

Global State of DevSecOps 2024

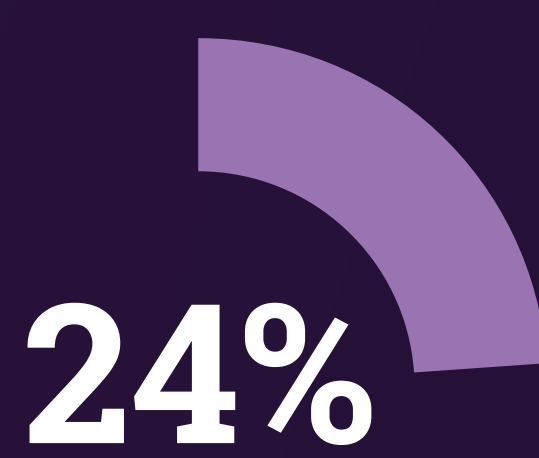
Key takeaways and trends

AI is on the rise in software development but confidence in its security is low



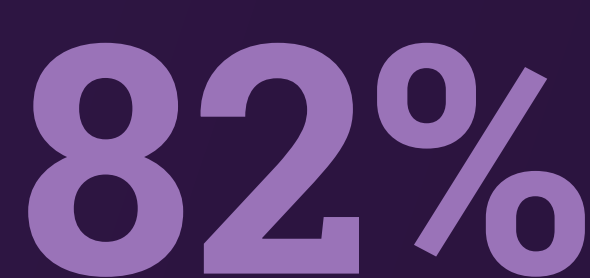
of organizations use AI in software development—

but only



are “very confident” in their testing of it

Too many security tools lead to too much noise



of organizations use between 6 and 20 security testing tools—

but most of them consider



of test results as “noise”

Developer/security tensions remain high despite automation



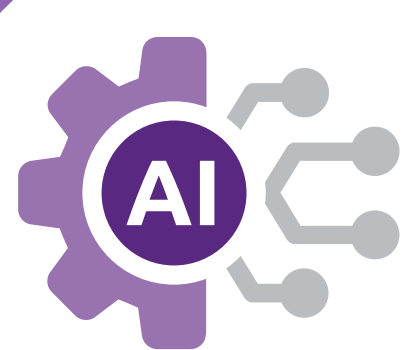
of organizations use automated prioritization for security issues—

and yet



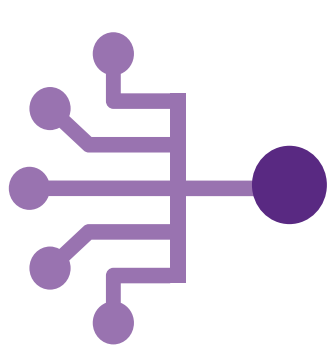
of developers say security testing slows down development

What to do about it



Establish AI governance now

- Create clear policies and procedures for AI use in development
- Invest in tools to vet and secure AI-generated code
- Protect sensitive data by limiting access to AI systems



Scrutinize your tool stack

- Aim for consolidation and results integration
- Reduce tool proliferation and complexity
- Implement application security posture management



Evaluate your automation levels

- Integrate automated security checks into your CI/CD pipeline
- Implement infrastructure-as-code with built-in security policies
- Provide developer IDE plugins for real-time security feedback and prioritized remediation guidance

Download the [full report](#) to learn more.