A Practical Approach for Injecting Sec into DevOps

Jon Jarboe
Developer Advocate

75B

Growing to
75 Billion by 2025

35B

35 Billion users and devices
connect to the cloud every day

*Source: The IoT Rundown for 2020: Stats, Risks, an d Solutions, Security Today

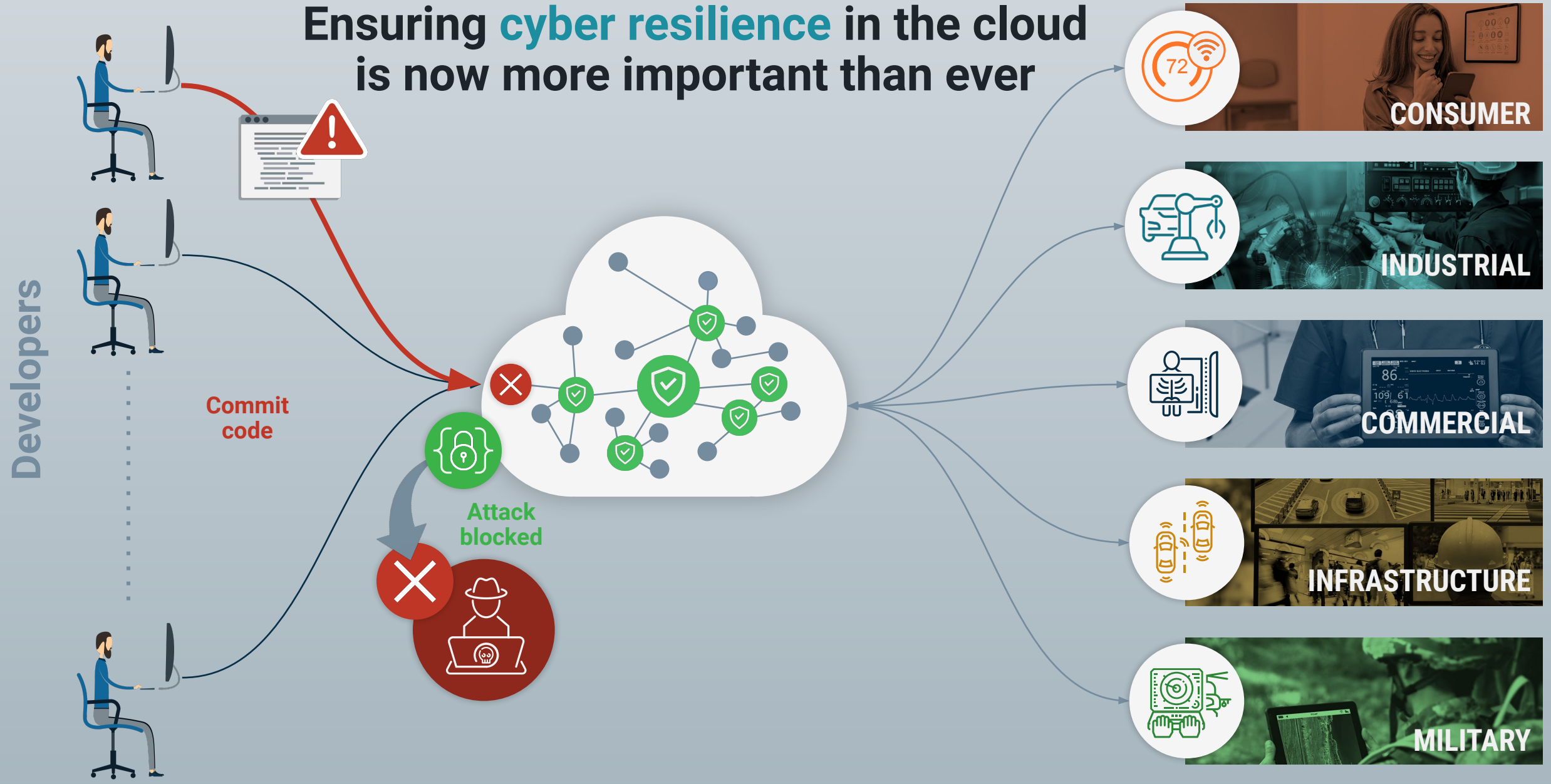
But the cloud is continuously changing ...

Developers

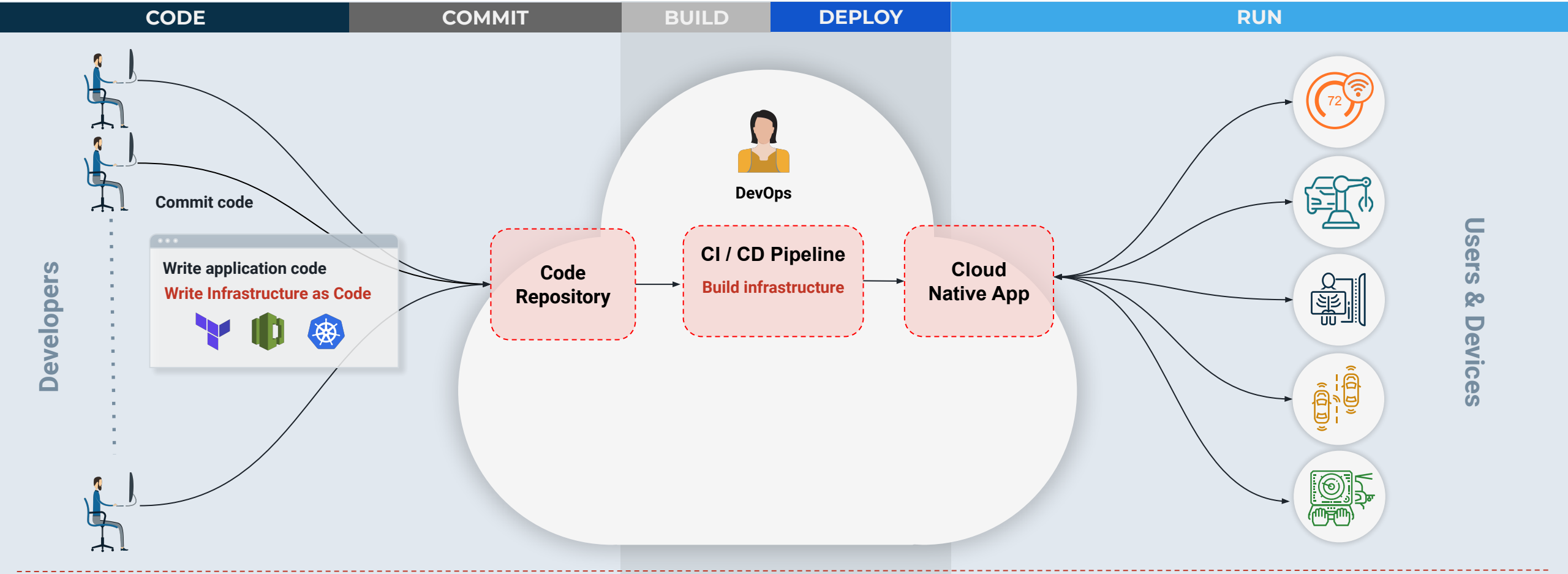
Commit code

4 Million
code commits in the cloud every day

Ensuring cyber resilience in the cloud is now more important than ever



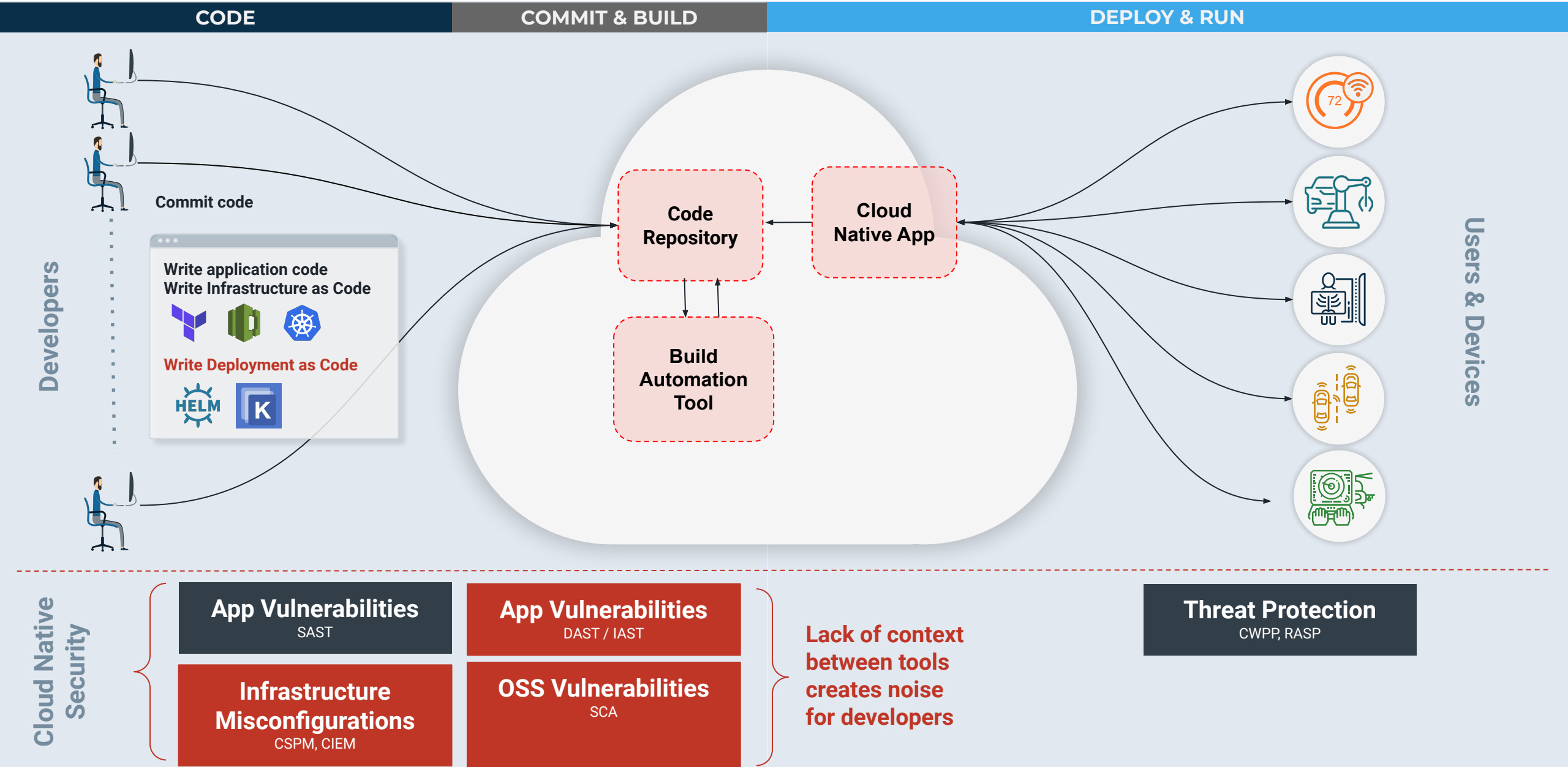
Traditional cloud security tools are **not built for developers**



Cloud Native Security

App Vulnerabilities SAST	**App Vulnerabilities** DAST / IAST	**Threat Protection** CWPP, RASP
Infrastructure Misconfigurations CSPM, CIEM	**OSS Vulnerabilities** SCA	**Infrastructure Misconfigurations** CSPM, CIEM

And security only gets more challenging as **developers embrace GitOps**



Programmatically Detect Breach Paths During Development

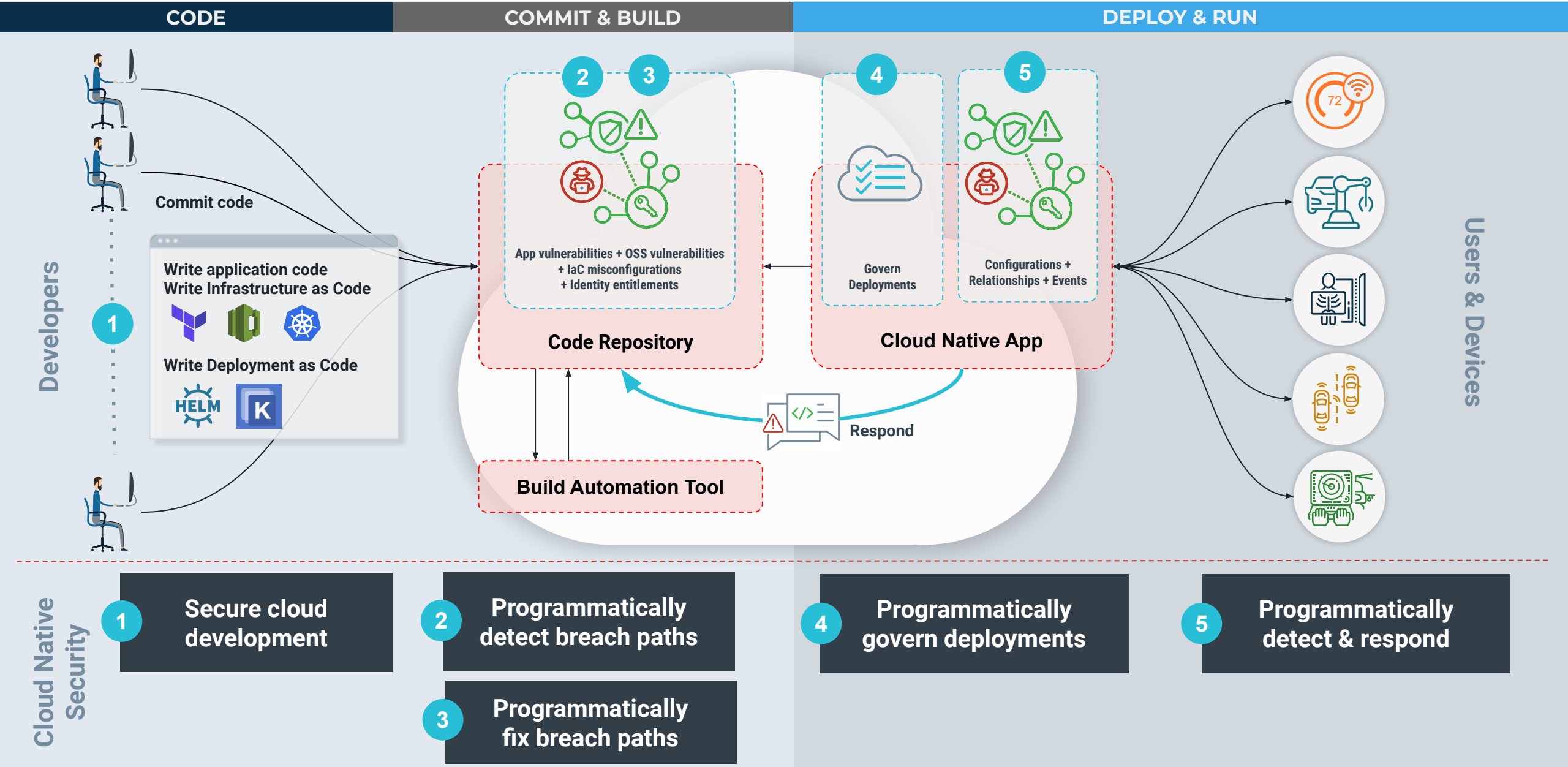
SSRF Vulnerability (CWE-918)

Misconfigured Compute Resource

Overly Permissive IAM / RBAC Policies

Unencrypted Database

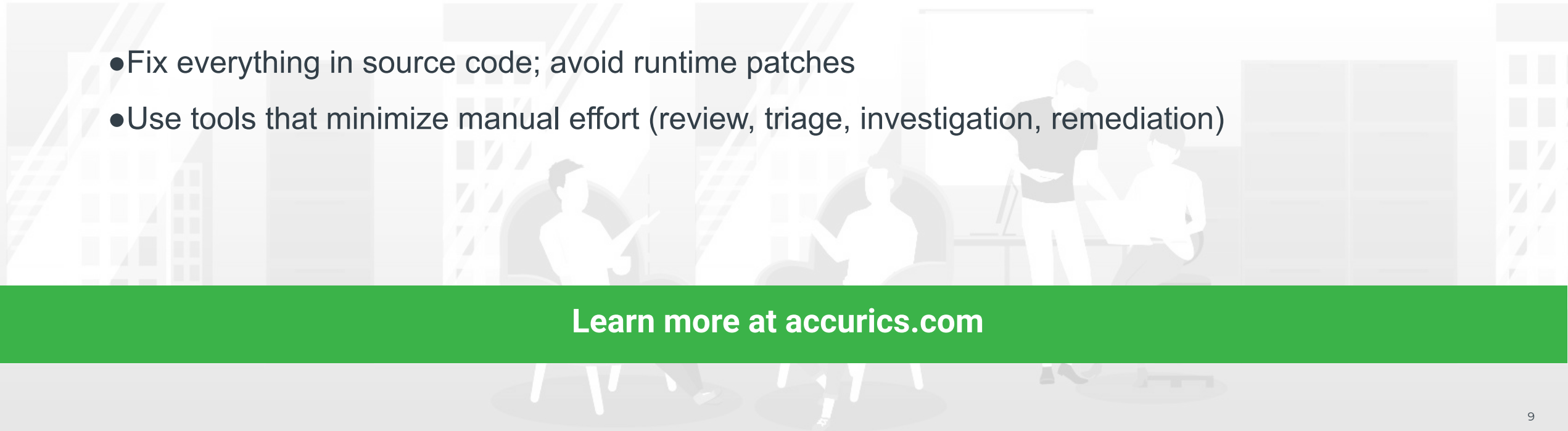
A developer-first approach to security enables DevSecOps



A Practical Approach for Injecting Sec into DevOps

1. Contextualize security findings
2. Programmatically detect breach paths
3. Programmatically fix breach paths
4. Programmatically govern deployments
5. Programmatically detect and respond to runtime threats

- Fix everything in source code; avoid runtime patches
- Use tools that minimize manual effort (review, triage, investigation, remediation)



Learn more at accurics.com

Thank You

Email: jon@accurics.com

accurics™

Immutable Security™