Speaker

meetup.com/Azure-Cloud-Security-Meetup-Group/

teiss London2020
European Information Security Summit
teiss London2020
The European Information Security Summit

David Okeyode (MVP)

Cloud Security Consultant

Speaker Bio: Microsoft Azure MVP. Over a decade of experience in Cybersecurity (consultancy, design, implementation). Over 6 years of experience as a trainer. Developed multiple vulnerable by design automation templates that can be used to practice cloud penetration testing techniques. Authored two cloud computing courses for the popular cybersecurity training platform – Cybrary.

@asegunlolu

http://www.youtube.com/c/DavidOkeyode

http://azurehangout.com

MVP Microsoft® Most Valuable Professional

Microsoft CERTIFIED AZURE AI ENGINEER ASSOCIATE

Microsoft CERTIFIED AZURE DEVELOPER ASSOCIATE

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Microsoft CERTIFIED AZURE DEVOPS ENGINEER EXPERT

aws certified Solutions Architect Professional

aws certified Security Specialty

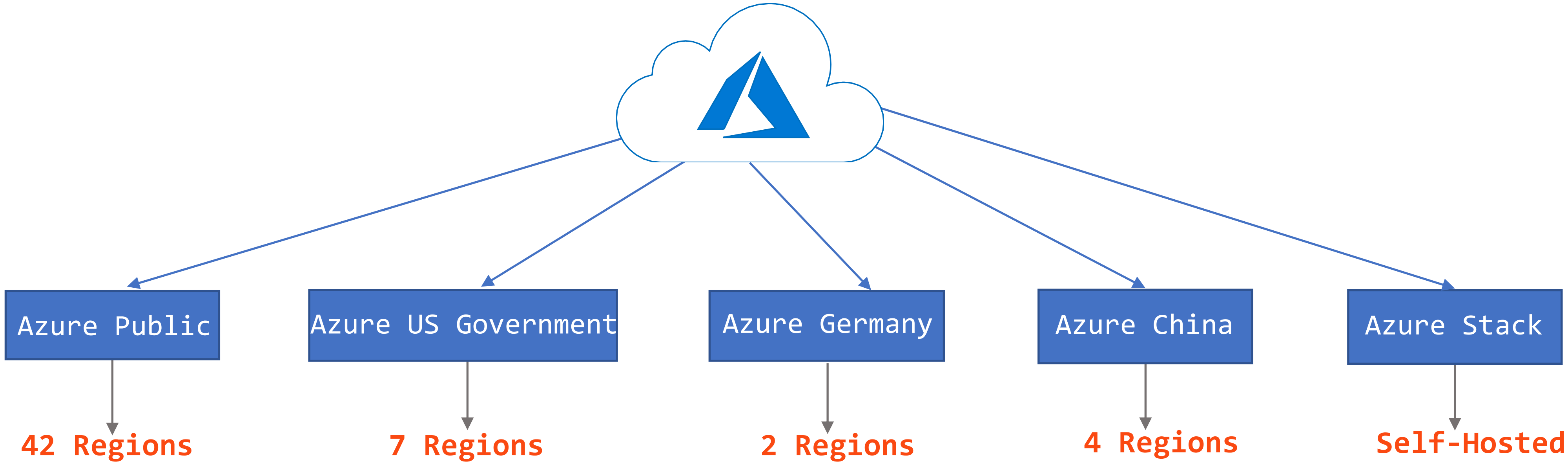
Agenda

- Azure Cloud Platform
- What is a vulnerability?
- Cloud Native Security Model
- Mapping Vulnerabilities
- Demo – Exploiting ACI
- Demo – Defending

Why a different approach?

- A lot of presentations, talks and videos already focus on best practices and the use of tools
- Understanding attacker behaviour is an important part of cybersecurity education
- Learn what not to do from the failures of others

The Azure Cloud Platform



Cloud

Regions

Azure Public

42 Regions

Azure US Government

7 Regions

Azure Germany

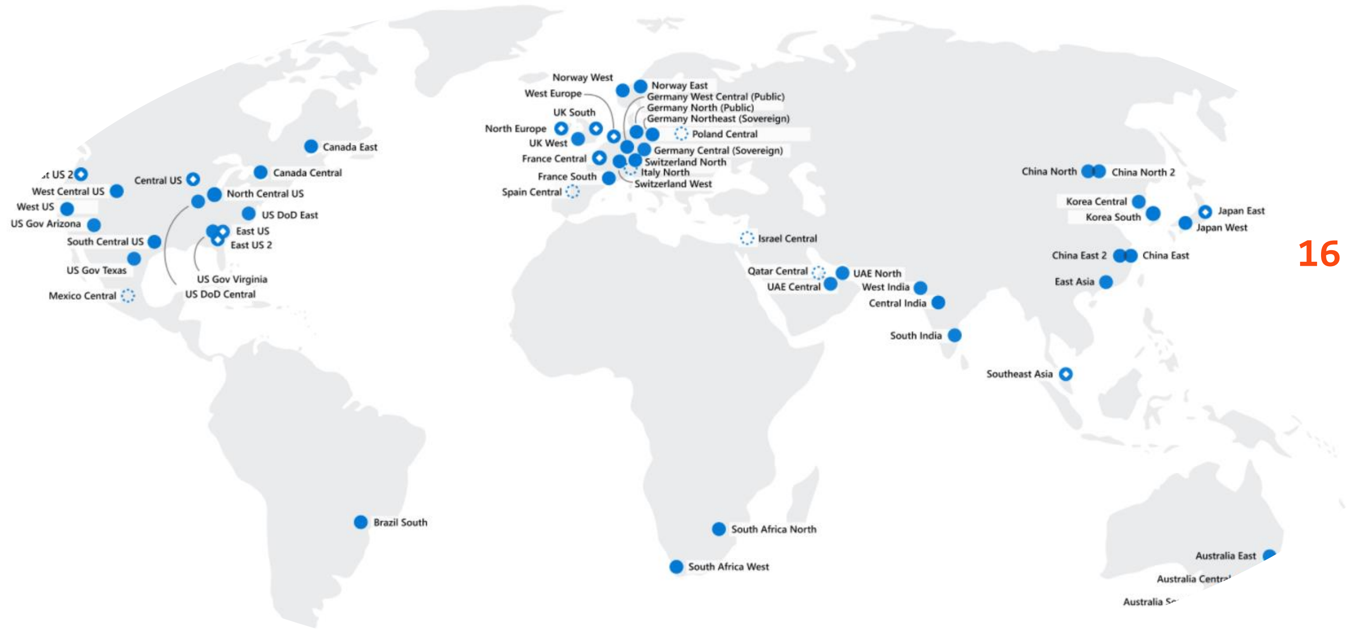
2 Regions

Azure China

4 Regions

Azure Stack

Self-Hosted

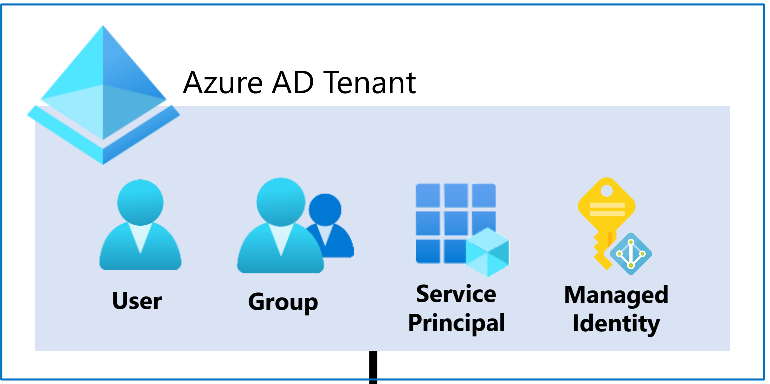


11 “announced” regions
16 regions with availability zones

Azure Organization Structure

Azure AD roles are used to grant access to Azure AD. Example roles are,

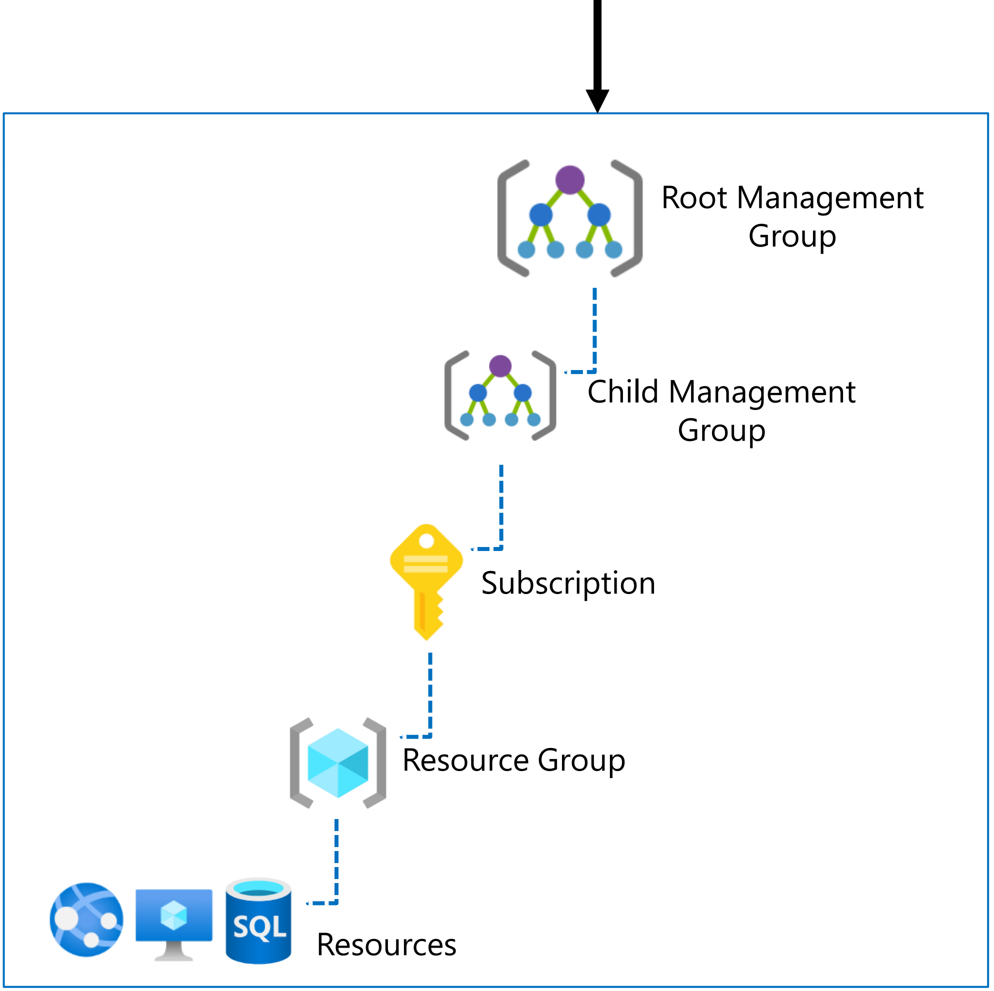
Global Administrator and User Administrator



Azure RBAC roles are used to grant access to Azure resources. Example roles are,

Owner, Contributor and Reader

```
"permissions": [
   {
     "actions": [ ],
     "notActions": [ ],
     "dataActions": [ ],
     "notDataActions": [ ]
   }
 ],
```



Azure Cloud Services

- Services that we can use to host our applications
- Services that we can use to store data for our applications
- Services that we can use to create applications
- Services that we can use to enhance our applications
- Services that we can use to integrate our applications
- Services that we can use to monitor/manage our applications

App Service
Service Bus
Logic Apps
Data Factory v2
Key Vault
Application Insights

App Service Environment
Event Hub
Azure AD
Virtual Network
Storage Account
Kubernetes Service

Function
VM Scale Set
Virtual Machine
API Management
Cognitive Services

https://bit.ly/azurecloudservices

What is a vulnerability?

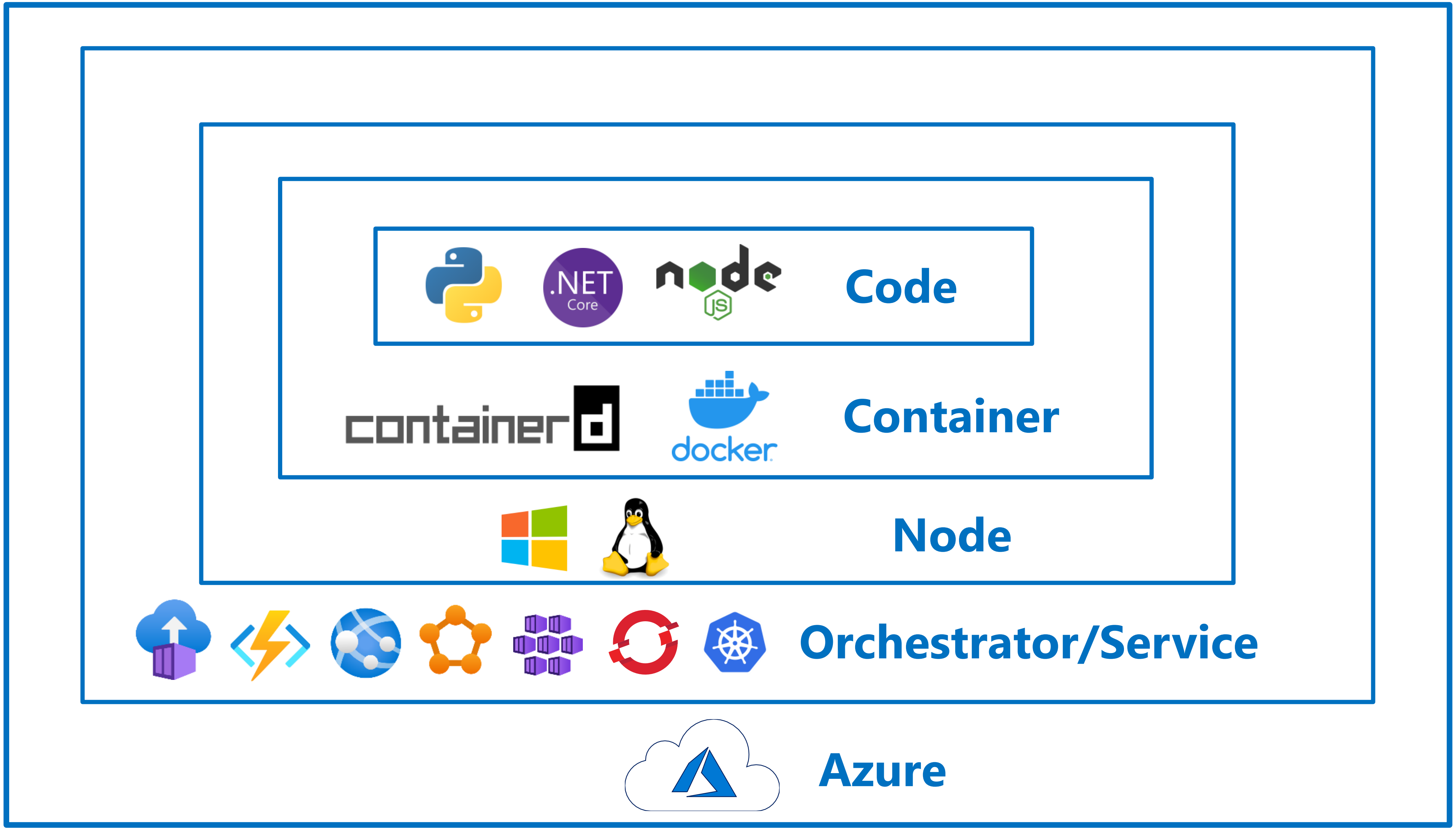
- A weakness in a system that can be exploited by an attacker to deliver a successful attack

- Software Flaws
  - Unintended functionality
  - Zero days or publicly reported

- Feature misuse
  - Intended functionality

- User error OR misconfiguration

Cloud Native Security Model



Code

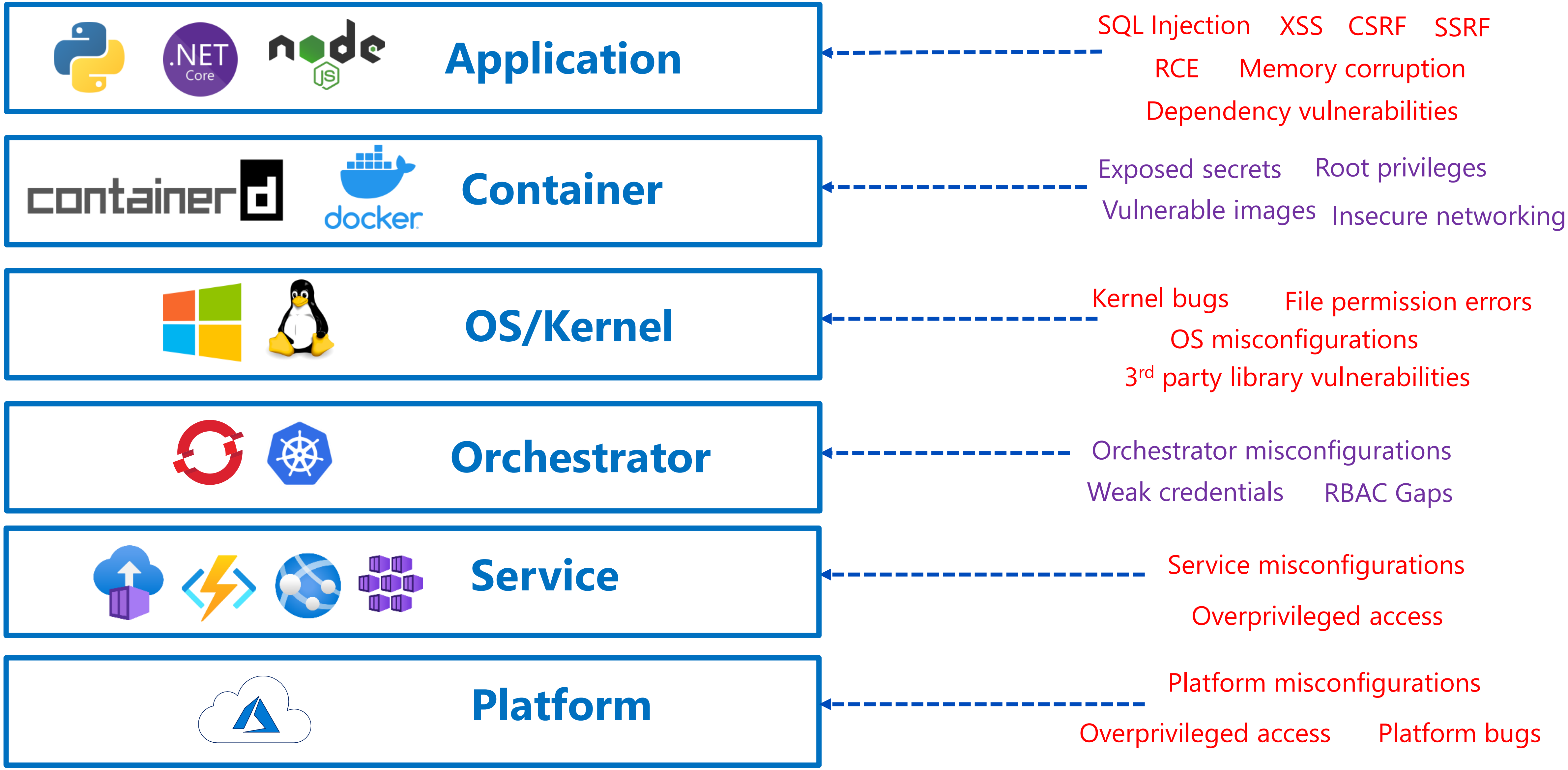
Container

Node

Orchestrator/Service

Azure

Mapping Vulnerabilities



Application

SQL Injection XSS CSRF SSRF

RCE Memory corruption

Dependency vulnerabilities

Container

Exposed secrets Root privileges

Vulnerable images Insecure networking

OS/Kernel

Kernel bugs File permission errors

OS misconfigurations

3rd party library vulnerabilities

Orchestrator

Orchestrator misconfigurations

Weak credentials RBAC Gaps

Service

Service misconfigurations

Overprivileged access

Platform

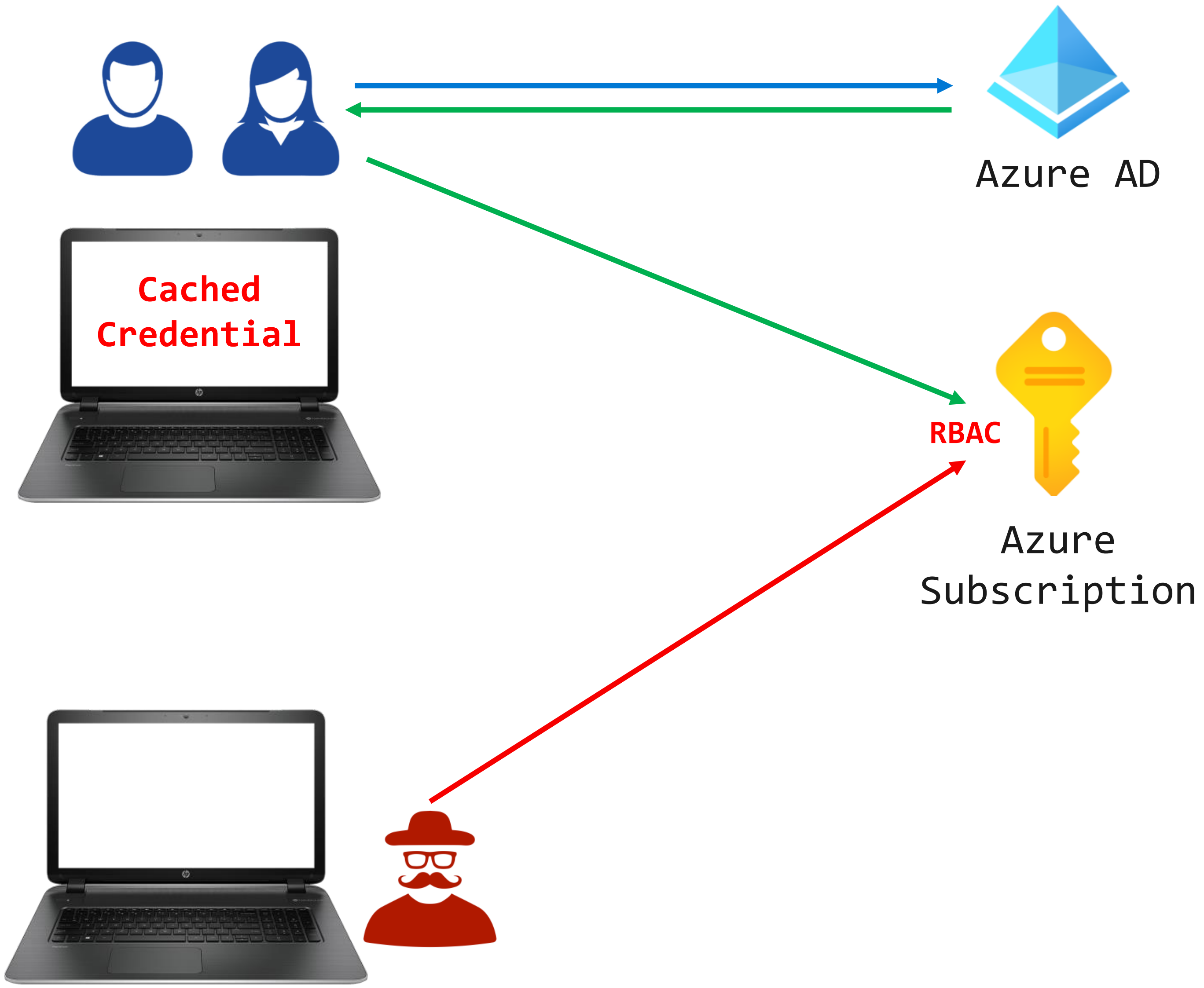
Platform misconfigurations

Overprivileged access Platform bugs

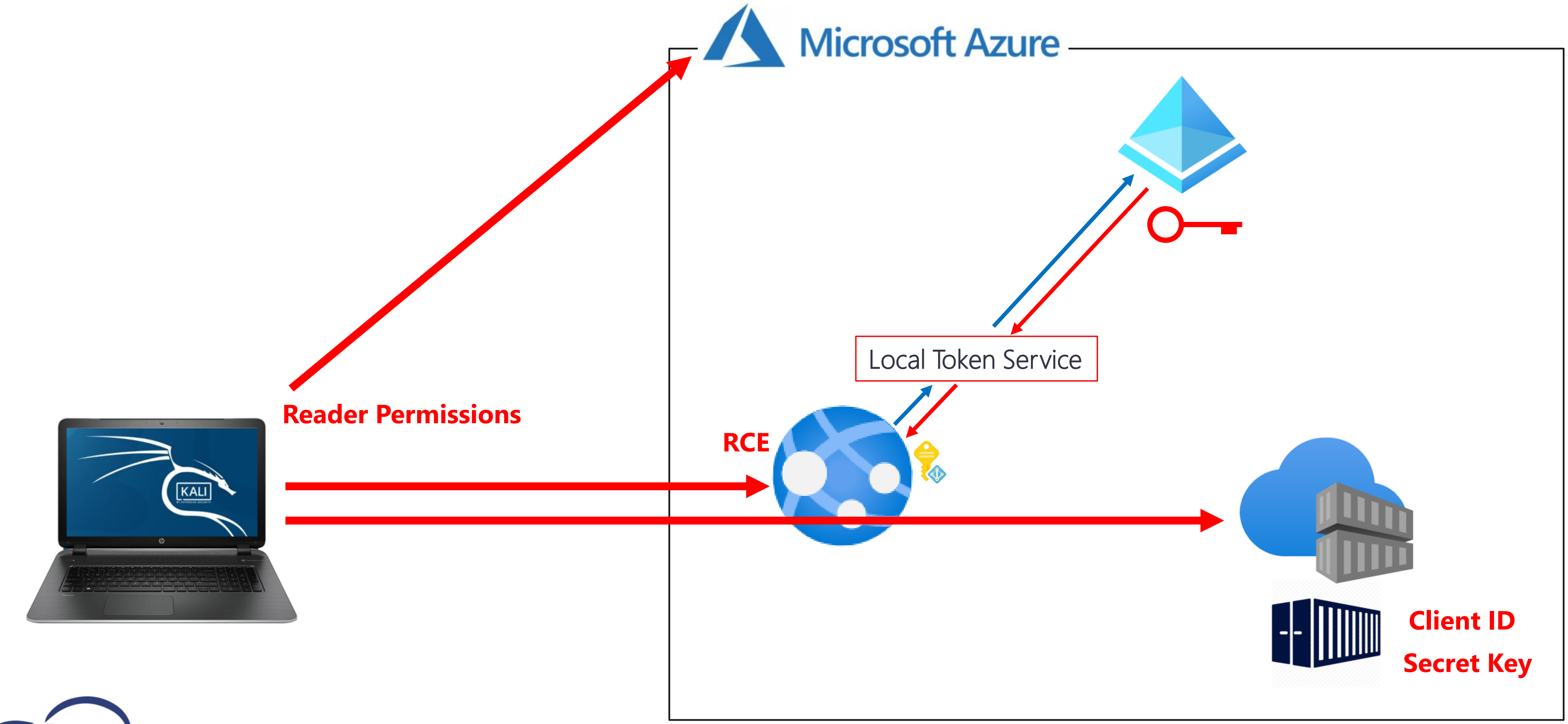
Azure Attack Matrix

Discovery	Credential Access	Initial Access	Execution	Privilege Escalation	Defense Evasion	Lateral Movement	Persistence	Impact
Cloud provider IP Range Network Scan	Credential Guessing	Cloud Credential Compromise	Server Side Request Forgery	Access Privileged Resources	Disable Security Services	Cloud Service Keys	Create Account	Data Destruction
Cloud Service DNS Enumeration	Brute Force	Weak/Default Service Credentials	Remote Code Execution	Automation Account Injection	Modify Trusted IPs/Allowlists	Managed Identity Compromise	Account Manipulation	Resource Hijacking
Cloud Service Discovery	Access Token Theft	Application Vulnerability	Automation Account Runbook	Privileged Group Membership	Unused Cloud Regions	Privileged On-Prem Identity	Modify Trusted IPs/Allowlists	Denial Of Service
Cloud Service Dashboard	Managed Identity Compromise	Trusted Relationship	Access Cloud Resources	Service Principal Secret Add	Create New Resources	Access Kubernetes API	Container Image Implant	Data Exfiltration
Cloud Access Discovery	Applications Credentials in Configuration Files				Delete Alerts	Network Mapping	Automation Account Runbook	Supply Chain Injection
Software or System Information Discovery					Connect From Proxy Server		Deploy VM/Function Backdoor	

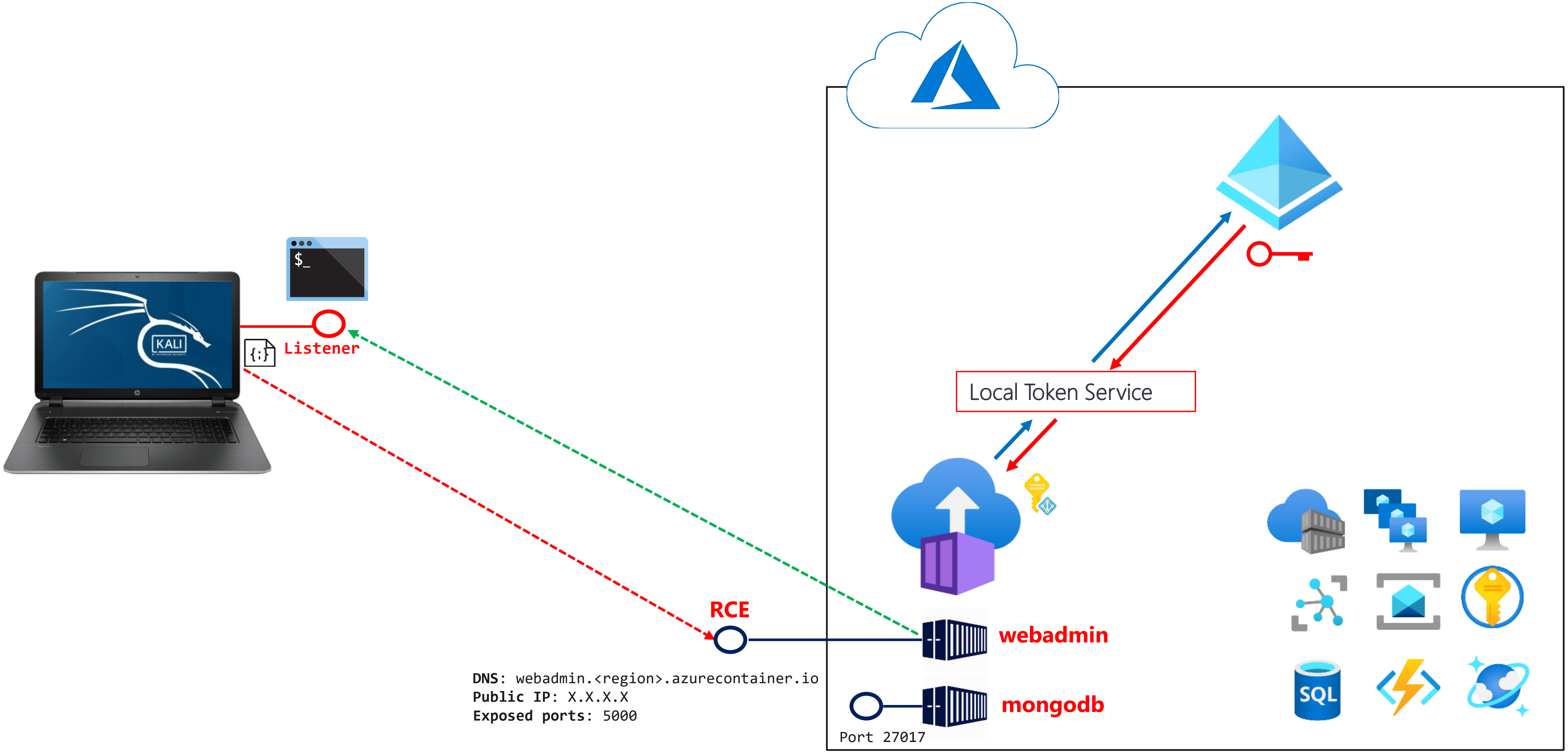
Credential Theft from Admin Workstation



ACR Privilege Escalation Scenario



DEMO - Exploiting Container Instance Workload



$_

Listener

RCE

Local Token Service

webadmin

mongodb

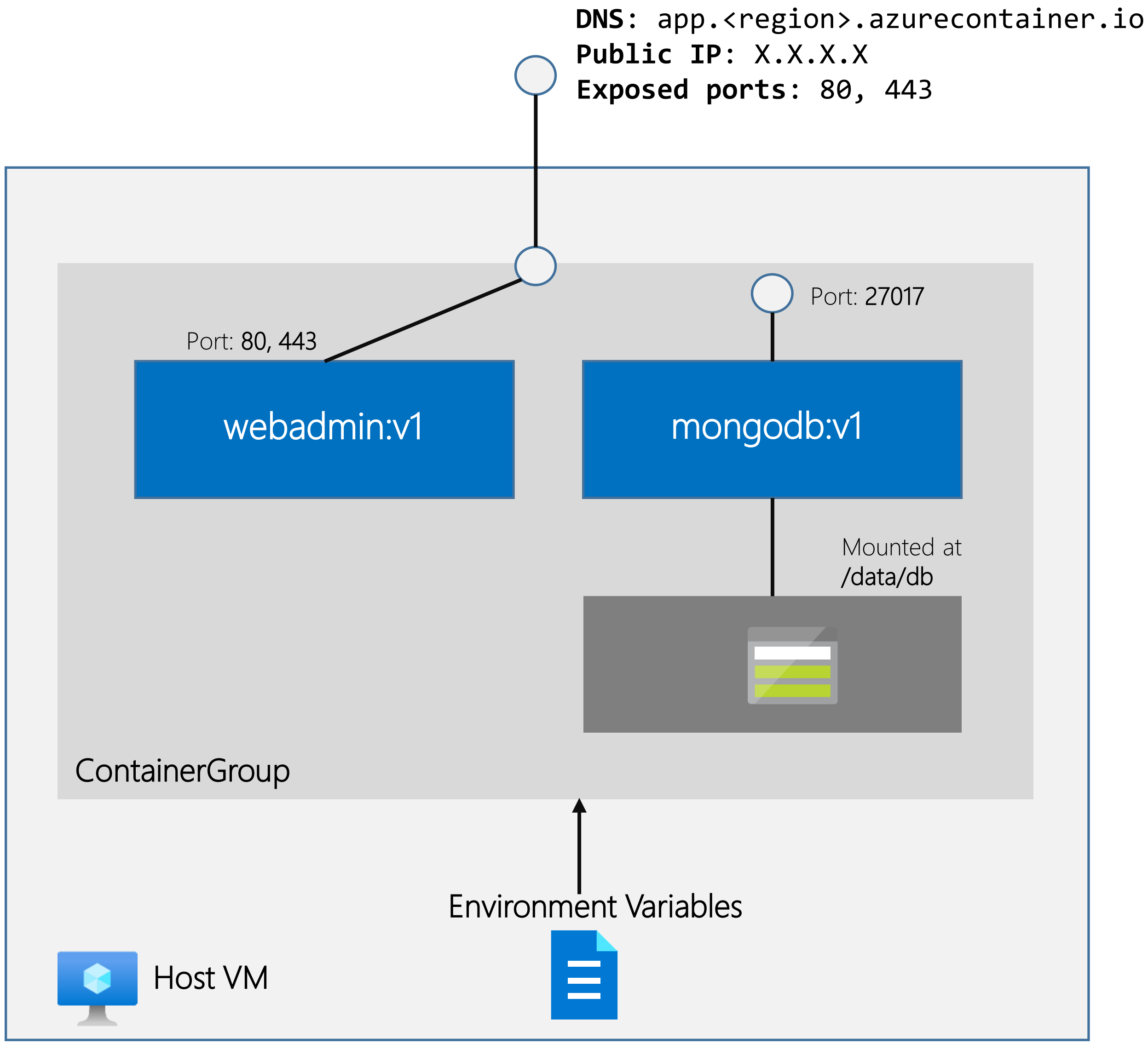
DNS: webadmin.<region>.azurecontainer.io
Public IP: X.X.X.X
Exposed ports: 5000

Port 27017

SQL

Azure Container Instances (ACI) Deep Dive

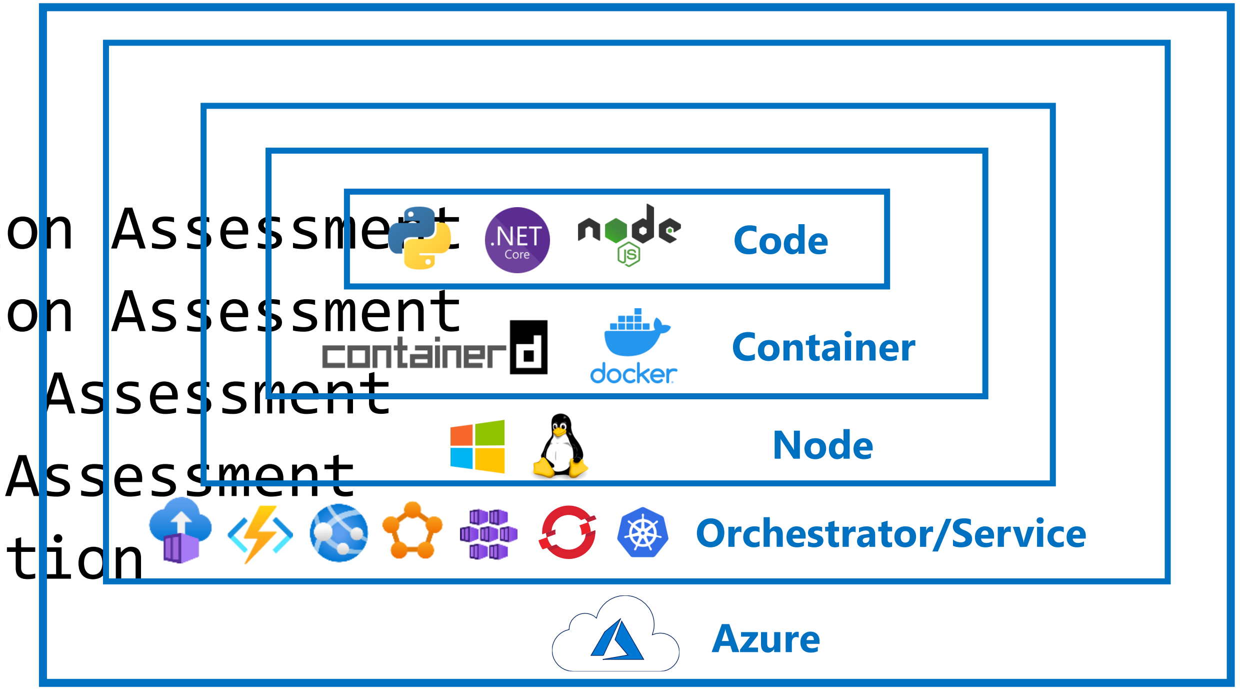
- Azure Container Instances offers the fastest and simplest way to run a container in Azure
  - Doesn’t require IaaS VM provisioning and ongoing maintenance
  - Faster startup time compared with VMs
- Ideal for isolated containerized workloads that does not require orchestration
  - Simple applications; Task automation; Build jobs
- Underlying Host (Managed by Microsoft)
  - Windows or Linux
  - No direct access to the underlying Docker API/OS/infrastructure
- Container group
  - Containers that are scheduled to run on the same host
  - Share a lifecycle, resources, local network, and storage volumes
  - Supports environment variables
  - Supports volume mounting
- Environment variables enable you to dynamically configure the application or script the container runs



Key Takeaway

- Your Azure environment is as vulnerable as your weakest security model

- Five Key Areas
  - Cloud Platform Configuration Assessment
  - Cloud Resource Configuration Assessment
  - Cloud Identity Entitlement Assessment
  - Application Vulnerability Assessment
  - Application Runtime Protection



Thanks! Questions?

meetup.com/Azure-Cloud-Security-Meetup-Group/

teiss London2020
European Information Security Summit
teiss London2020
The European Information Security Summit

David Okeyode (MVP)

Cloud Security Consultant

@asegunlolu

http://www.youtube.com/c/DavidOkeyode

http://azurehangout.com

Microsoft CERTIFIED AZURE AI ENGINEER ASSOCIATE

Microsoft CERTIFIED AZURE DEVELOPER ASSOCIATE

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Microsoft CERTIFIED AZURE DEVOPS ENGINEER EXPERT

aws certified Solutions Architect Professional

aws certified Security Specialty