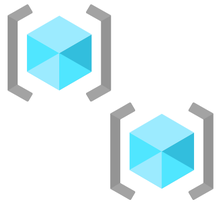
#GLOBALAZURE
BY COMMUNITY • FOR COMMUNITY
2024

#GlobalAzure
#GlobalAzureMilano

Migliora la tua architettura Azure: una guida pratica alla sicurezza, disponibilità e gestibilità

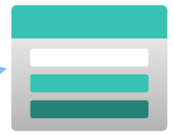
Lorenzo Barbieri – SOFTWAREONE
Marco Obinu - MICROSOFT

EVERYTHING starts with a “good” architecture



RG for
- Dev-Test
- Production

Web UI

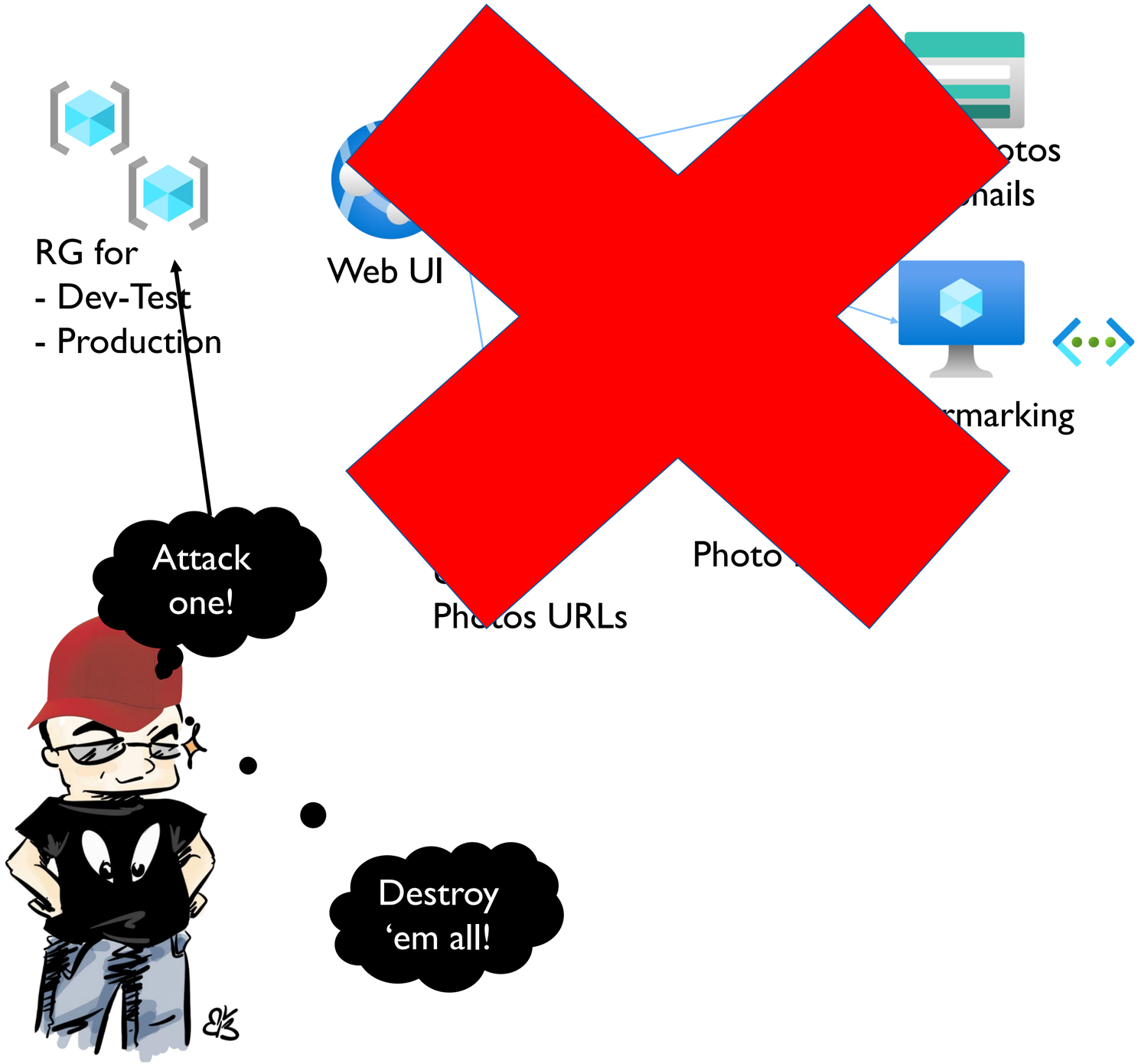


RAW Photos
Thumbnails

Watermarking

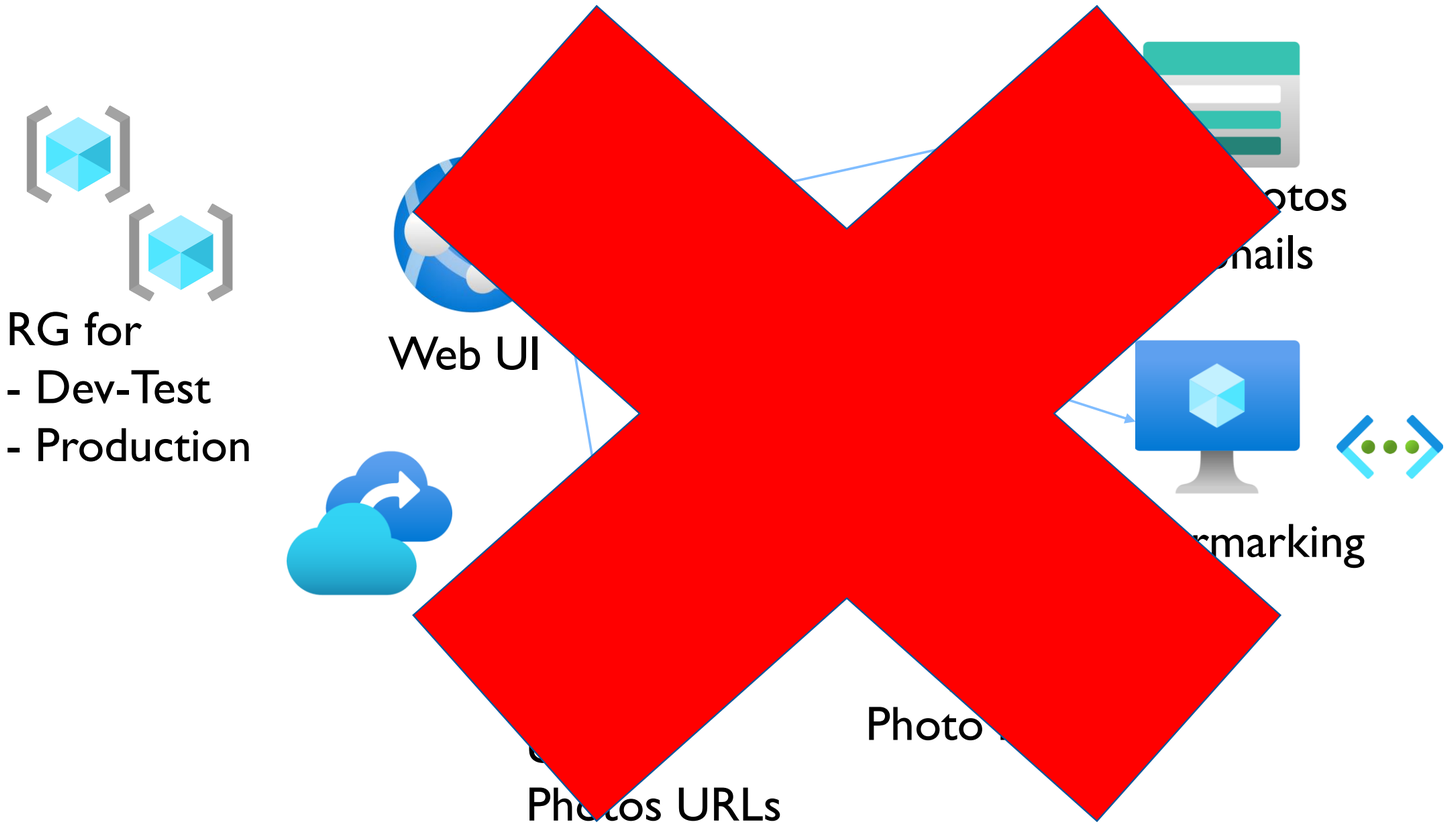
Users
Photos URLs

Photo resize



1st Strike

The case of disappearing resources



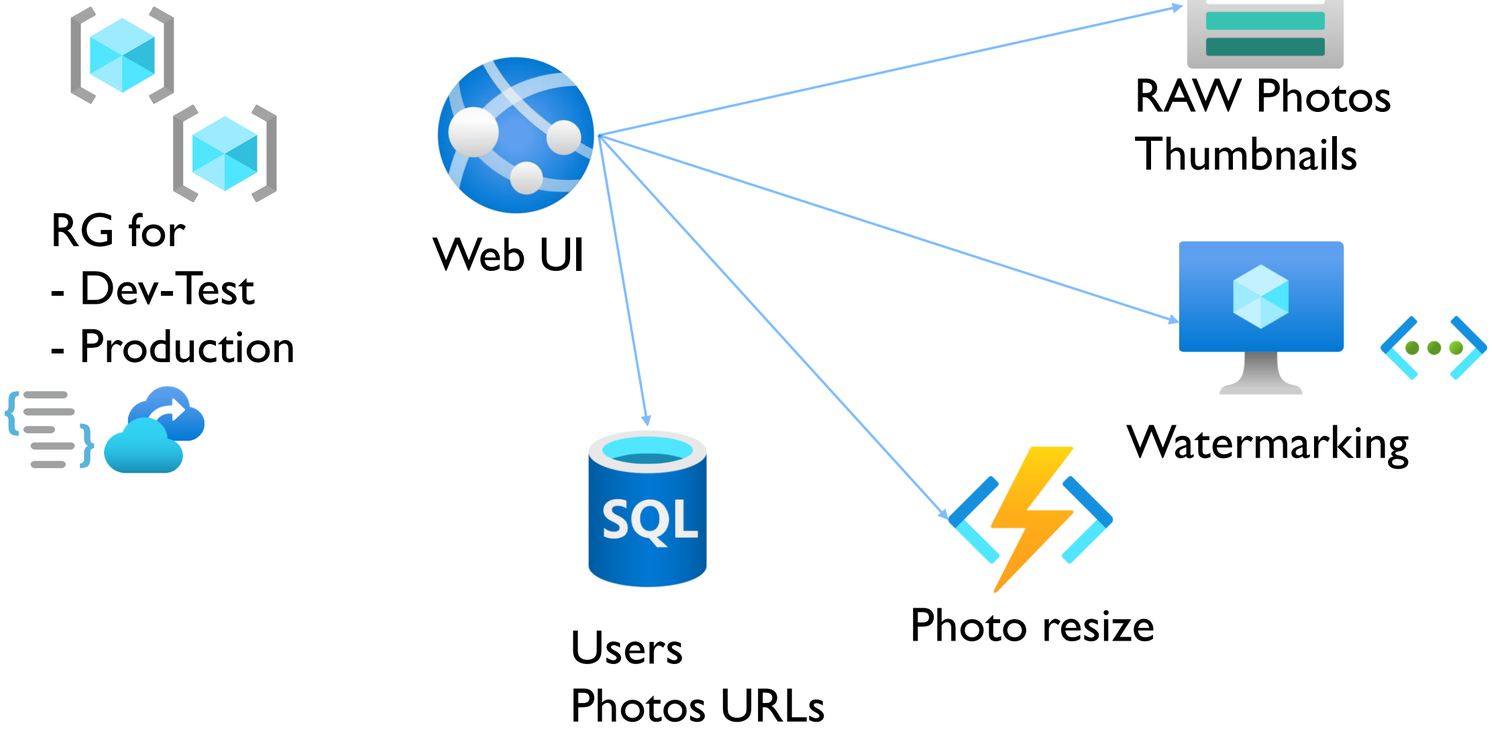
Mitigation

Infrastructure as Code:

- **Script & Backup everything**
- **ARM, Terraform, Bicep…**

Safeguards:

- **Azure Web App Undelete**
- **SQL Point in time restore**
- **Blob Storage restore**
- **Azure Backup**



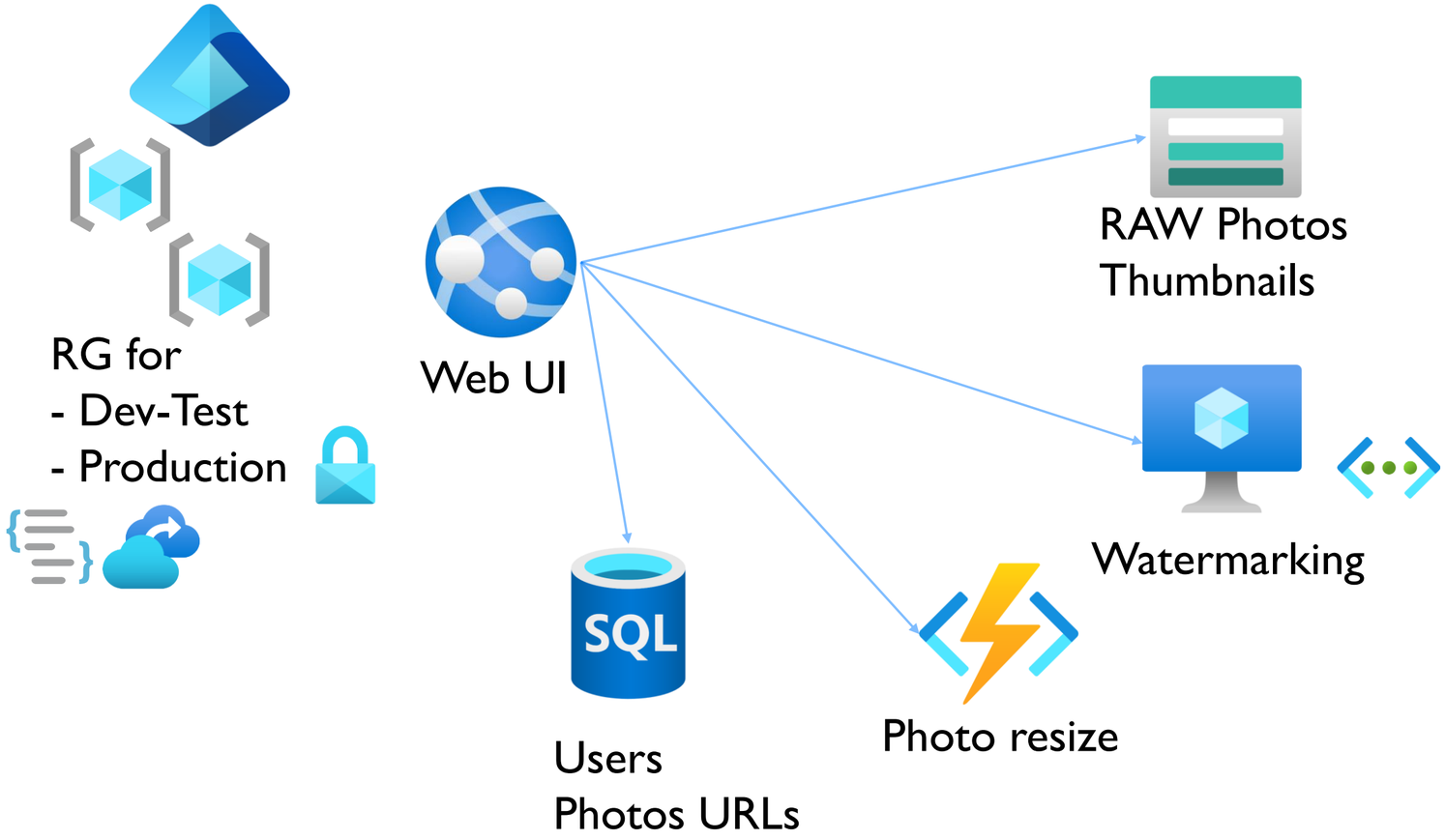
Remediation

Least Privilege

- **RBAC**
- **PIM**

Entra ID protected with MFA

Azure DevOps or GitHub



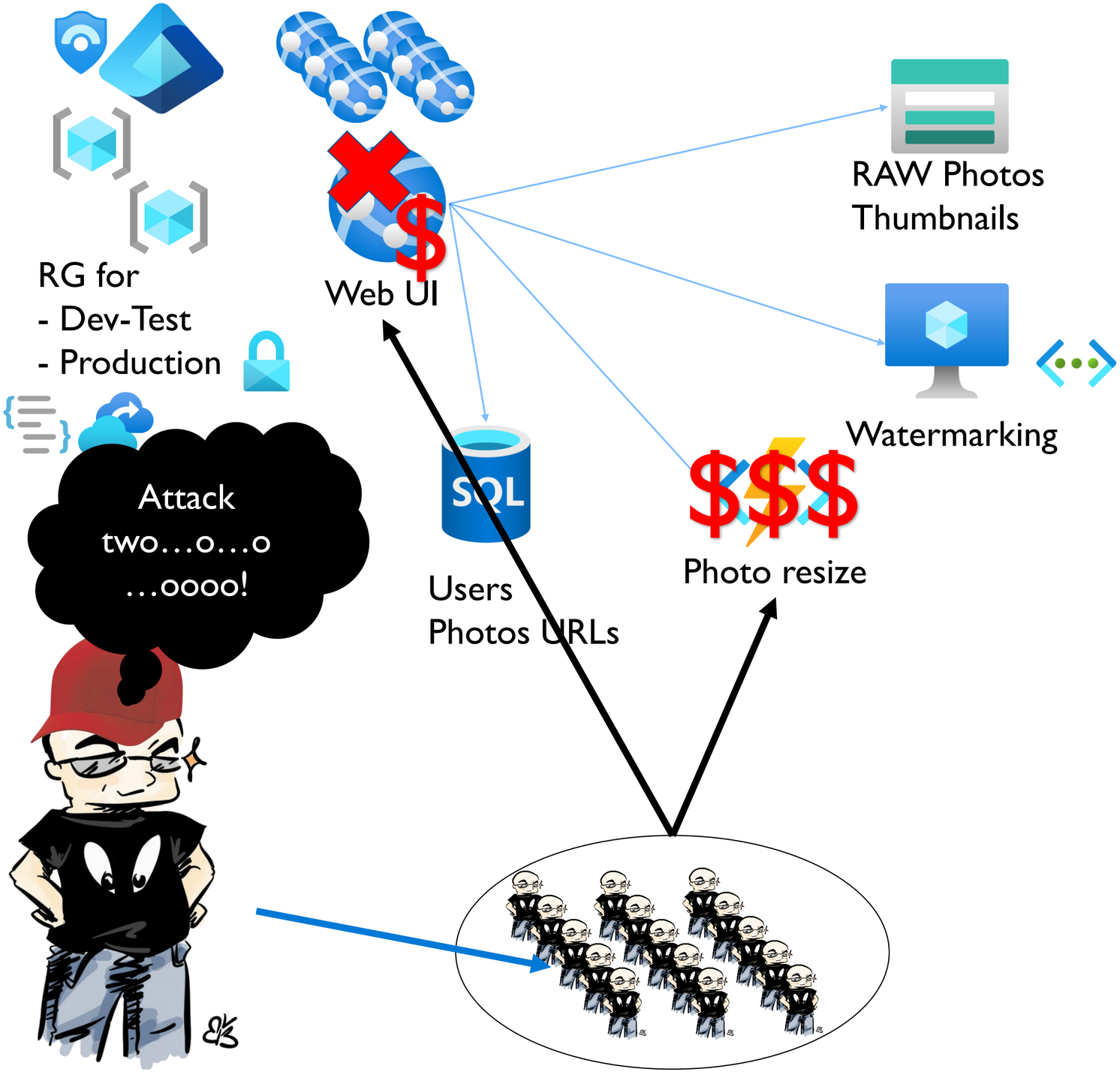
Remediation

Landing Zone

- **Deployment Stack**
- **Deny Assignments**
- **Delete Locks**
- **Azure Policy**

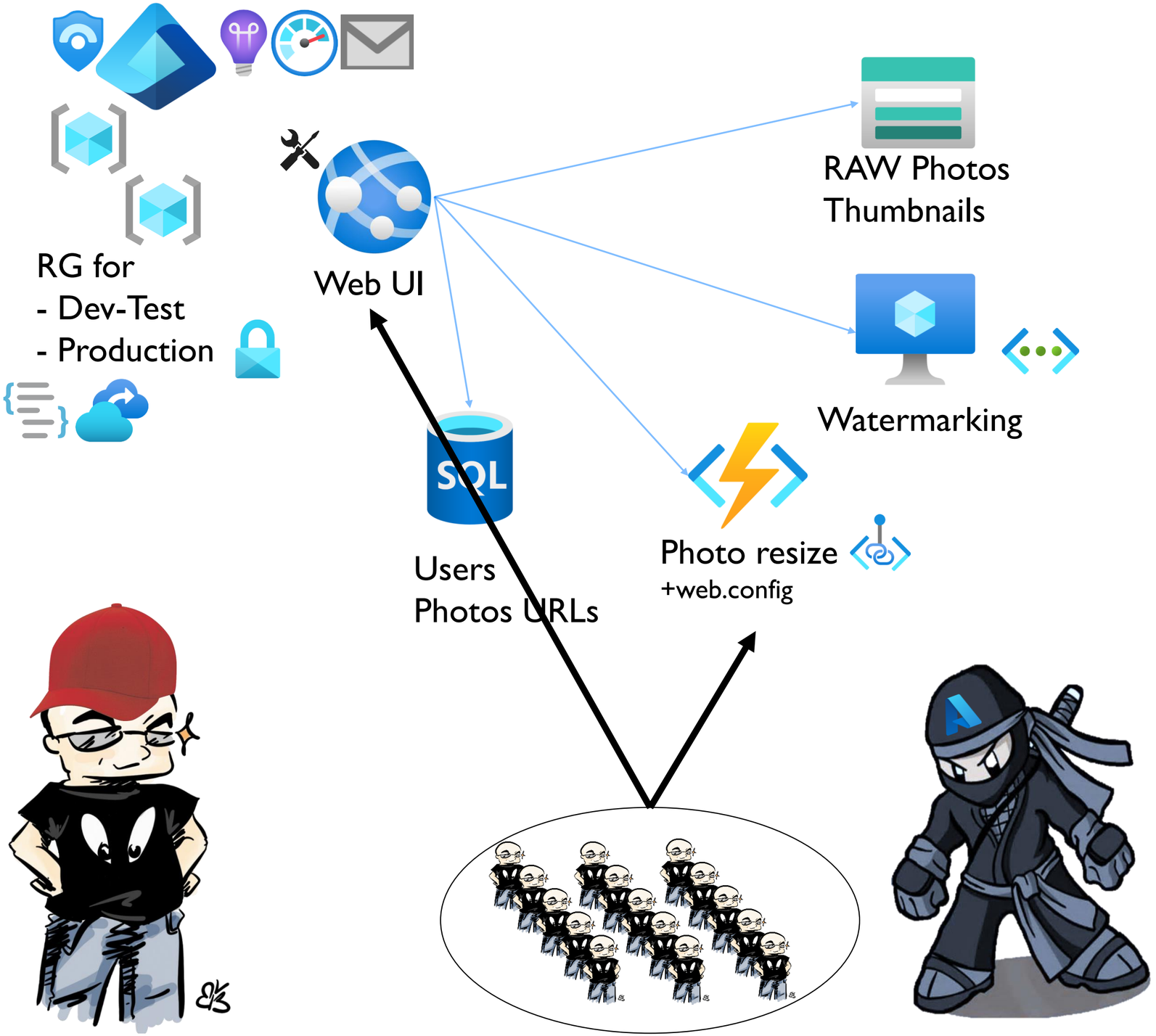
Defender for Cloud

Defender XDR



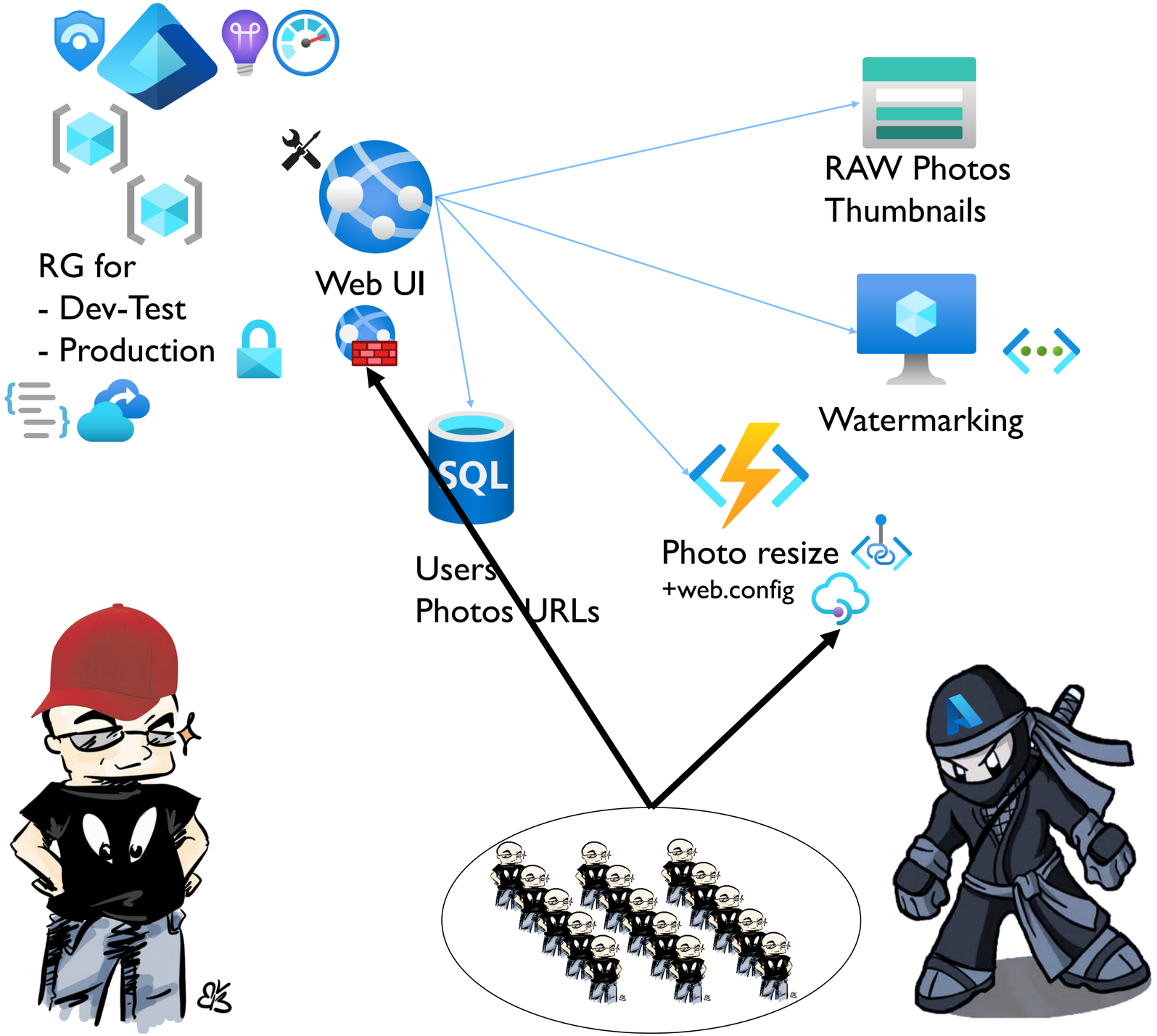
2nd strike

The case of unexpected load



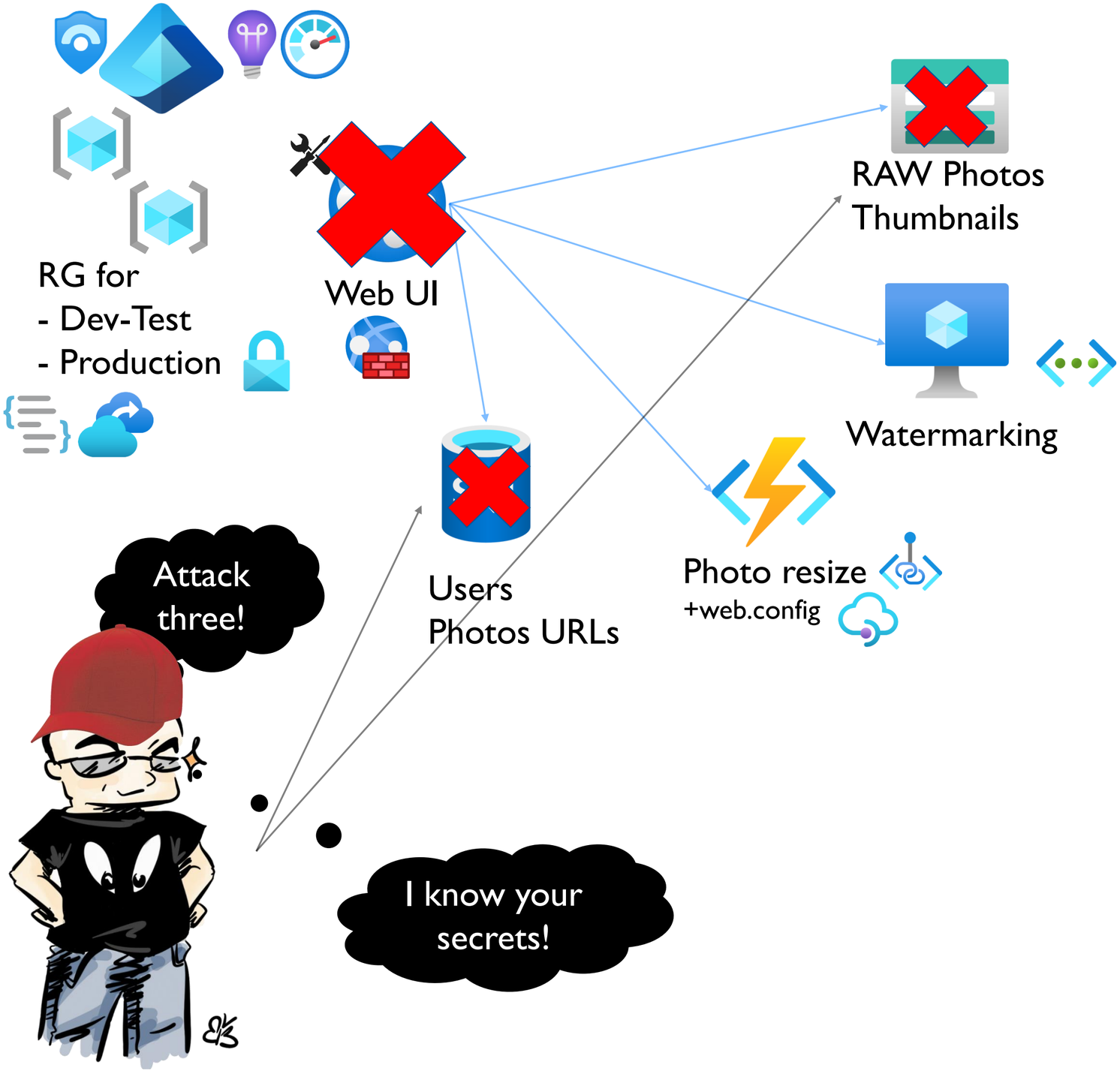
Mitigation

- **Alert rules and monitoring**
- **IP restrictions (i.e., web.config) OR Private Endpoint**
- **Functions in App Service Plan**
- **GB*s daily quota**
- **App Service Diagnostics**



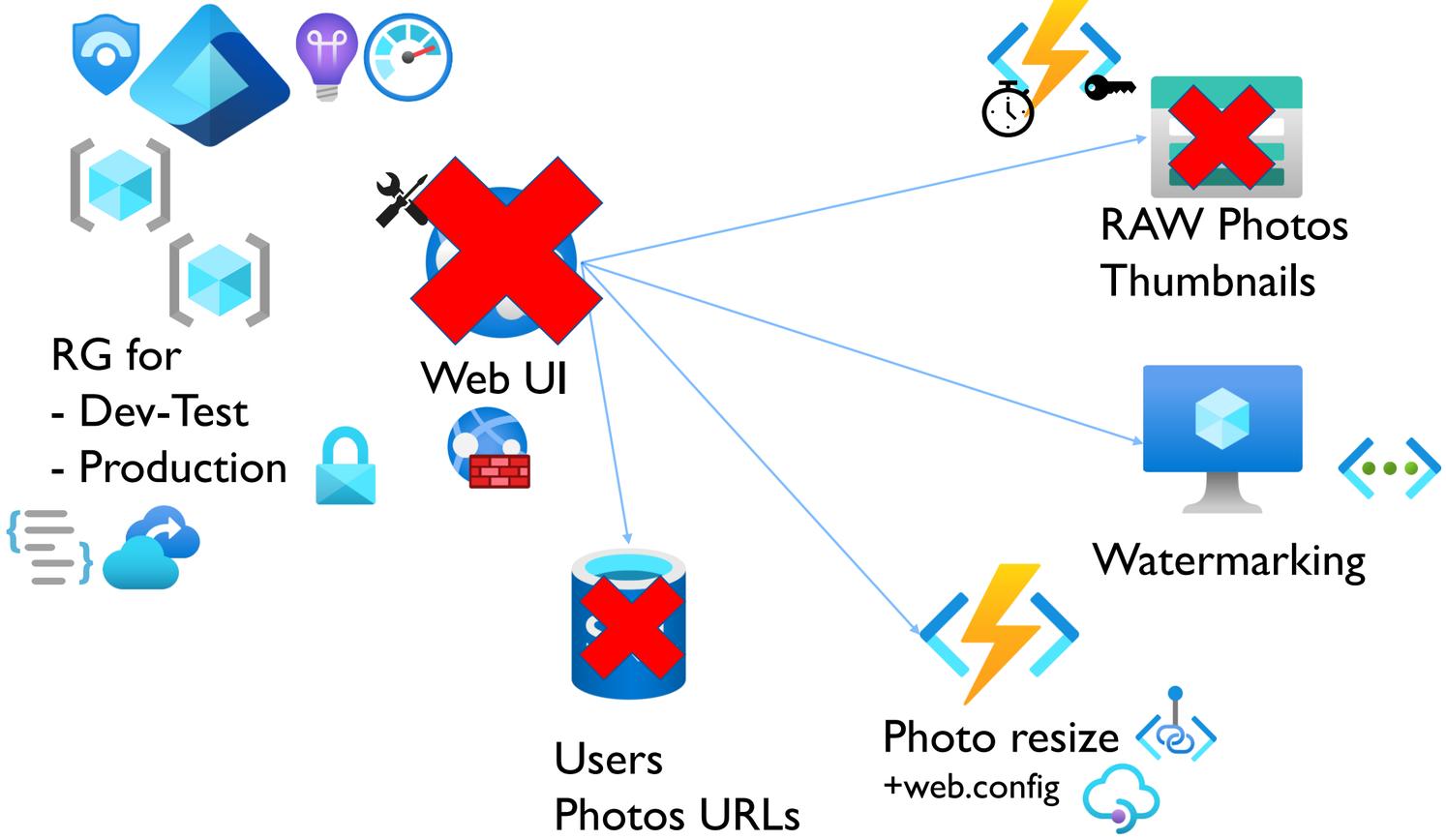
Remediation

- **Web App Firewall, Azure FrontDoor, Azure Firewall, Application Gateway, 3rd party**
- **API Management**
- **Azure DDOS Protections for VNET**



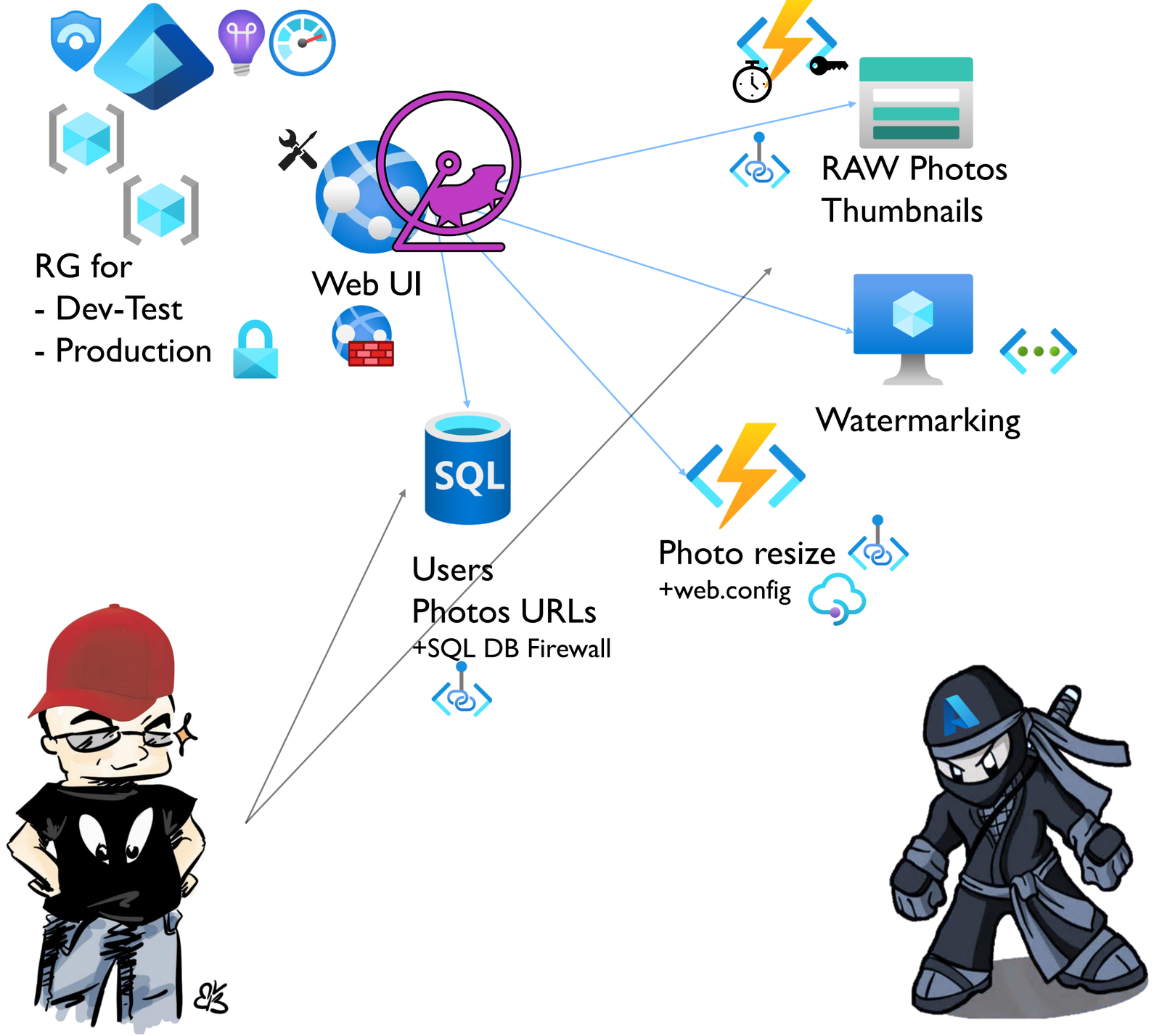
3rd Strike

The case of data and storage loss



Mitigation

- **Key rotation**
- **Least user privilege (DB)**
- **Defender for Cloud**
- **(Alerting)**

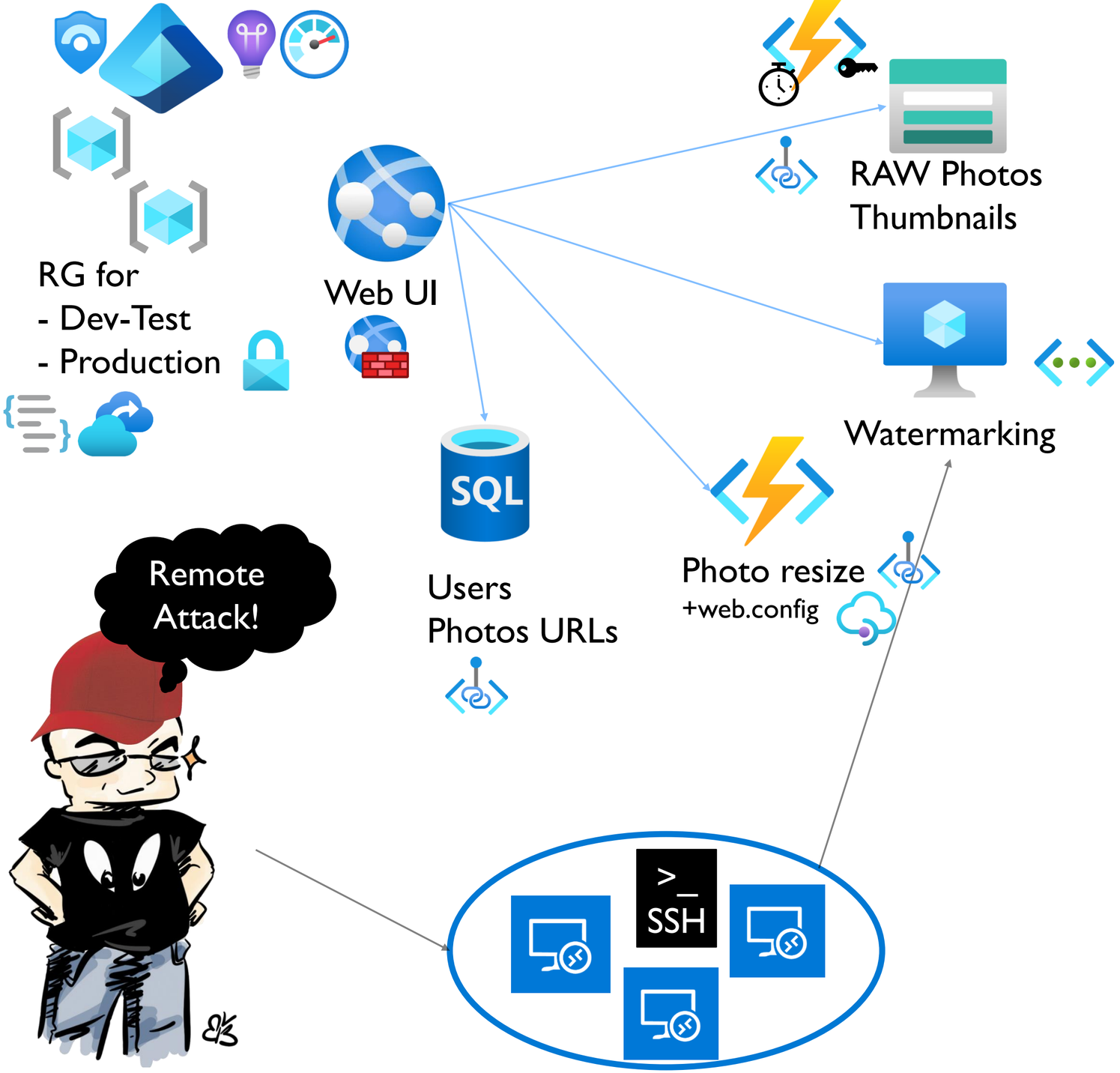


Remediation

- **SQL DB Firewall**
- **VNET Storage**
- **Private Endpoint**
- **Managed Identity**

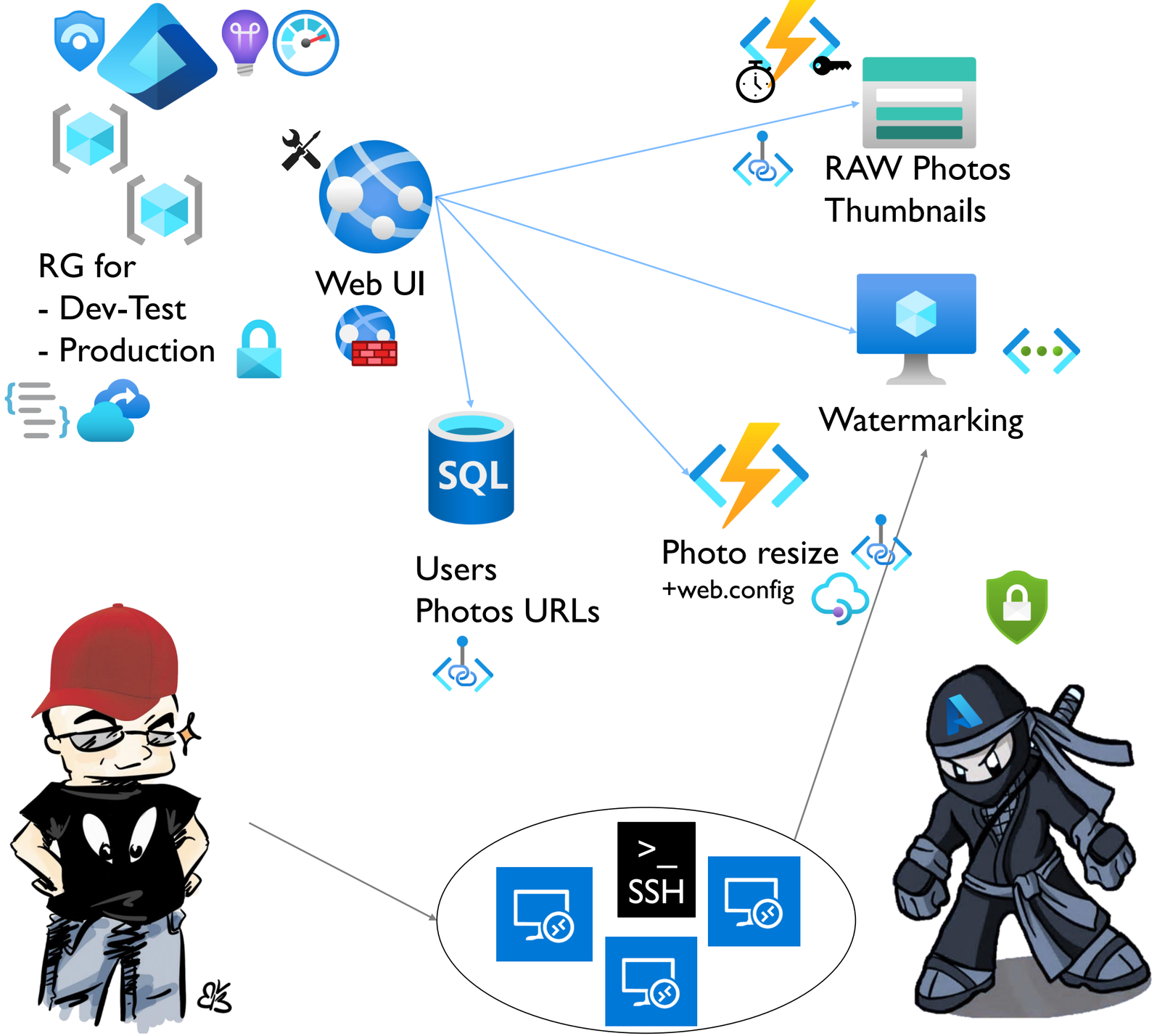
Handle Disconnect

Business Continuity and Disaster Recovery



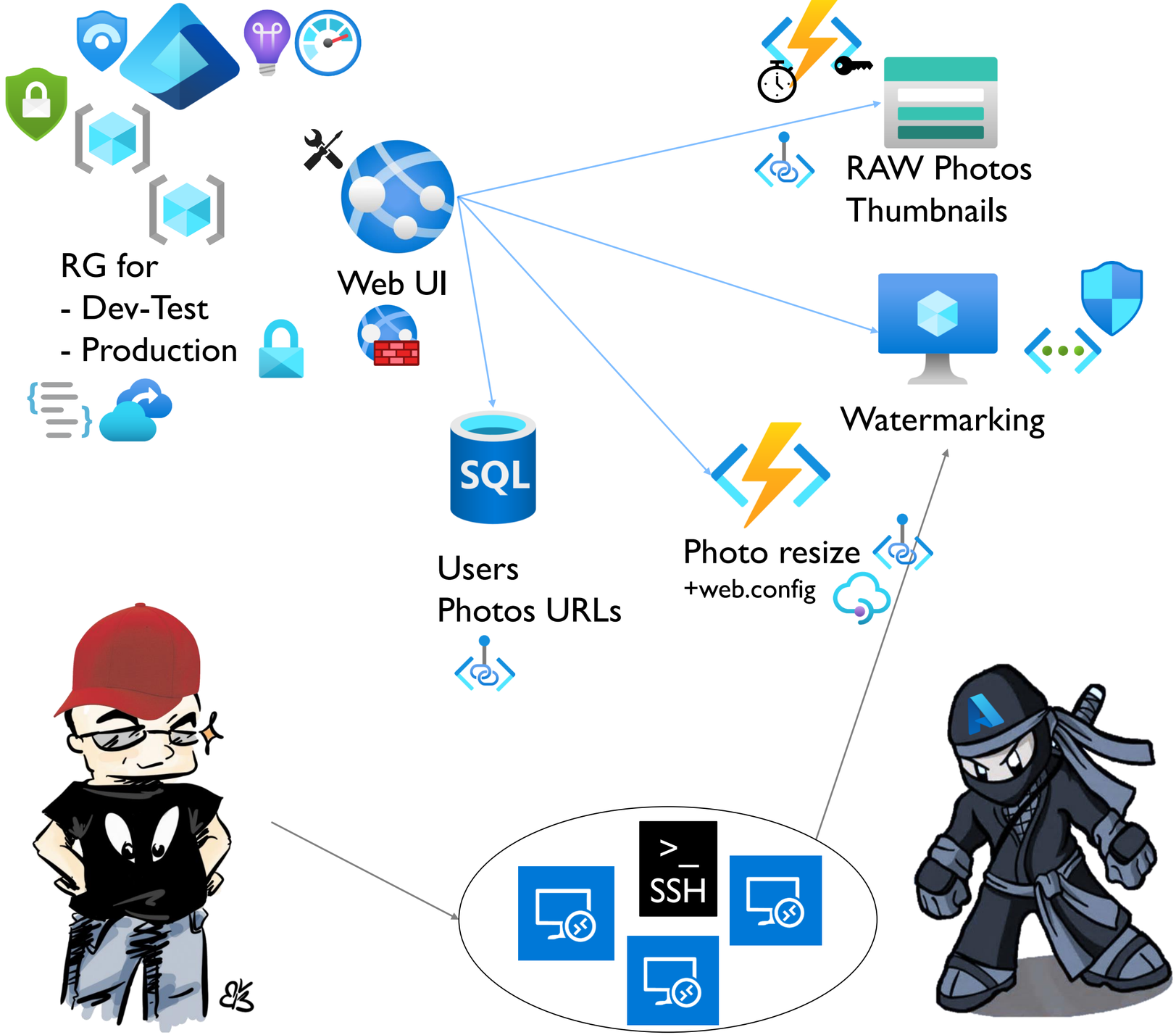
4th Strike

The case of remote connections



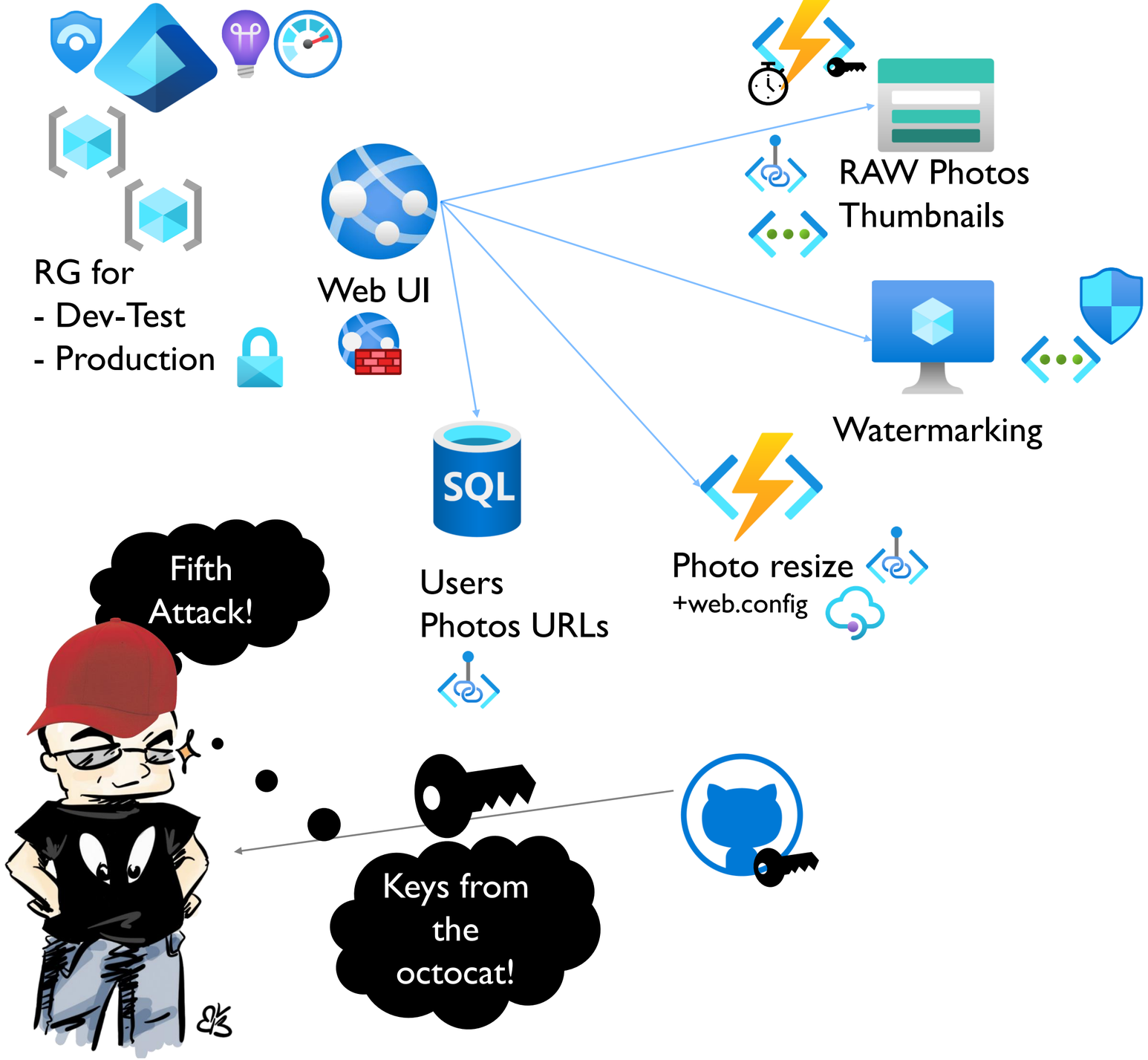
Mitigation

- **Patching and security policies**
- **Defender for Cloud**
  - **Not only for VMs, could check networks, App Services, Blob Storage, SQL, etc…**



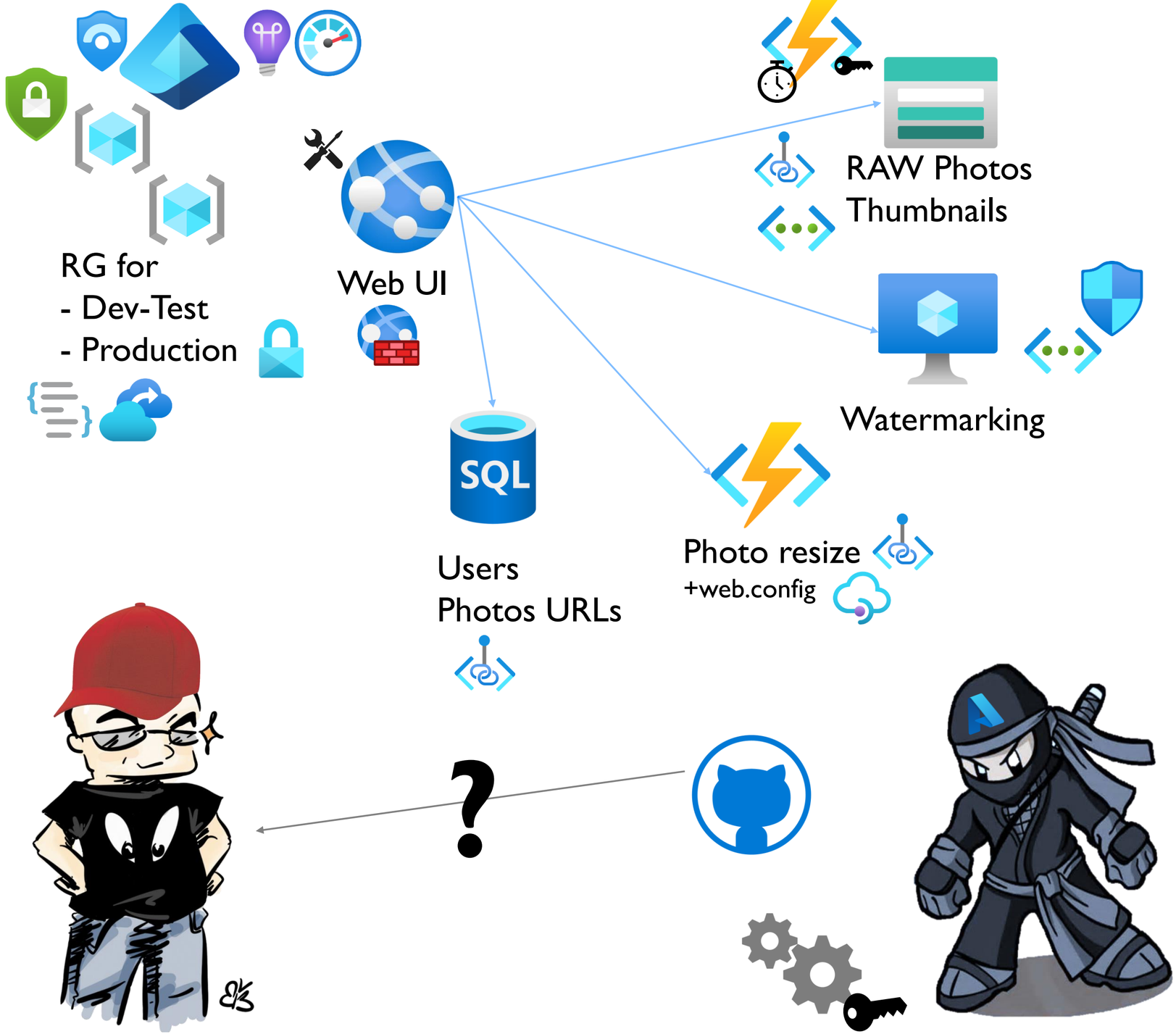
Remediation

- **Network Security Groups**
- **VNET**
- **Private Endpoint**
- **Azure Bastion**



5th Strike

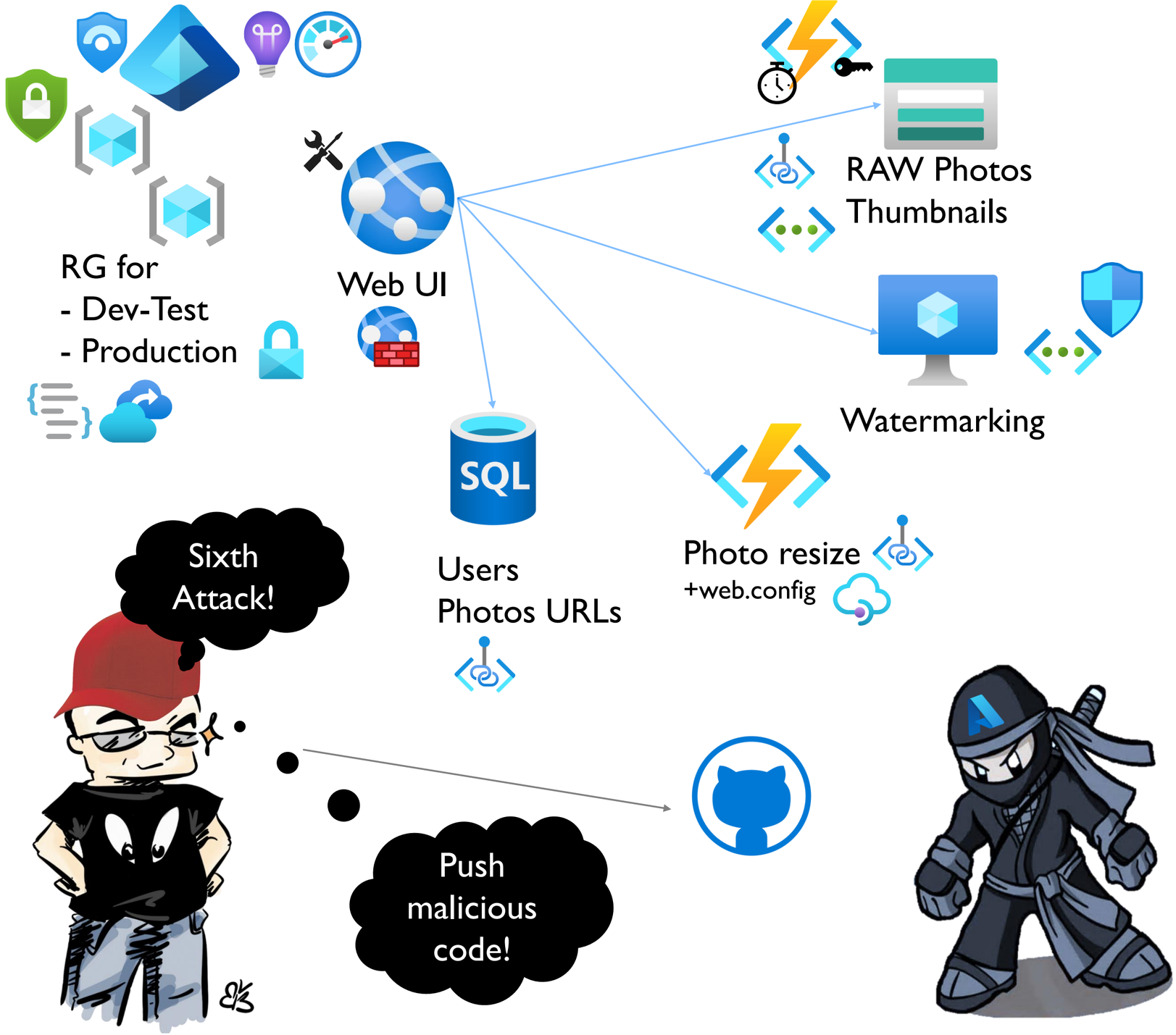
The case of being Gitted



Remediation

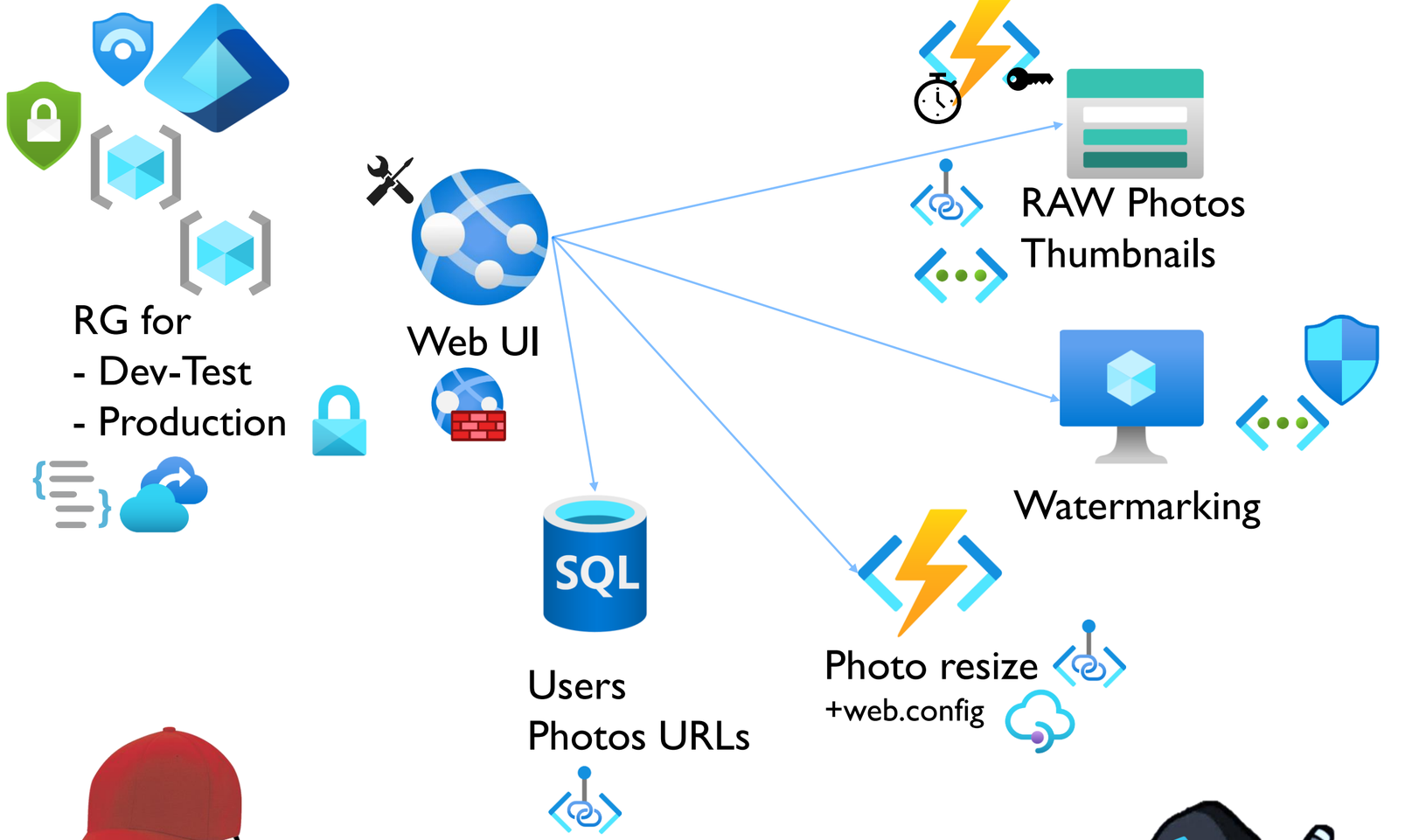
- **Move all the keys to a secure path**
- **GHAS Secret Scanning**
- **Use Azure Pipelines or GitHub Actions to set them before deployment**

- **Azure Key Vault**
- **Managed Identity**



6th Strike

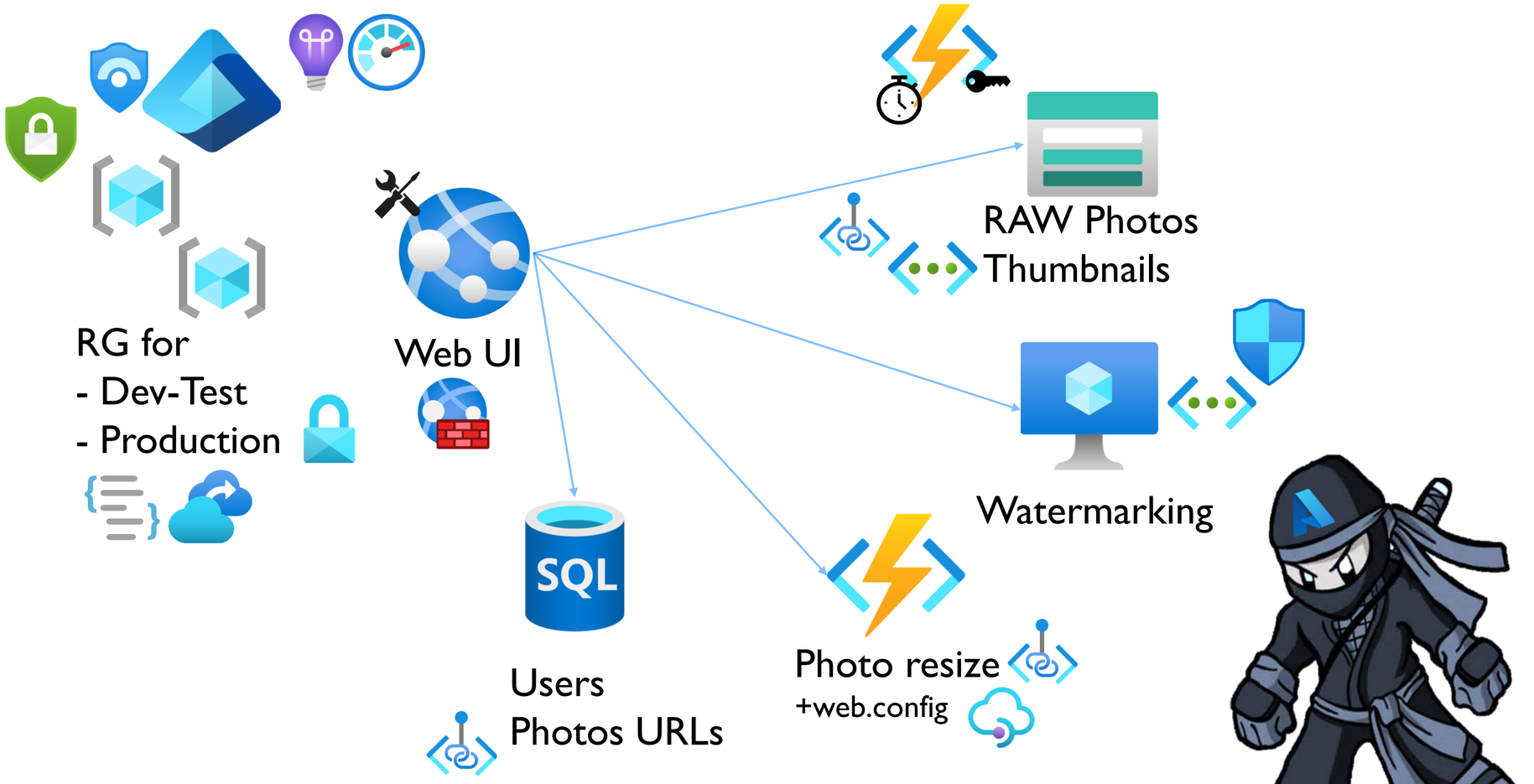
Push Malicious Code or Use Outdated Libraries



Remediation

- **Dependabot**
- **Code QL**
- **Code Scanning**
- **GitHub Copilot Enterprise**
- **PR Analysis**
- **Defender for Cloud**

A BETTER architecture



Recap – the 7 golden rules

- Script everything
- Backup everything
- Least user privilege
- Trust no one
- Monitor everything
- Assume cloud failure
- Protect your secrets and data

#GlobalAzure
#GlobalAzureMilano

GRAZIE!!!

Le slide saranno disponibili sulla pagina
Global Azure 2024 del sito di Azure Meetup Milano