PUTTING 'SECURITY' INTO DEVSECOPS:

LESSONS LEARNED AT MICROSOFT: ONE PERSPECTIVE

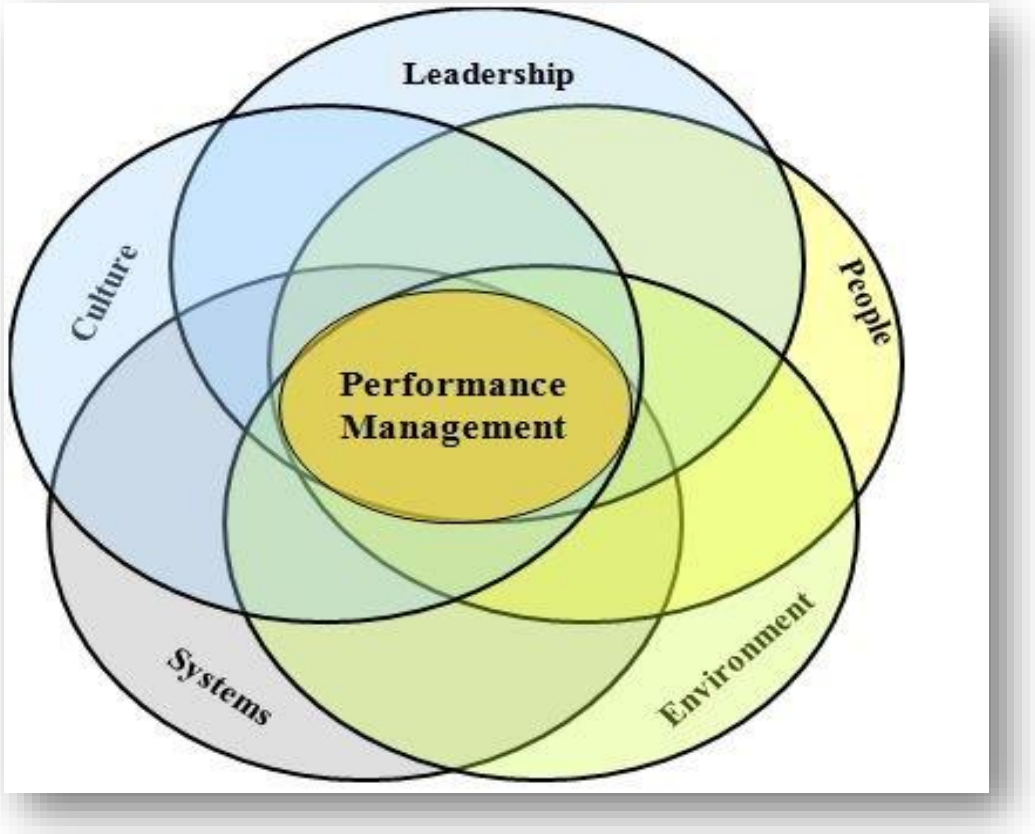
Michael C. Fanning
mikefan@microsoft.com

MICROSOFT ONE ENGINEERING SYSTEM (1ES)

The Microsoft One Engineering System (1ES) team was formed in 2014, with the goal of gaining efficiencies through a common engineering tool set.

https://azure.microsoft.com/en-us/solutions/devops/devops-at-microsoft/one-engineering-system/

LESSON: ONCE YOU'VE SOLVED CORE TECHNICAL PROBLEMS IN PROCESS IMPROVEMENTS, YOU'RE LEFT WITH THE NON-TECHNICAL.



Performance Management and the Human Error Factor: A New Perspective | Expert Commentary | IRMI.com

Fastest loop wins!

DevOps

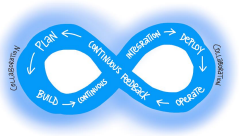
DevOps?

Fastest new product feature wins!

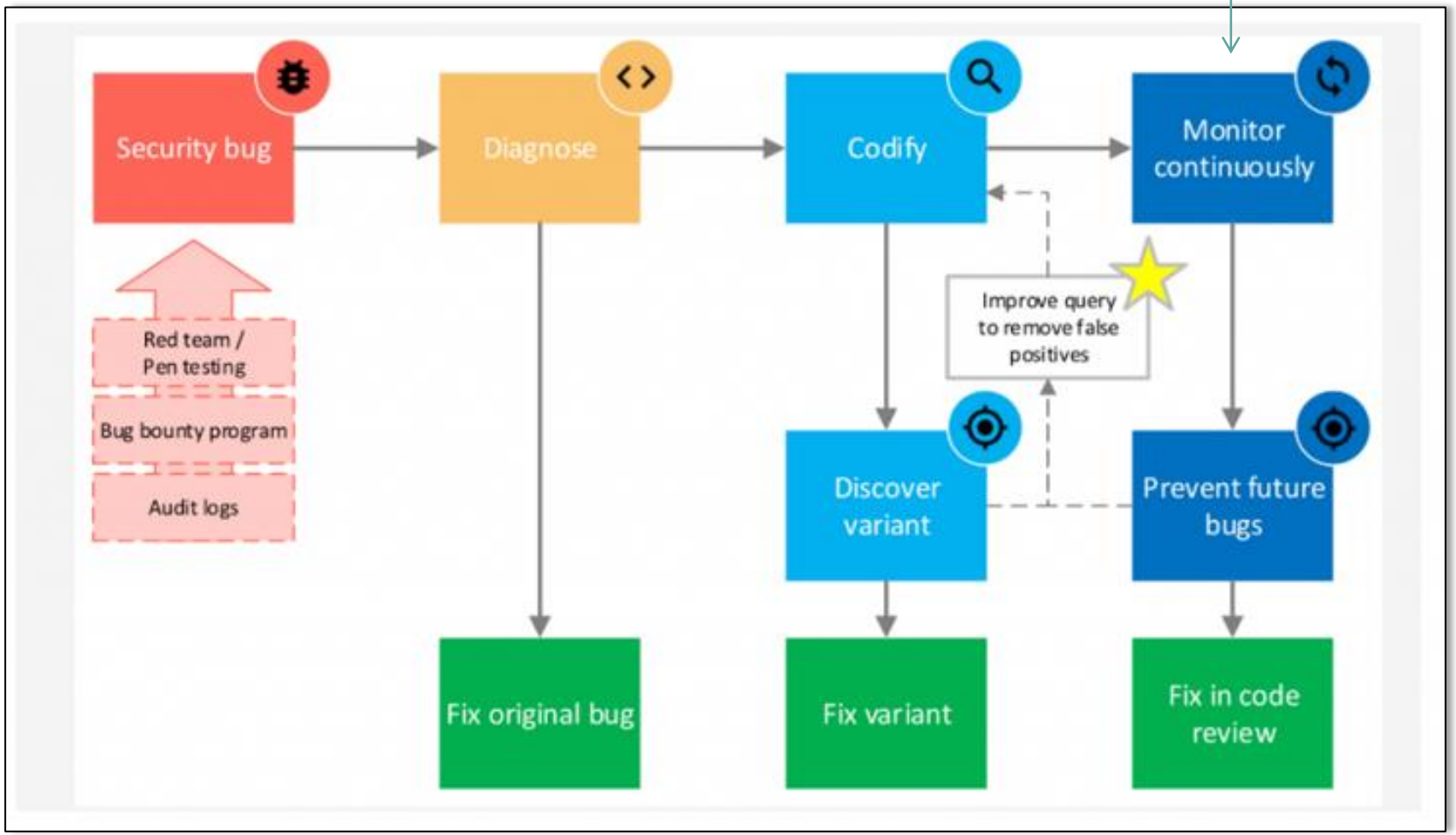
DevSecOps [...] is the principle of implementing security decisions and actions at the same scale and speed as development and operations decisions and actions.

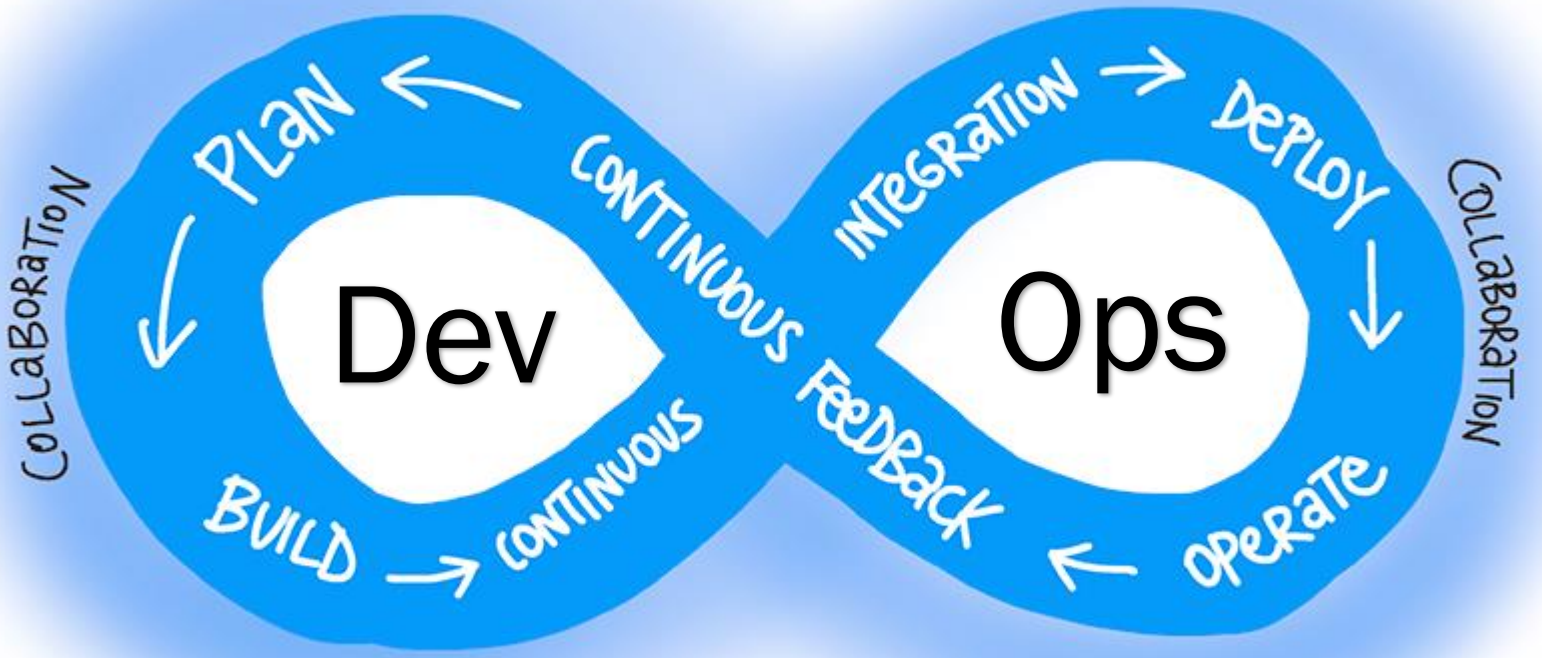
https://www.forcepoint.com/cyber-edu/devsecops | https://sonraisecurity.com/who-we-serve/devsecops/

A STATIC ANALYSIS SECURITY TESTING (SAST) LOOP



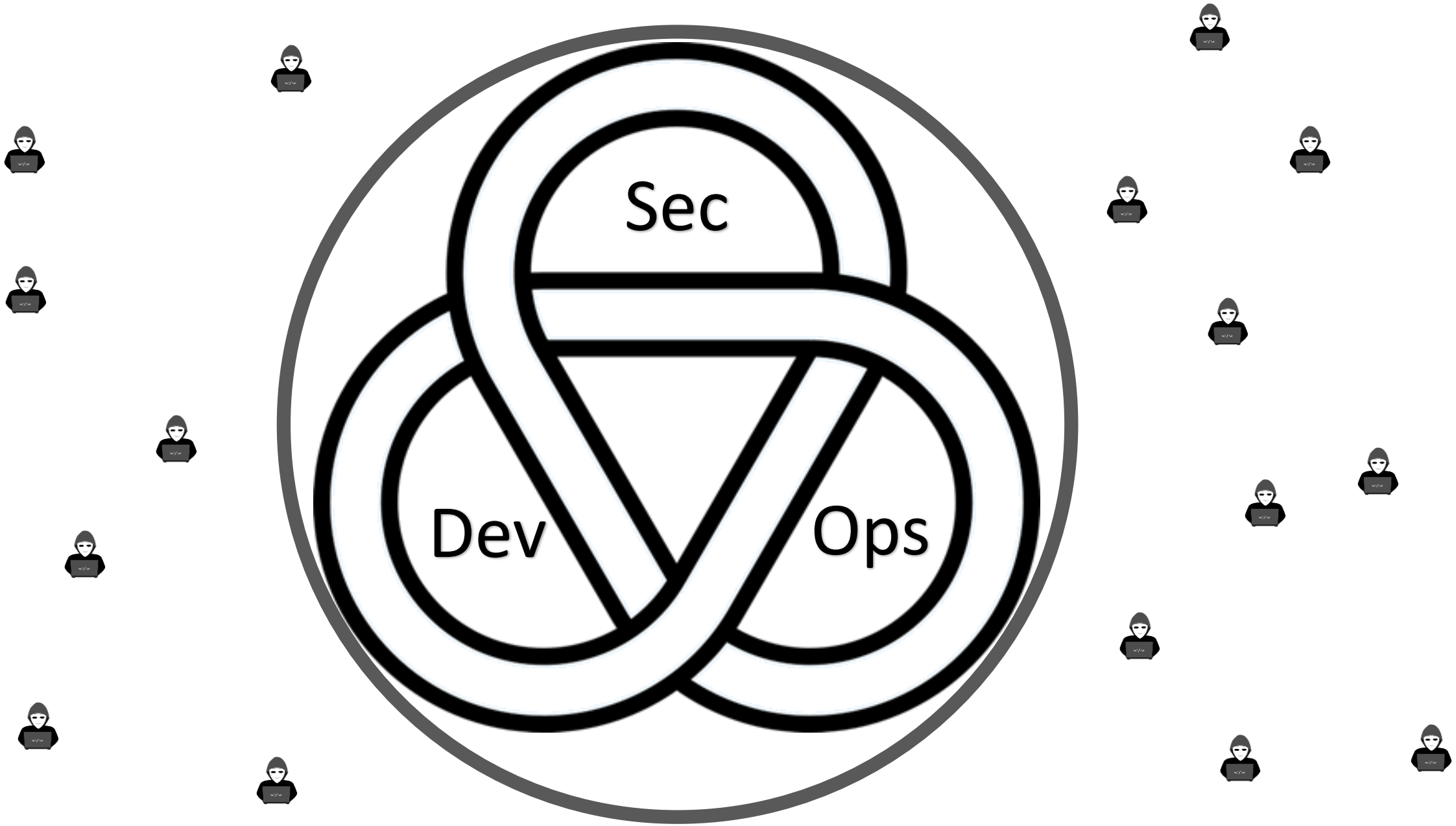
Drivers for security actions

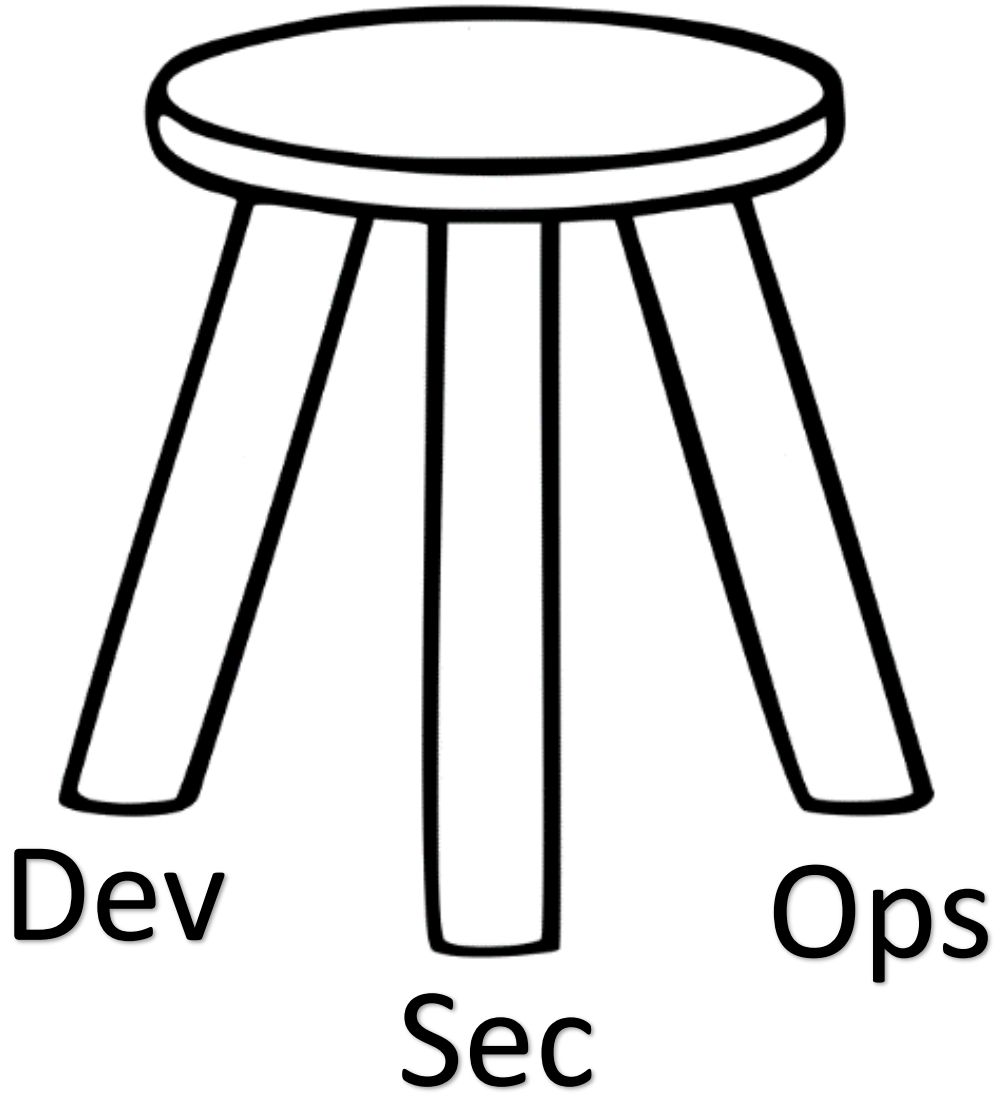




[What is DevOps? - Azure DevOps | Microsoft Docs]

https://docs.microsoft.com/en-us/azure/devops/learn/what-is-devops

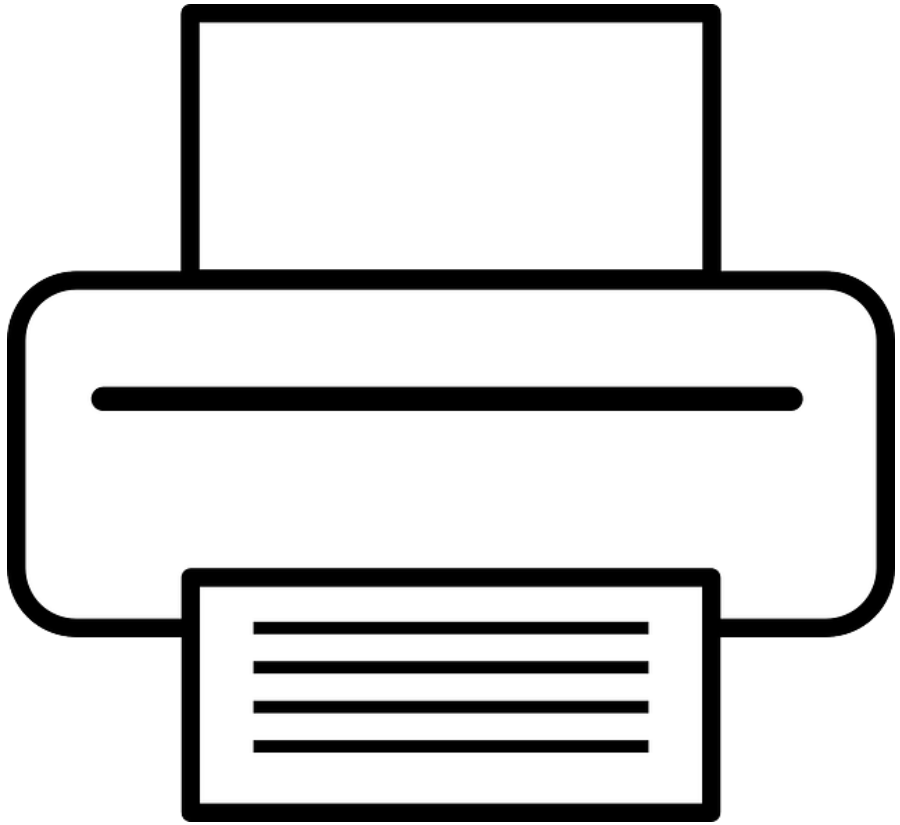

Sec
Dev
Ops


Dev
Sec
Ops

DevSecOps

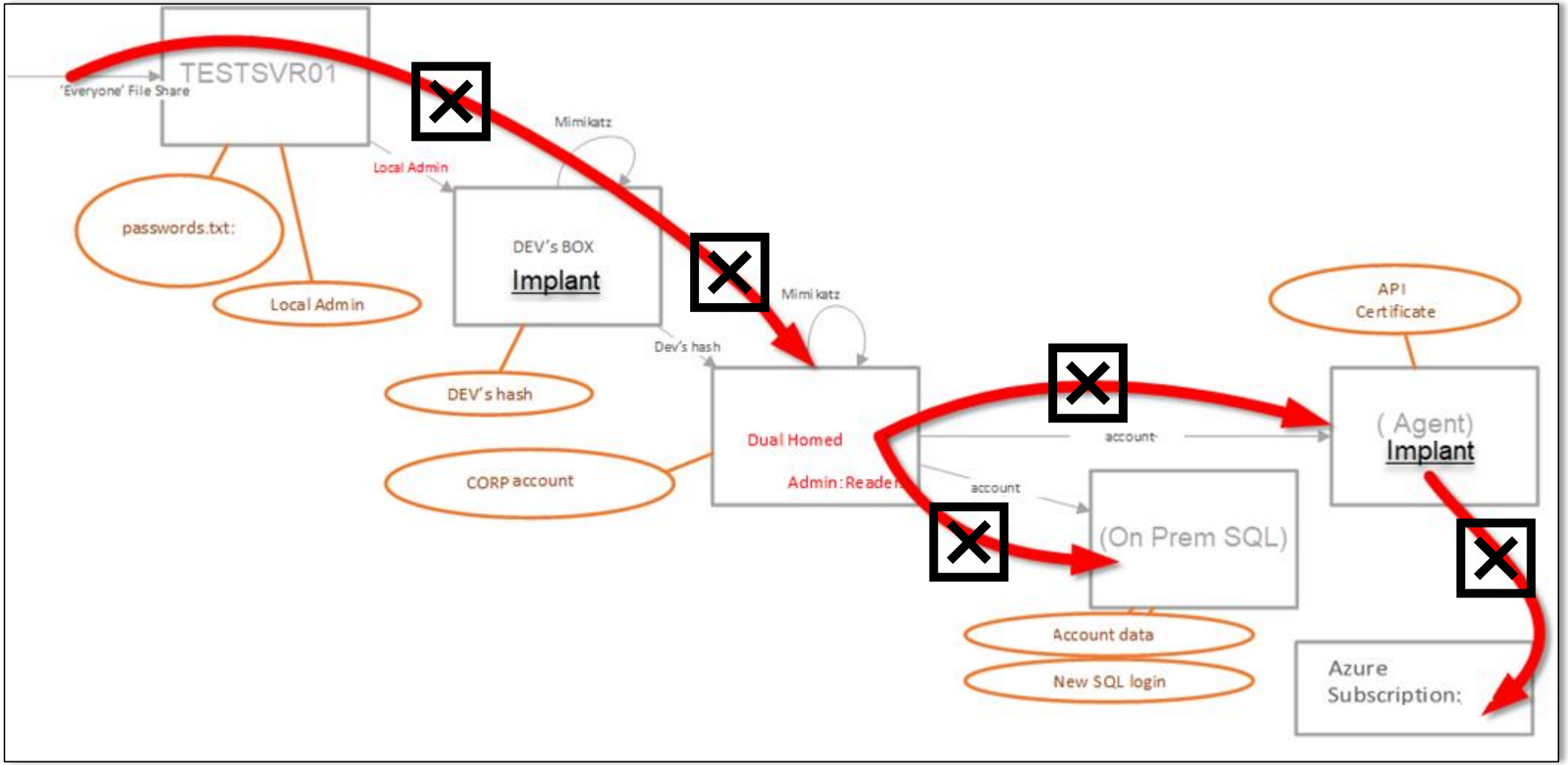
Fastest new product feature, of verified quality & provenance, deployed to a secure environment, wins!

FOUNDATIONAL LESSONS FROM SECURITY EXERCISES

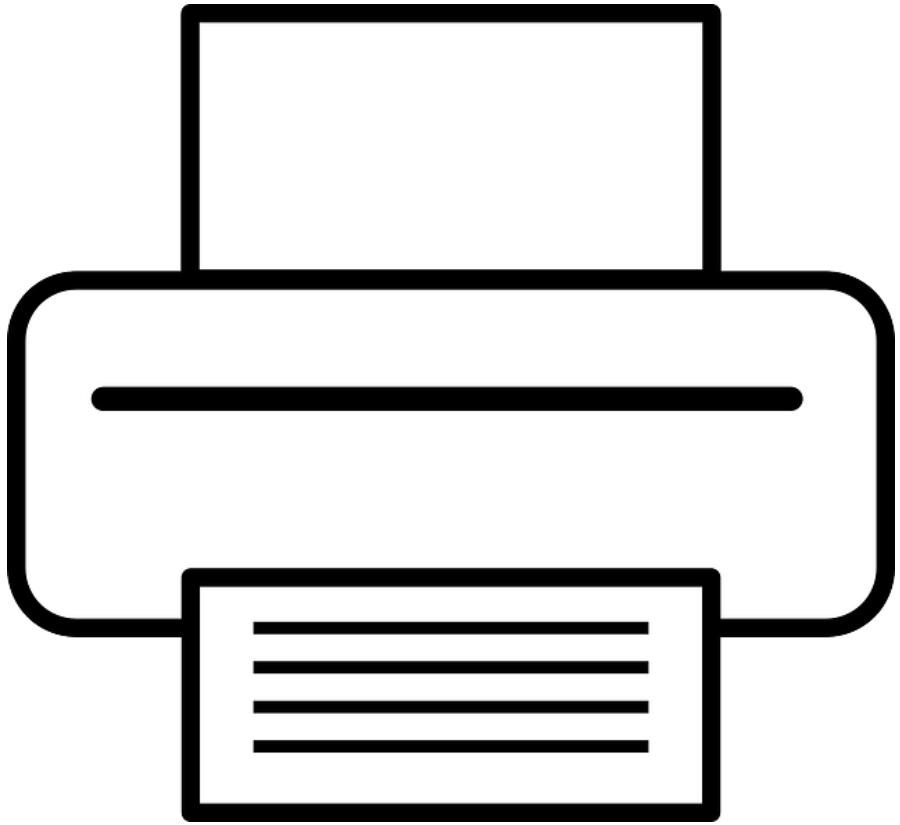


- Plaintext secrets and OSS vulns are a primary source of potential attacker foothold
- Entire system needs hardening to block lateral movement

ILLUSTRATIVE RED-TEAM (PENETRATION TEST) ATTACK WITH LATERAL MOVEMENT



FOUNDATIONAL LESSONS FROM SECURITY EXERCISES

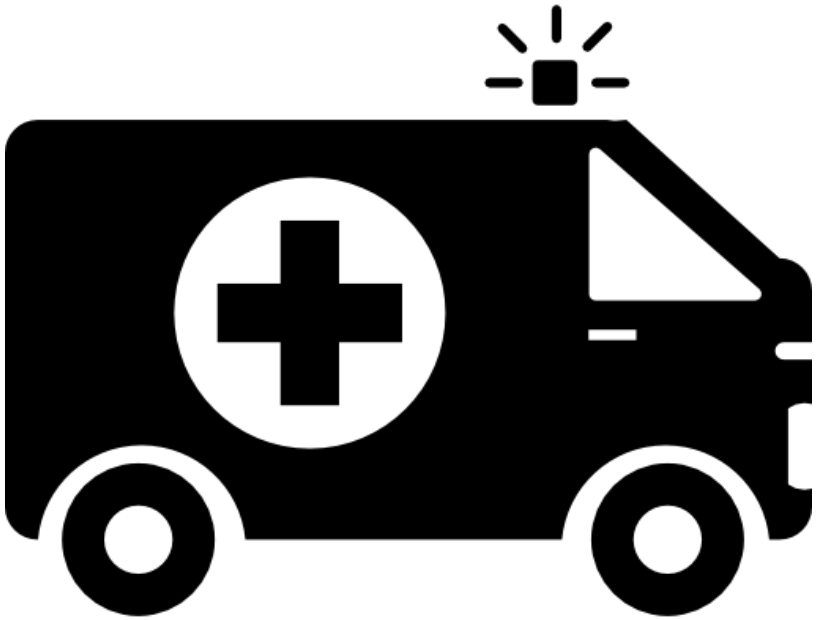


- Plaintext secrets and OSS vulns are a primary source of potential attacker foothold
- Entire system needs hardening to block lateral movement
- Identity verification is critical
- Build processes warrant dedicated, secure environment

BEST PRACTICES: ISOLATION & IDENTITY

- MFA
- No direct access to production
- Just-In-time perms elevation only: no persistent access
- Zero persistent admin accounts
- Secure Access Workstation only

TOP OF MIND FOR REMEDIATION & RESPONSE



Inject communication and control points throughout the dev loop

Drop in code attribution for risk and ownership

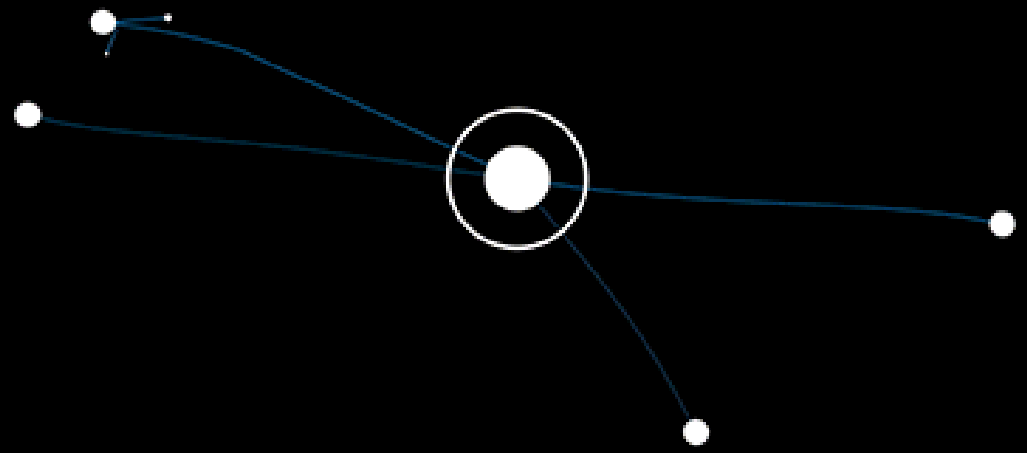
Developer Education

SUPPLEMENTAL LINKS

- A Microsoft DevSecOps Static Application Security Testing (SAST) Exercise
- Reproducible Builds
- Software Bill of Materials | CISQ
- A case study on how SAP built a git repos scanner to detect credentials
- Behind the scenes of GitHub Token Scanning
- Scan open-source components for vulnerabilities in Azure Pipelines
- Microsoft DevOps Stories

Microsoft

Thank you!



Michael C. Fanning
mikefan@microsoft.com