white duck

DevOps practices for small teams and organizations, with a focus on security

Microsoft DevOps Forum 2021 – DevOps & Security

Microsoft Partner

Microsoft

Gold DevOps
Gold Cloud Platform

GitHub

Nico Meisenzahl

- Senior Cloud & DevOps Consultant at white duck
- Microsoft MVP, Docker Community Leader & GitLab Hero
- Container, Kubernetes, Cloud-Native & DevOps

Phone: +49 8031 230159 0
Email: nico.meisenzahl@whiteduck.de
Twitter: @nmeisenzahl
LinkedIn: https://www.linkedin.com/in/nicomeisenzahl
Blog: https://meisenzahl.org

Agenda

- Current state of DevSecOps in small teams & orgs
- Demo: Implementing quick wins
- Get started with DevSecOps
- Implement quick wins

Current state of DevSecOps

DevOps is now widely known and increasingly implemented in small teams & organizations.

DevSecOps practices, on the other hand, are not well-known and typically not yet adopted.

Current state of DevSecOps in small teams & orgs

- overall low Cloud / Cloud-Native security knowledge
- same “problems” with security as with QA
  - no big invests
  - no real focus until there is breach or issue
- no shift-left and fail-fast cultures
- no security baseline
  - like governance, policies and landing zones

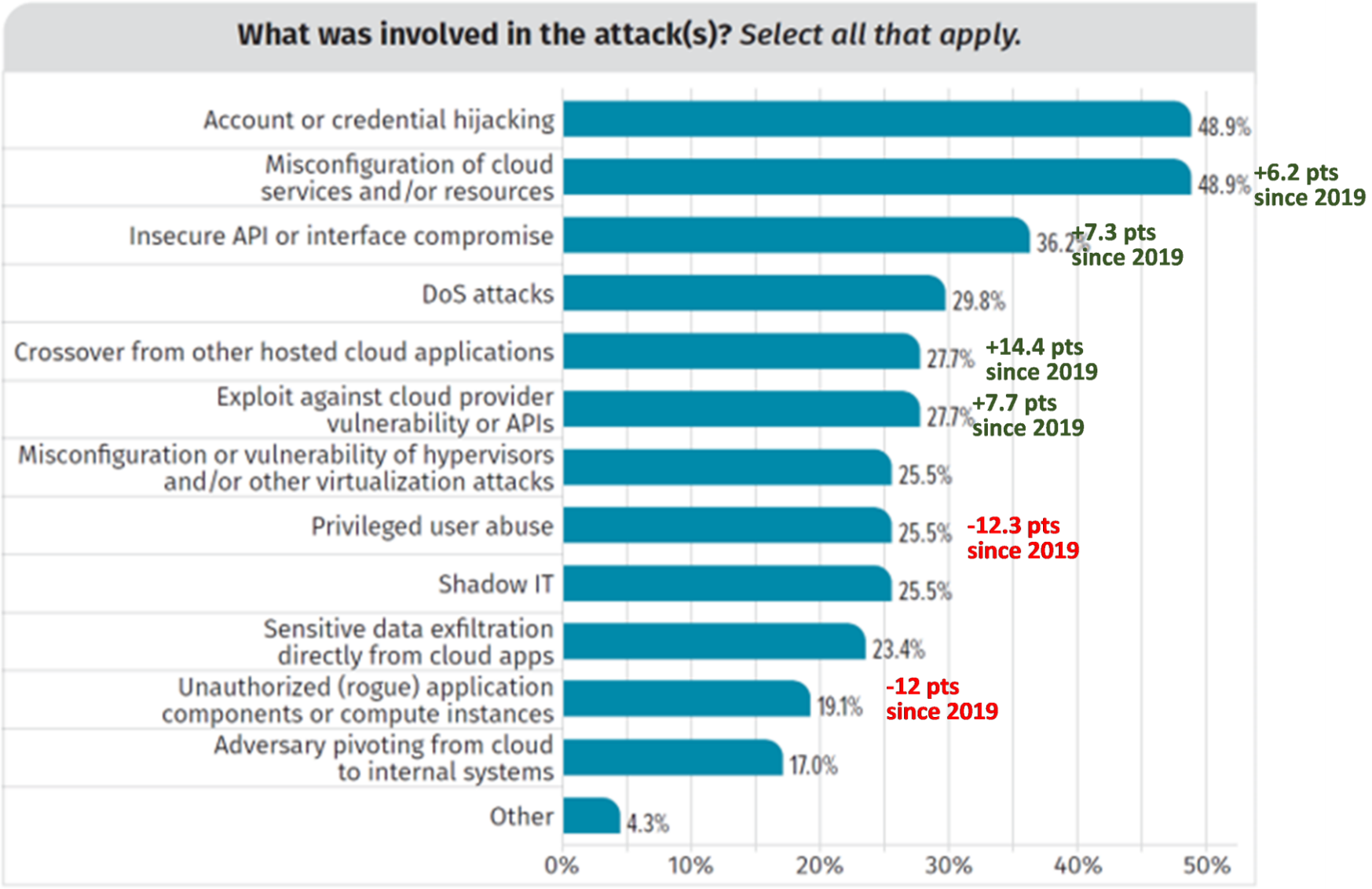
What we see at clients

- traditional IT departments trying to secure cloud-native projects by relying on on-premises and outdated patterns
  - slowing down of projects & inovation, but no real increased security
- an MVP (Minimum Viable Product) is leveraged as a long-term solution
  - skipped topics (in terms of time-to-market) are not considered anymore

What we see at clients

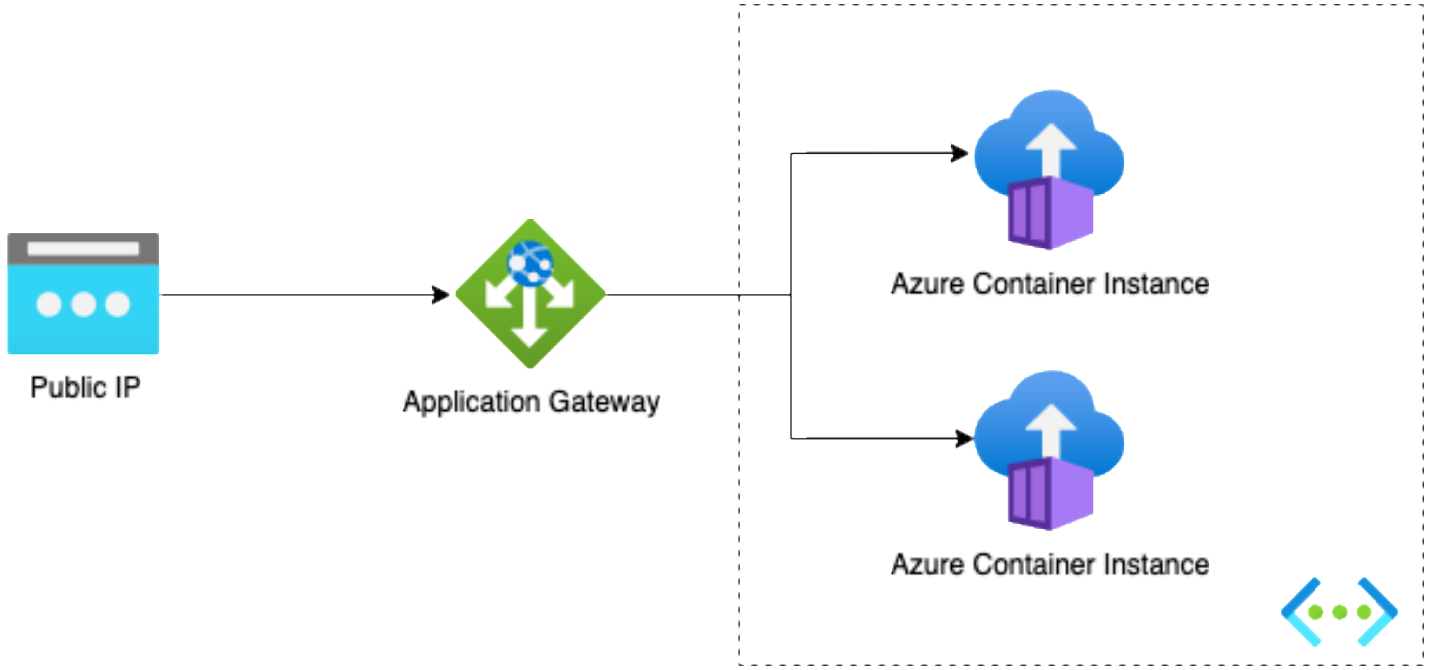
- self-managed resources are sometimes preferred over PaaS and SaaS
  - then, not maintained with the necessary staff to operate them safely
- self-implemented Identity management (AuthN, AuthZ)
  - without utilizing common best practices, managed services, and libraries/frameworks

SANS 2021 Cloud Security Survey



Demo – Implementing quick wins

- “Ping me app”, based on Golang, deployed to ACI and exposed via App Gateway



Demo recap

- we found a security vulnerability and injected commands
- we consulted the docs for security recommendations
- we implemented a Web Application Firewall (WAF) to secure our app
- we enabled Code Scanning in our GitHub Repo to fix the issue as well as to find future security issues in earlier stages

Get started with DevSecOps

- start small and grow
- introduce security into all DevOps stages
  - try to shift security to the left
  - implement zero-trust

Tip: Security should be easy to use, integrated and automated

Educate yourself

- consult documentation
  - general docs
  - Cloud Adoption Framework
    - https://docs.microsoft.com/azure/cloud-adoption-framework
  - Azure & GitHub at Microsoft Learn
    - https://docs.microsoft.com/learn
- join a local Meetup group
  - https://www.meetup.com/pro/azuretechgroups

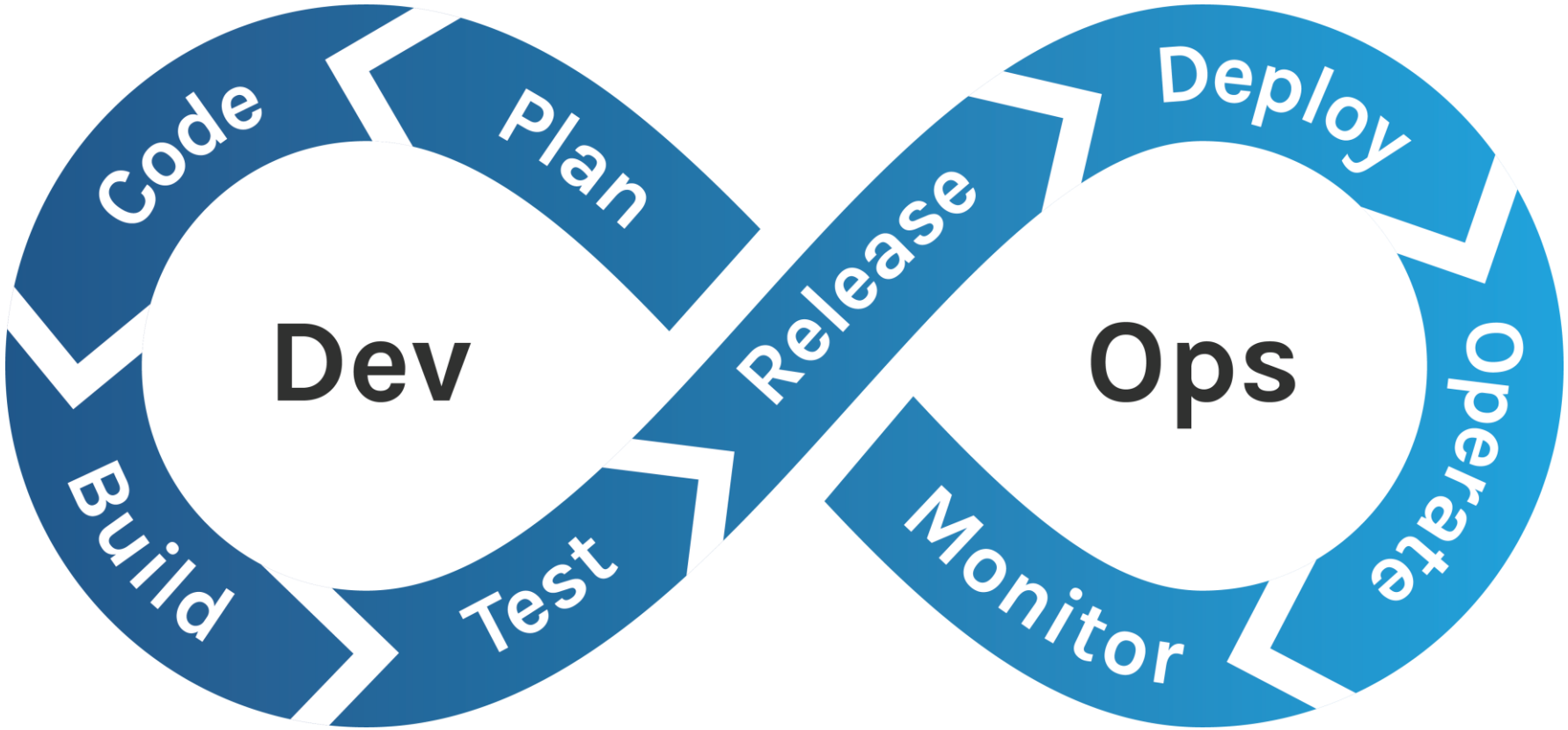
Tip: Get certified

Stay up-to-date

- Azure Updates
  - https://azure.microsoft.com/updates
- GitHub Updates
  - https://github.blog/changelog
  - https://github.blog/category/product
- Azure Friday
  - https://azure.microsoft.com/resources/videos/azure-friday

white duck

Security quick wins through the DevOps cycle



Enable your team

- integrate security staff in your development lifecycle (Sprint)
- educate developers to raise their security awareness
- implement pair programming
- enforce PR reviews

Ensure secure code

- automate and enforce code checks
- check your code for secret
- schedule dependency scanning
  - Dependabot
- enforce Static Application Security Testing (SAST) in PRs
  - scans your code to identify potential security vulnerabilities

SAST Tooling

- GitHub CodeQL
  - https://codeql.github.com
- .Net & .Net Core
  - https://security-code-scan.github.io
- Golang
  - https://securego.io
- Kubernetes manifests
  - https://kubesec.io
- Terraform
  - https://github.com/tfsec/tfsec

Ensure secure code (next stage)

- implement automated Dynamic Application Security Testing (DAST)
  - black-box scanning against a running web application
- scheduled scan your artifacts and containers
- sign your artifacts and containers

App Vulnerability Management Tooling

- Zed Attack Proxy
  - https://www.zaproxy.org
- DefectDojo
  - https://www.defectdojo.org

Ensure a secure runtime

- implement zero-trust
- automate everything (App and infrastructure deployments)
- prefer PaaS and SaaS over unmanaged services
- review Azure Advisor recommendations
  - opt-in for Azure Security Center to get even more insights
- design & implement a Cloud Governance strategy
  - IAM, Polices, Landing Zone, …

Monitor, review and iterate

- implementing security is not a one-time job
  - you need to stay up-to-date
- think big, but start small and iterate
  - as we do in application development

Implement best practices

- https://docs.microsoft.com/de-de/azure/security/
- https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra
- https://docs.microsoft.com/de-de/azure/architecture/solution-ideas/articles/devsecops-in-github

Questions?

Nico Meisenzahl (Senior Cloud & DevOps Consultant)
Phone: +49 8031 230159 0
Email: nico.meisenzahl@whiteduck.de
Twitter: @nmeisenzahl
LinkedIn: https://www.linkedin.com/in/nicomeisenzahl
Blog: https://meisenzahl.org