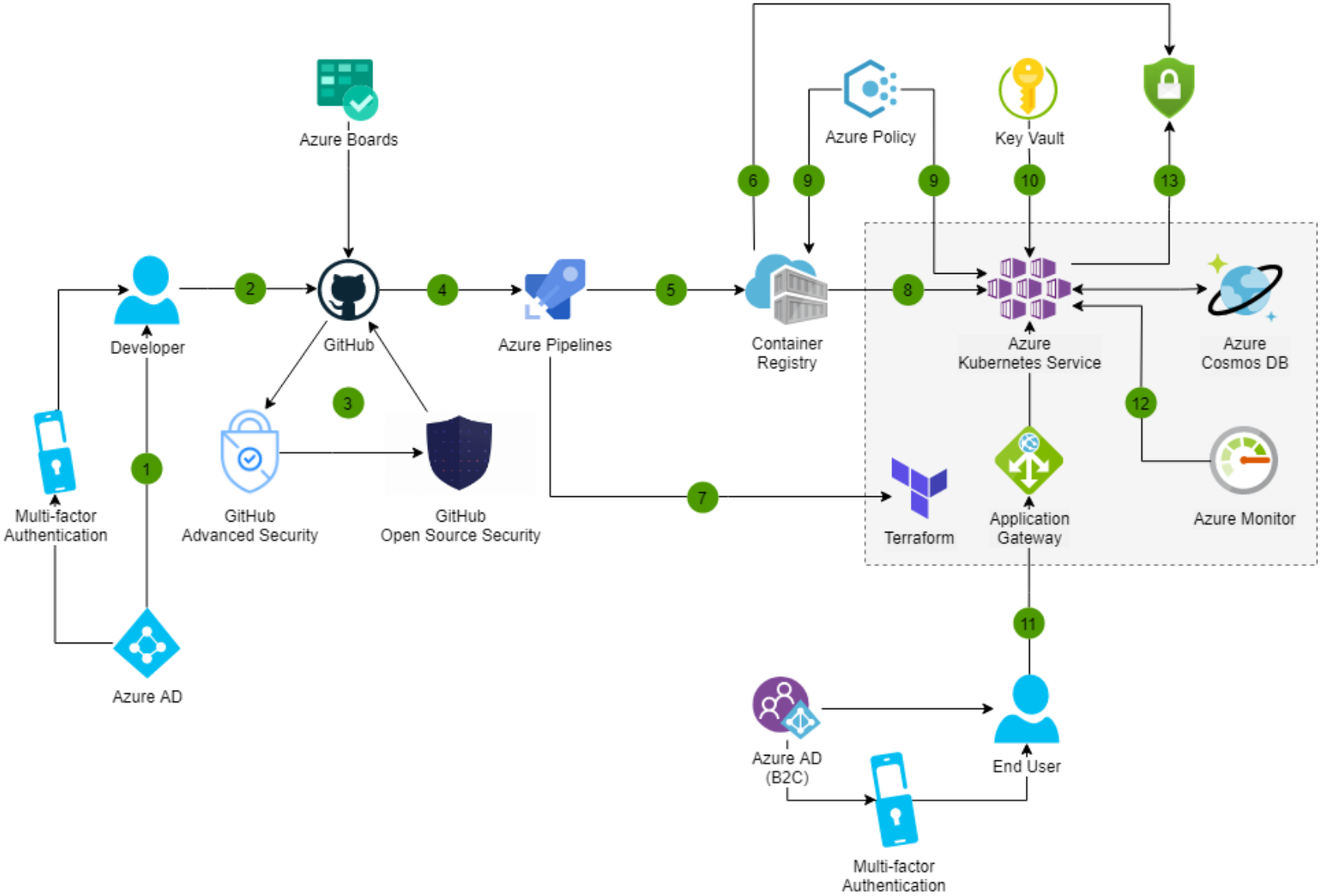


DevSecOps in Azure

4. Pull Requests trigger CI builds and automated testing in Azure Pipelines

5. CI build generates docker image and stores in Azure Container Registry

6. Azure Security Center will scan the pushed image for Azure-native vulnerabilities and for security recommendations



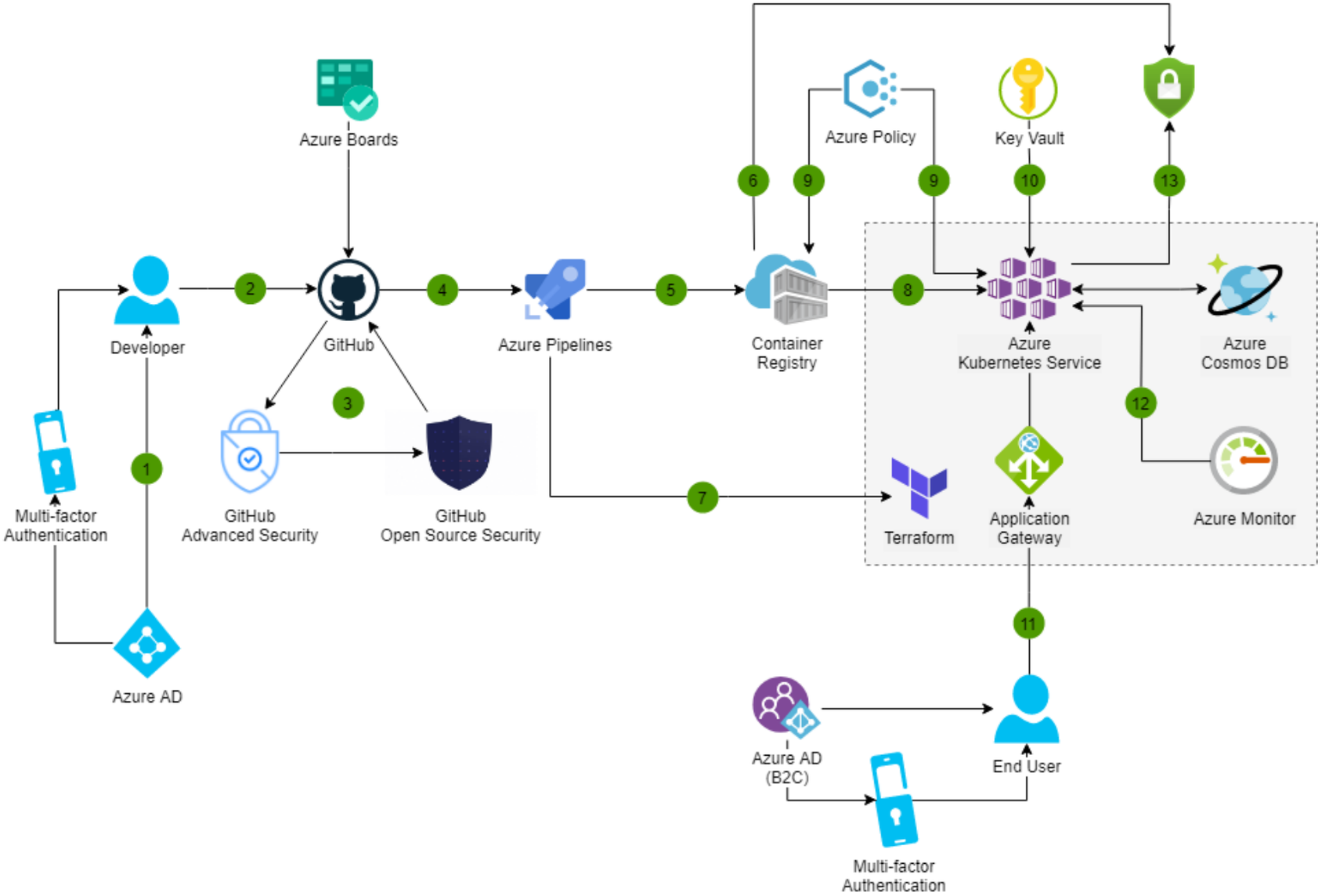
DevSecOps in Azure

7. Azure Active Directory (AD) can be configured as the identity provider for GitHub

8. GitHub Commit tracked by Azure Board

9. Azure Pipelines integrates with the Terraform tool which can managing cloud infrastructure as code

10. Azure Pipelines enable Continuous Delivery (CD) to Azure Kubernetes Service

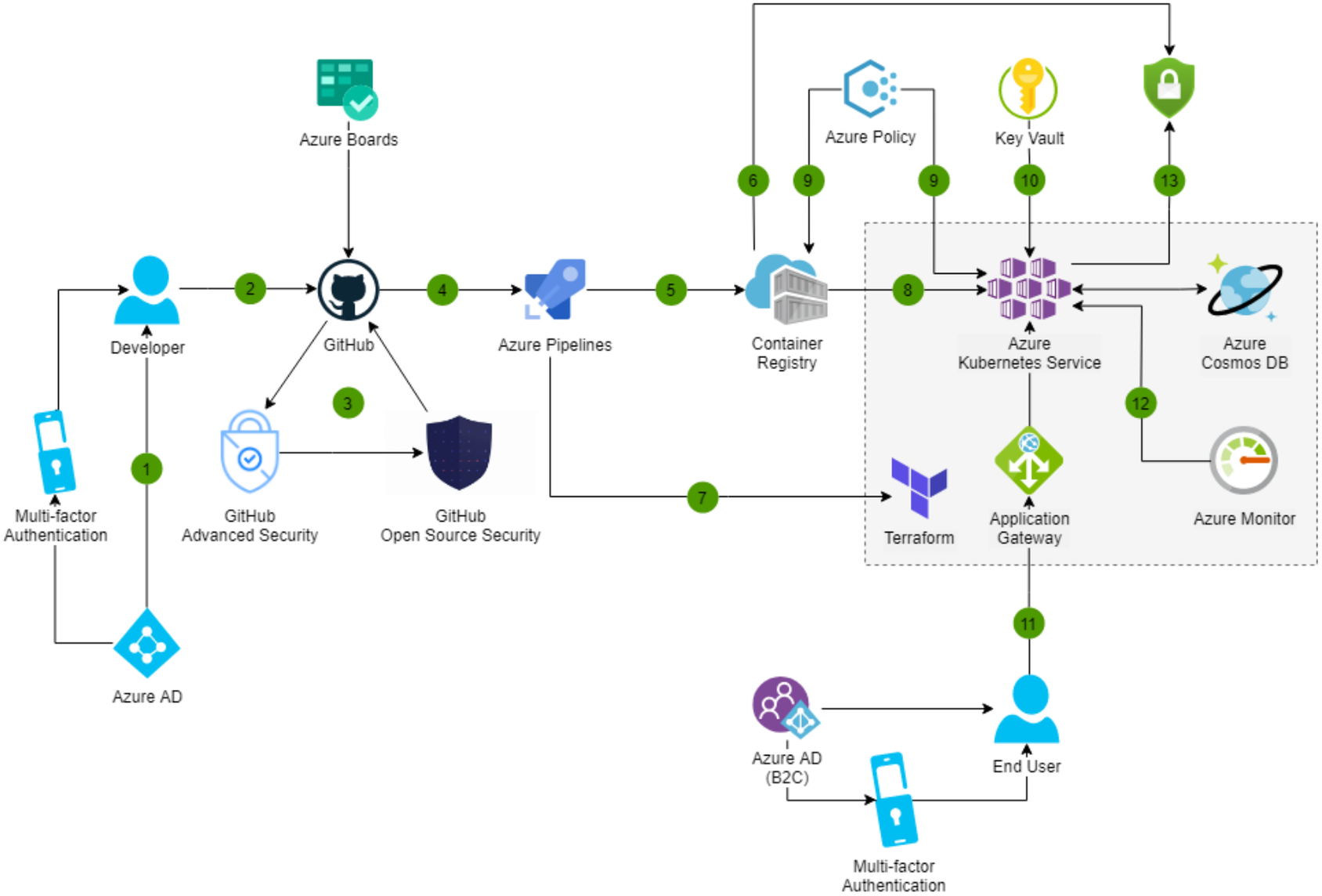


DevSecOps in Azure

11. End user access can be secured with Azure AD B2C

12. Pipeline releases or rollback can be done based on monitoring data from Azure Monitor

13. Azure Pipelines enable Continuous Delivery (CD) to Azure Kubernetes Service

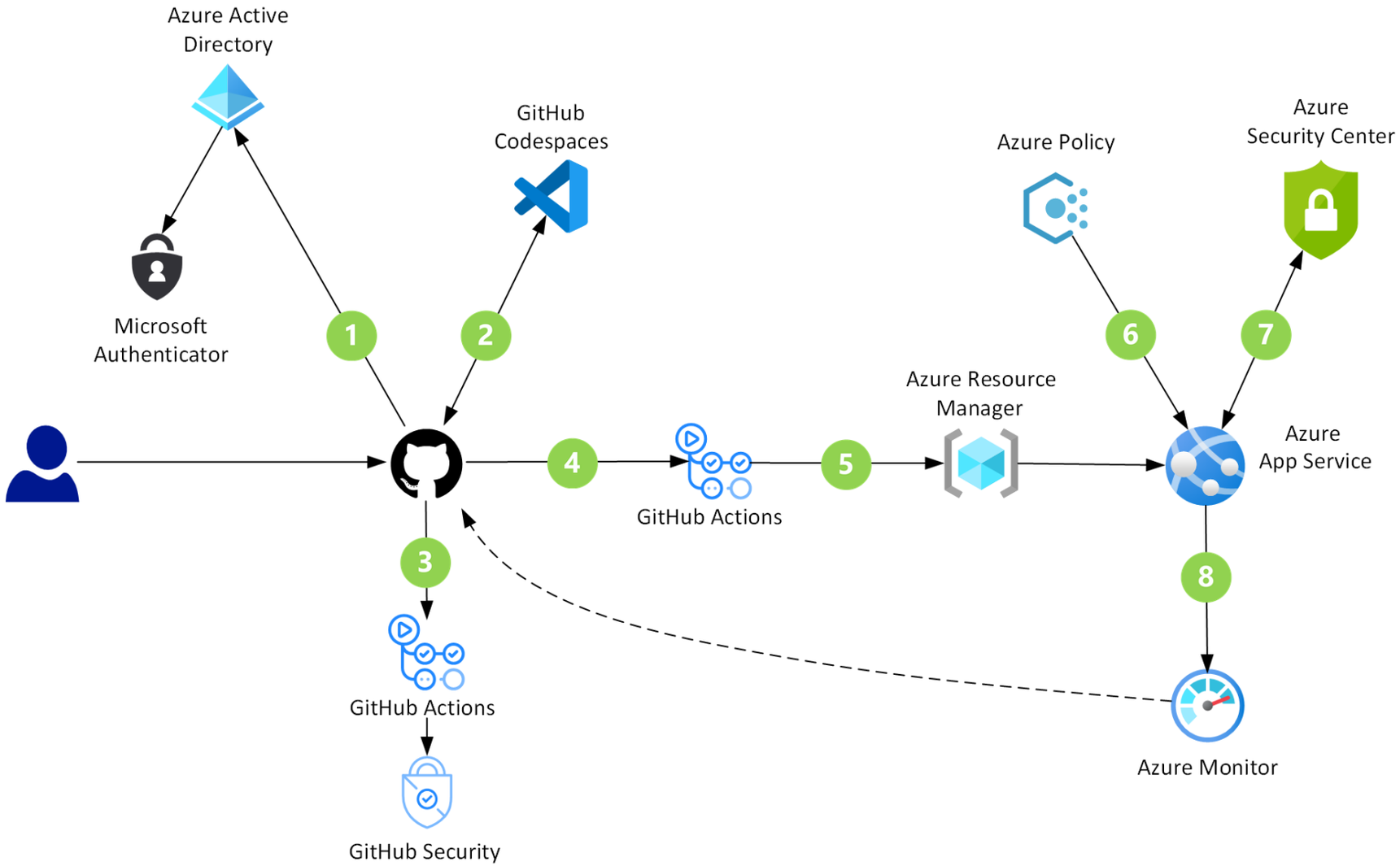


DevSecOps in GitHub

1. Azure Active Directory (AD) can be configured as the identity provider for GitHub

2. Development can be done through GitHub Codespaces (currently in limited public beta)

3. GitHub Actions automatically scan the code to find vulnerabilities when there are code commits

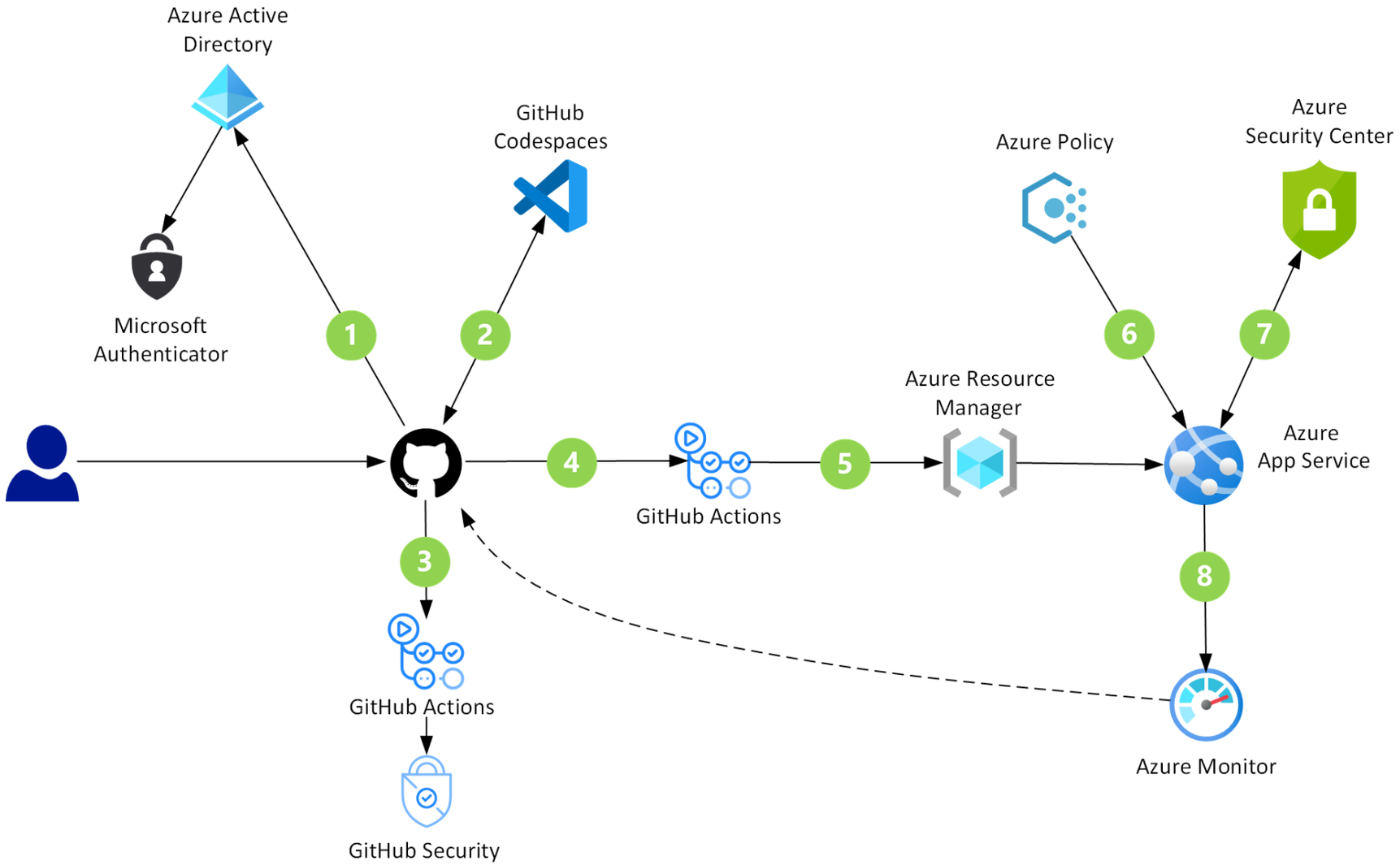


DevSecOps in GitHub

4. Pull requests (PRs) trigger code builds and automated testing through GitHub Actions

5. GitHub Actions deploy build artifacts to Azure App Service

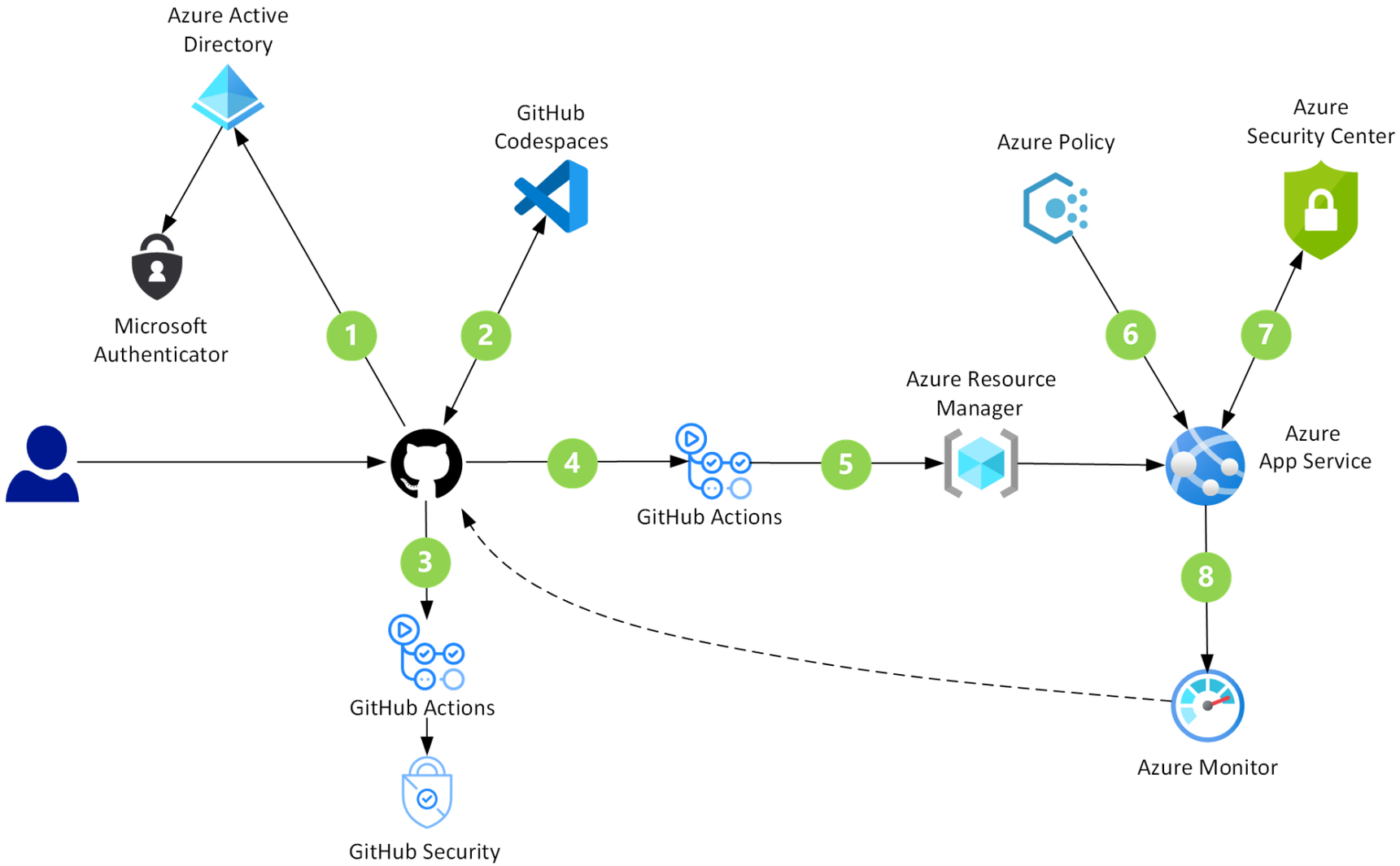
6. Azure Policy evaluates Azure resources that are in deployment



DevSecOps in GitHub

7. Azure Security Center identifies attacks targeting applications

8. Azure Monitor continuously tracks and evaluates app behavior, may trigger rollback when necessary



Demo

Key Takeaway

- Include security setting and configuration in earlier stage of the development workflow design
- Using encrypted at rest service to hold credentials, e.g. GitHub Secret, Azure Key Vault
- Continuous monitoring on the application

Additional Resources

Microsoft Learn
https://Microsoft.com/learn

Azure Architecture Center
https://docs.microsoft.com/en-us/azure/architecture/

DevOps Resource Center
https://aka.ms/devops

Azure DevOps Hands-On Labs
https://azuredevopslabs.com

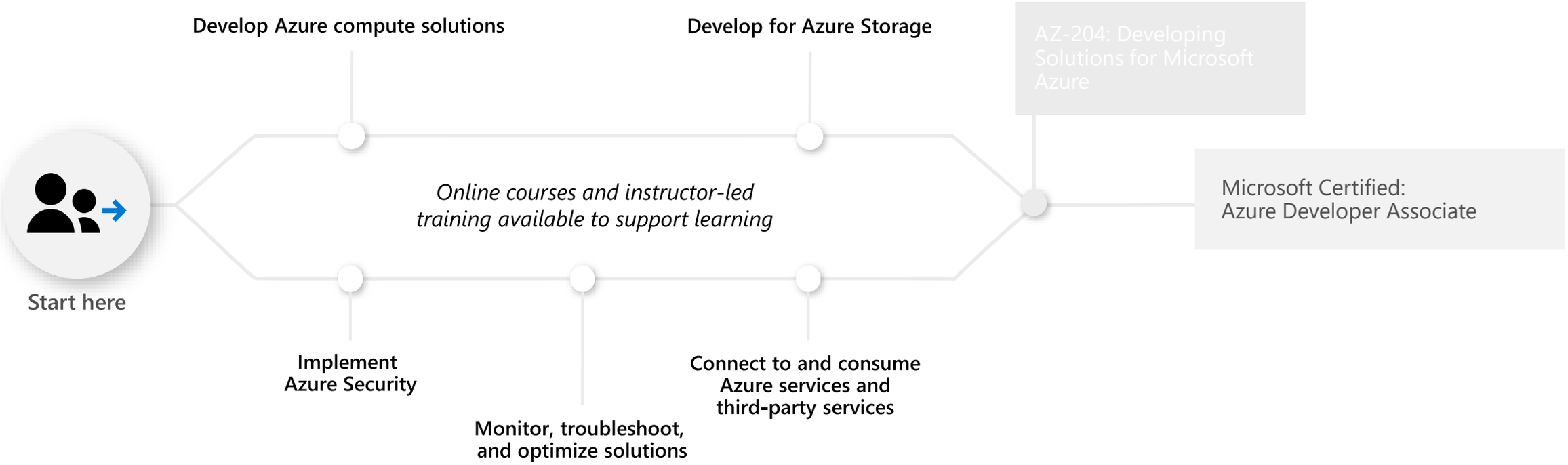
What the Hack: Azure DevOps
https://github.com/microsoft/WhatTheHack/tree/master/010-AzureDevOps

Microsoft Professional Program for DevOps
https://academy.microsoft.com/en-us/tracks/devops/

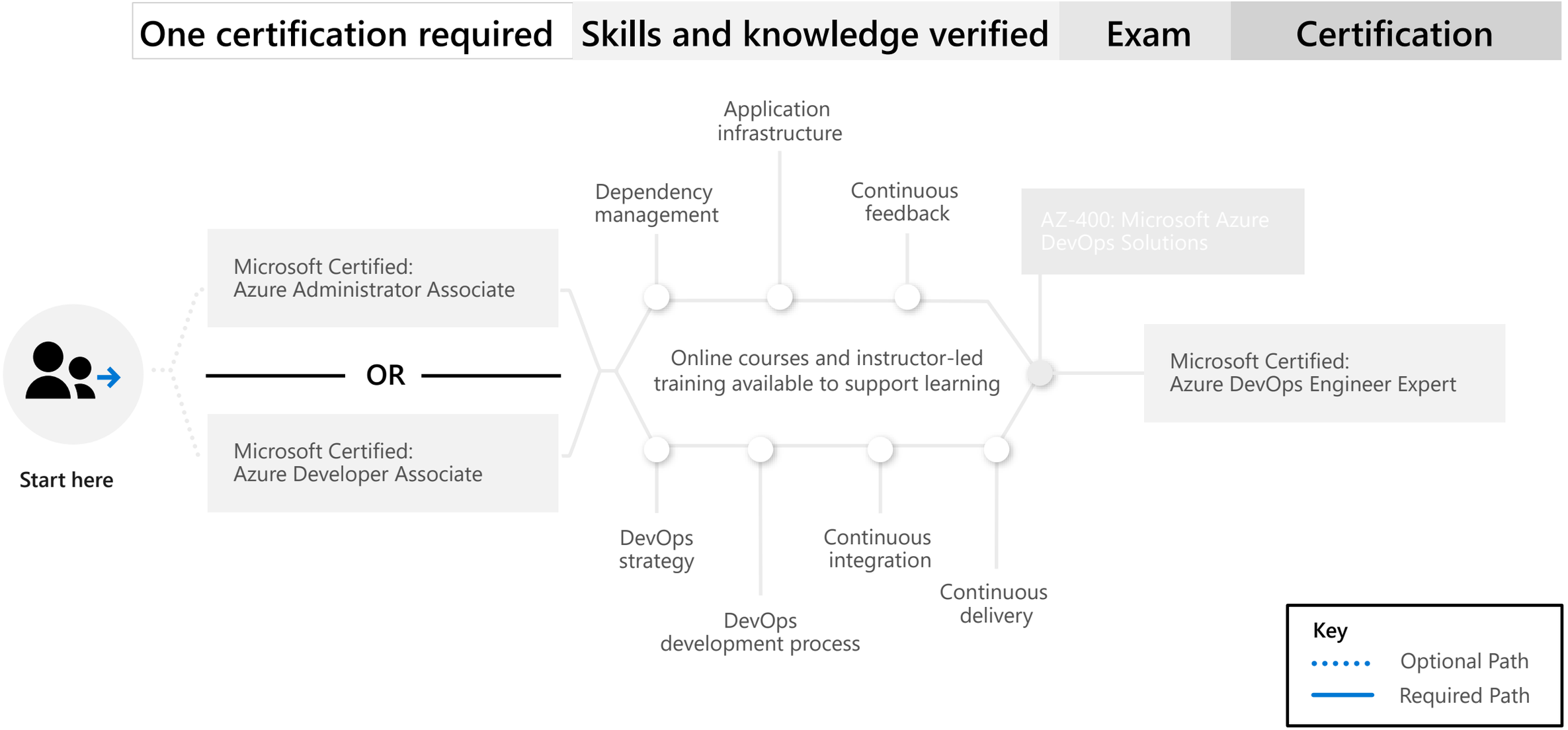
Azure DevOps YouTube Channel
https://www.youtube.com/channel/UC-ikyViYMM69joIAv7dlMsA

Learning path for Azure Developer Associate

Skills required for certification	Exam	Certification



Learning path for Azure DevOps Engineer Expert



Free Digital event

Open Azure Day Hong Kong

Feb. 23, 2021| 9:15AM-1:00PM

Language: Cantonese

Run Linux apps your way on Azure

Learn about the latest Linux and open-source trends and capabilities on Azure. Watch demos and get best practices to turbocharge your apps and data, whether you're new to Azure or new to Linux and OSS workloads.

Topics Highlights:

- Secure Software Development with GitHub & Azure
- Architecting Secure, Enterprise Ready solutions for the Cloud with Azure & MySQL
- Cloud Native Platform for your Microservice apps with Azure Spring Cloud
- Running SAP with SUSE on Azure
- Be Future Ready with Azure: The Open Cloud

Register now

https://aka.ms/openazuredayhk

Brendan Burns
Corporate Vice President, Azure
Microsoft

Scott Guthrie
Executive Vice President, Cloud+AI
Microsoft

Brandon Pulsipher
Vice President, Cloud Engineering
Adobe

Michael Chau
Customer Engineer
Microsoft HK

Derek So
Principle Technologist
SUSE, Asia Pacific

Douglas Lam
Cloud Solution Architect – Infrastructure
Microsoft HK

George Liu
Sr Cloud Solution Architect
Microsoft HK

Aaron Chong
Cloud Solution Architect
Microsoft HK

Yuki Hon
Cloud Solution Architect
Microsoft HK

Felix Chan
Regional Solution Specialist
SoftwareONE HK Ltd

Microsoft Azure

Thank you