Alkalmazásbiztonsági trendek

DevOps Success

208x
More frequent
code deployments

106x
Faster lead time
from commit to deploy

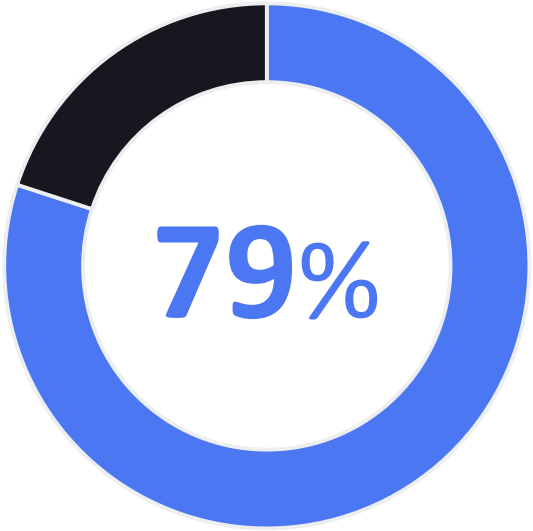
2604x
Faster time to recovery
from incidents

But security was left out

Why?

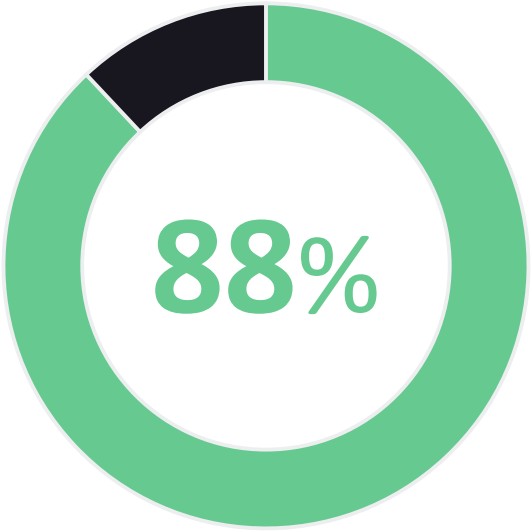
- Security is a specialist discipline
- Security is driven by compliance, which is not the focus of DevOps
- Developers deliver functional code fast
- Anything else is friction
- Security creates too much noise

Most applications have security issues!



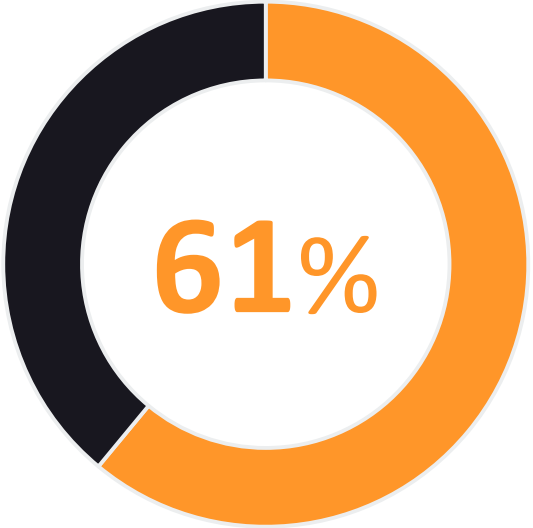
of web apps

have at least one critical or high severity issue



of mobile apps

have at least one critical or high severity issue



of apps

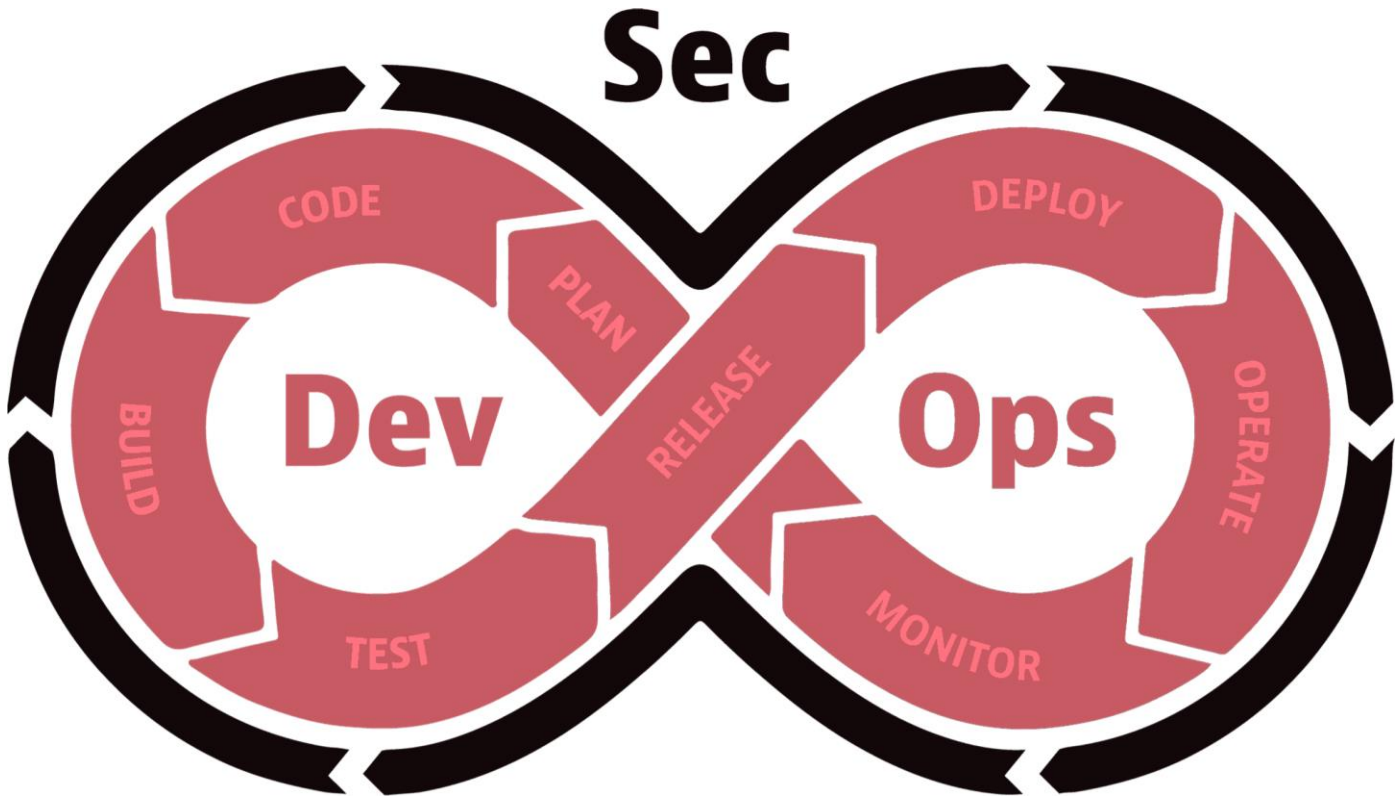
have critical or high vulnerabilities not covered by the OWASP Top 10

Source: “2019 Application Security Risk Report” by the Fortify Software Security Research team

Time to put the Sec into DevOps → DevSecOps

AppSec tooling becomes embedded in the DevOps toolchain

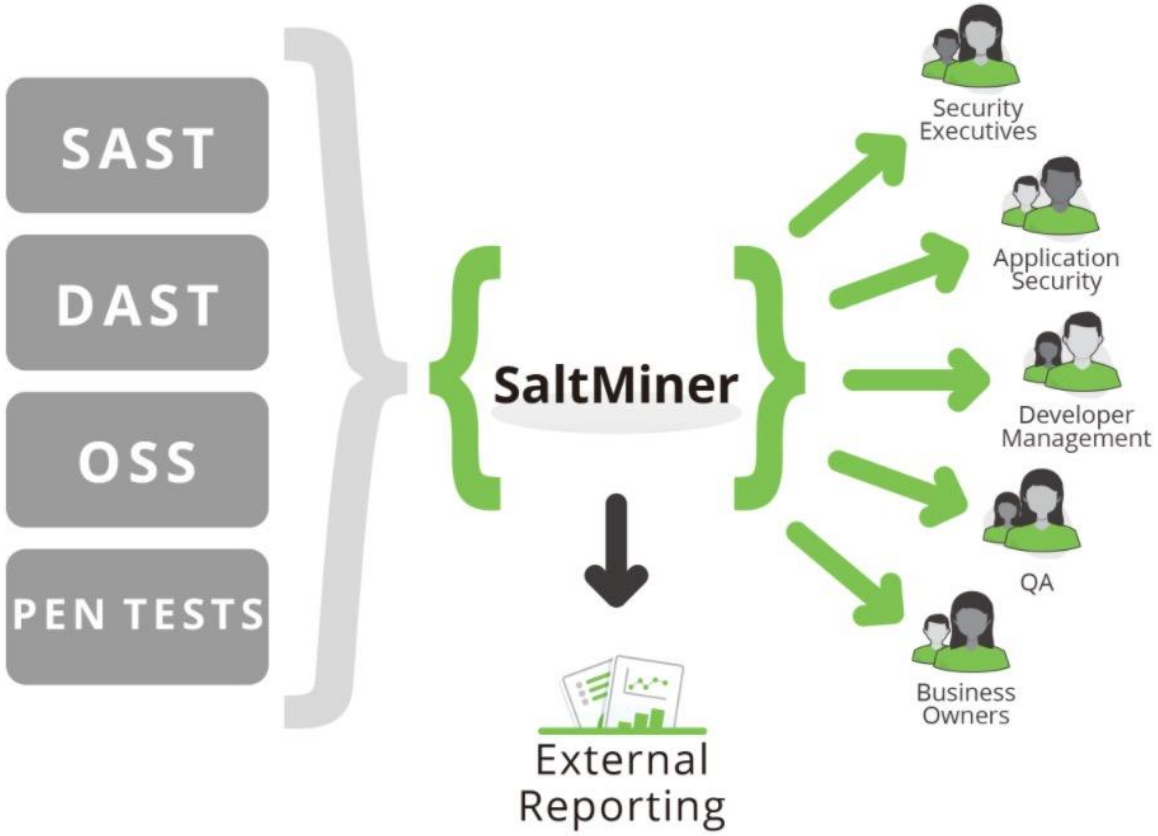
- Speed > Accuracy
- Ease of use > Depth
- Cloud platforms on the rise
- Developer driven



SAST and DAST become truly integrated

Vulnerability Management takes a step forward

Tools that **aggregate information** from multiple sources and present that risk in a rollup view

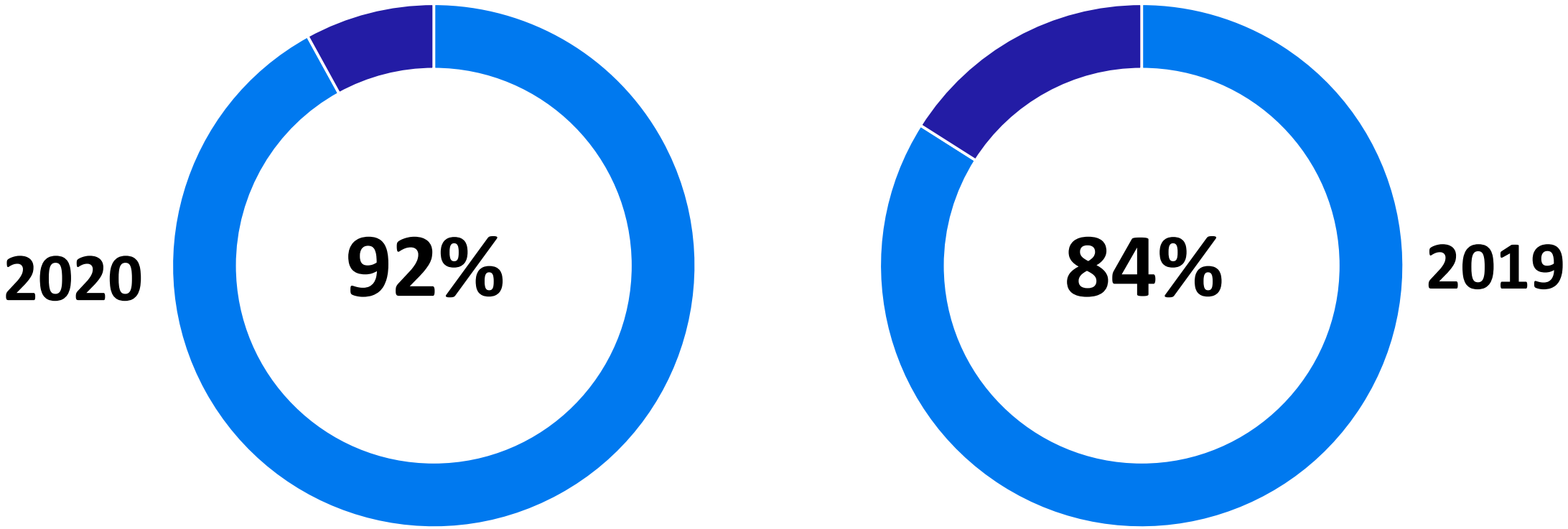


APIs enable rapid innovation, but have unique security challenges

APIs (Application Programming Interfaces):

- critical part of modern mobile, SaaS and web applications
- found in customer-facing, partner facing and internal applications
- APIs expose application logic and sensitive data such as PII and because of this have increasingly become a target for attackers

Container Security



Organizations using containers in production*

*2020 report from Cloud Native Computing Foundation

Open Source Prioritization

Open source vulnerabilities are an ongoing issue

OWASP Top 10 - 2013	OWASP Top 10 - 2017
A1 - Injection	A1 - Injection
A2 – Broken Authentication and Session Mngmt	A2 – Broken Authentication
A3 – Cross-Site Scripting (XSS)	A3 – Sensitive Data Exposure
A4 – Insecure Direct Object References	A4 – XML External Entities (XXE)
A5 – Security Misconfiguration	A5 – Broken Access Control
A6 – Sensitive Data Exposure	A6 – Security Misconfiguration
A7 – Missing Function Level Access Control	A7 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Insecure Deserialization
A9 – Using Known Vulnerable Components	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Insufficient Logging & Monitoring

Open Source Prioritization

99%

of codebases audited in 2019 contained open source components

82%

of codebases had components that were more than four years out of date

37%

of firms surveyed still plan on doing software composition analysis (SCA) only during the testing phase, where remediation is much harder

95%

of 1,000 enterprise IT leaders thought open-source is "strategically important to their organization's overall enterprise infrastructure software strategy."

Open Source Prioritization

Auditing open source issues is a long, manual process…

20

Minutes spent

On average to manually research an open source finding

38

Open source issues

The average application SCA scan identifies

100

Applications+

Each enterprise organization has on average

Source: 2020 State of the Software Supply Chain

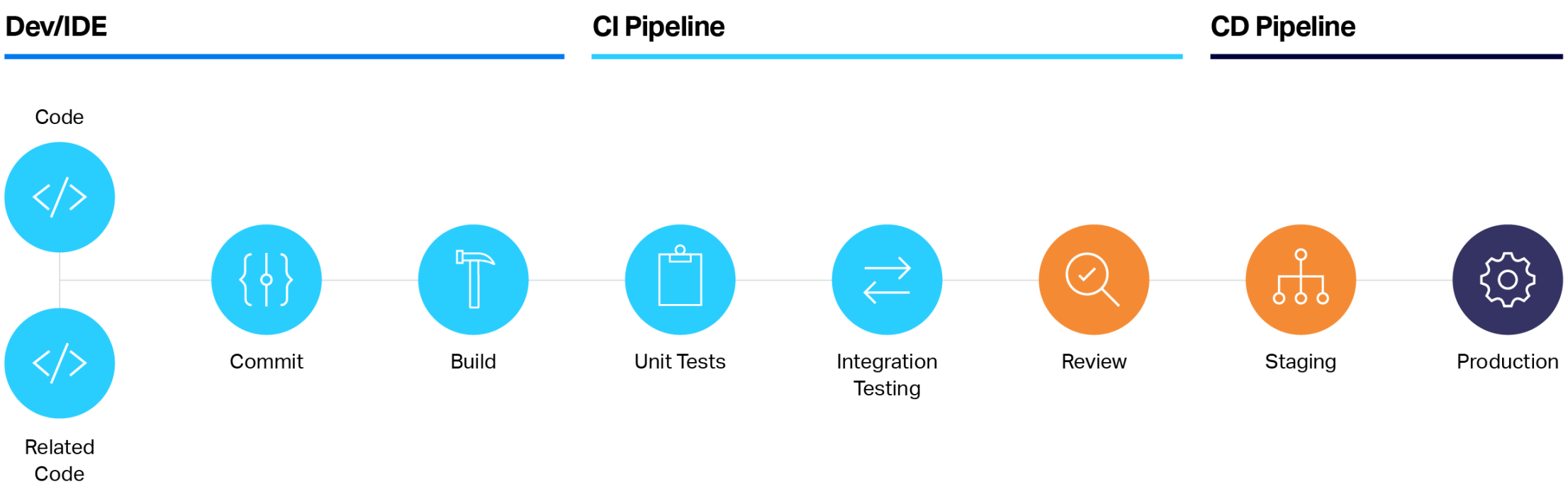
1266+ hours

that could be spent investigating issues with no security impact

Susceptibility Analysis focuses on exploitable open source vulnerabilities

- Reduce known vulnerability false positives
- Prevent spending months of effort upgrading a library that has almost zero security benefit
- Save time on investigation of known issues in open source
- Better data / Better decisions

Fortify simplifies application security



SCA
Sonatype Software Composition Analysis
Fortify on Demand

SAST
Fortify Static Code Analyzer
Fortify on Demand

DAST
Fortify WebInspect
Fortify on Demand

RASP
Fortify Application Defender
Fortify on Demand

Fortify Portfolio

Automate testing throughout the CI/CD pipeline, enable developers to quickly resolve issues

- **Static Code Analyzer (SCA):** Analyzes source code for security vulnerabilities (SAST)
- **WebInspect:** Dynamic testing (DAST) analyzes applications in their running state and simulates attacks against an application to find vulnerabilities. Includes IAST agent.
- **Fortify on Demand (FoD):** AppSec as a Service, that includes SAST, DAST, and MAST.
- **Software Security Center:** Holistic application security platform included with on-premises solutions to get complete visibility of application security risks.
- **Sonatype:** Scans open source components for vulnerabilities
- **Application Defender:** Real-time protection & monitoring from attack on running applications (RASP)

	Static (SAST)	Dynamic (DAST)
On Prem	✓ *Static Code Analyzer (SCA)*	✓ *WebInspect*
As a Service	✓ *Fortify on Demand (FoD)*	✓ *Fortify on Demand (FoD)*

Solutions that Align With DevSecOps Success Integration Automation Speed

Backed by the Market Leading Software Security Research Team

1,022 Vulnerability Categories | 27 Programming Languages | 1M+ Individual APIs

Thank You.

MICRO FOCUS®