Extending DevSecOps Security Controls into the Cloud:

A SANS Survey

Today's Speaker

- Eric Johnson
  - Senior SANS instructor and co-author of SANS courses SEC540, 510, and 584
  - Principal Security Engineer, Puma Security

Attend the Panel Discussion

Extending DevSecOps Security Controls into the Cloud: A Panel Discussion of the 2020 SANS Survey

Wednesday, November 4, 2020
1 PM Eastern Time

https://www.sans.org/webcasts/114630

Today's Agenda

1. Cloud & DevSecOps Landscape
2. Shift Left Analysis
3. Shift Right Analysis
4. Moving Forward

1. Cloud & DevOps Landscape

Increasing Velocity

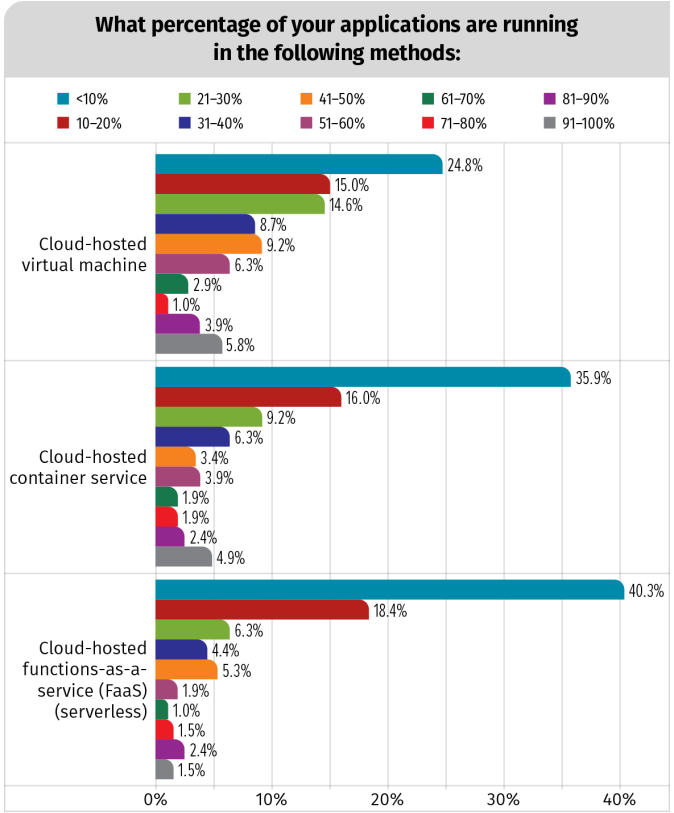
Year-over-year comparison of how often changes are deployed to production systems:

- 74% of organizations are delivering changes to production more than once per month.
- 14% increase in velocity during the past 4 years

Frequency of Delivery to Production	2017	2018	2020
Continuously (several times per day)	5.3%	10.0%	**11.1%**
Daily	12.0%	7.0%	**12.1%**
Weekly	25.4%	24.0%	**31.4%**
More than once per month	17.7%	25.0%	**19.8%**
Monthly	18.7%	15.0%	11.1%
Quarterly	13.4%	11.0%	6.3%
More than once per year	3.8%	4.0%	3.9%
Annually	1.9%	1.0%	1.0%
Other (ad hoc/more than once per year)	1.9%	3.0%	3.9%

Increasing Cloud Adoption

Delivery increases as systems transition to the cloud provider's responsibility model.



Multiple Cloud Providers

Most organizations (92%) use at least one public cloud provider, with slightly more than 60% using three or more public cloud providers. Why?

- Corporate mergers & acquisitions
- Select the best platform/service available
- Avoid cloud vendor lock-in

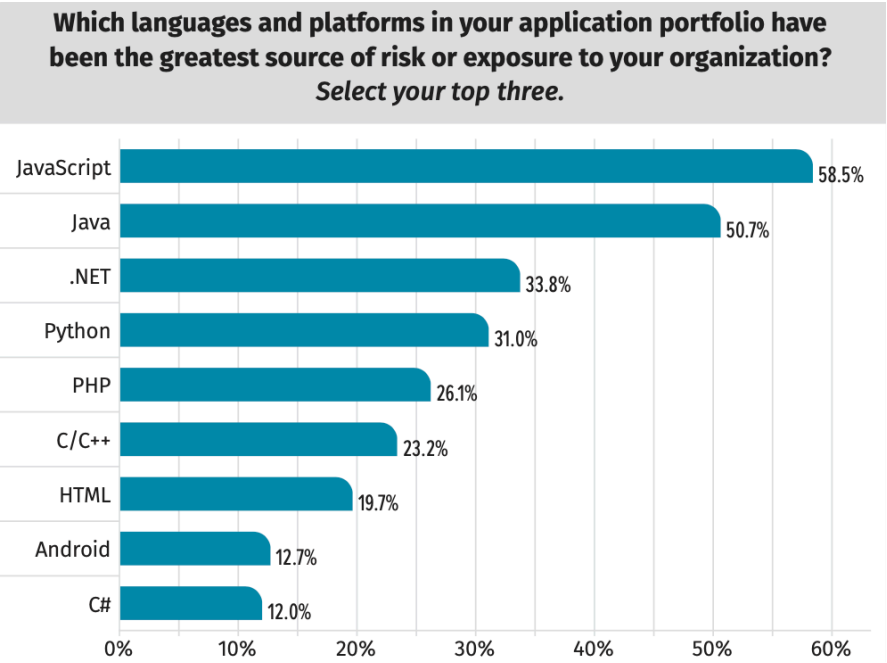
SECURITY IMPACT

MULTIPLE CLOUD PLATFORMS COMPOUNDS SECURITY RISKS

Increasing Platform Risks

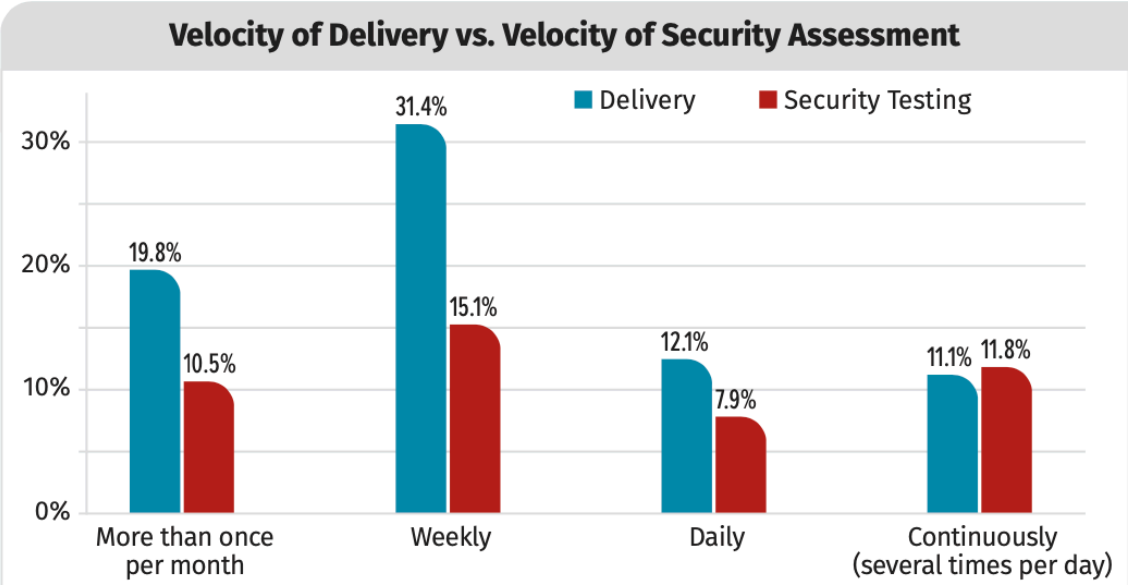
Development programming languages present risk to application security teams:

- JavaScript leaps into the top position as cloud & microservice adoption increases.
- Java, .NET, C++ continue to remain high-risk due to legacy usage.



Security vs. Delivery

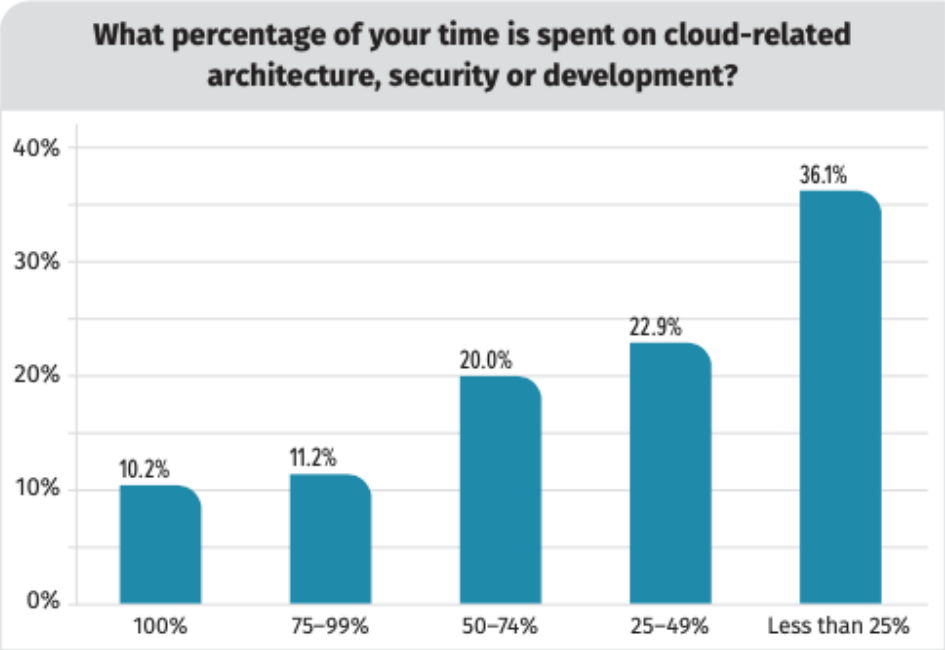
27% of organizations do not perform security assessments at all.



Security vs. the Cloud

Are security teams shifting right and learning how to harden public cloud?

- Operations
- Monitoring
- Runtime security controls



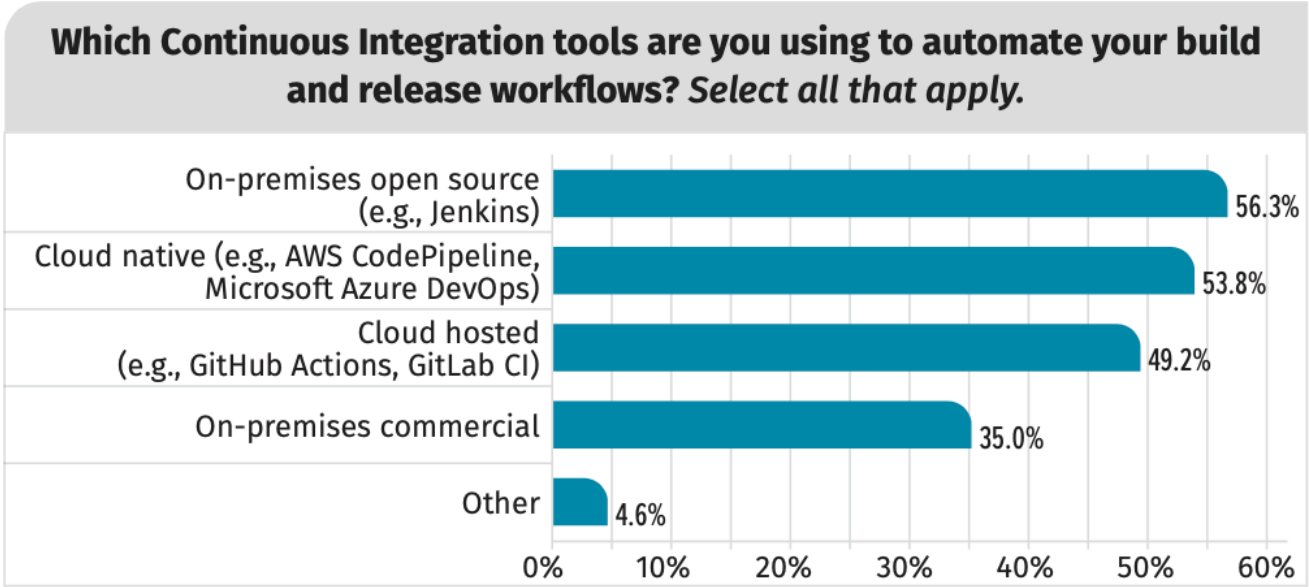
2. Shift Left Analysis

Top 5 Shift Left Controls

- Risk Assessments & Threat Modeling
- Developer Security Training
- Manual Code Review
- Security Stories
- Dependency/Supply Chain Analysis

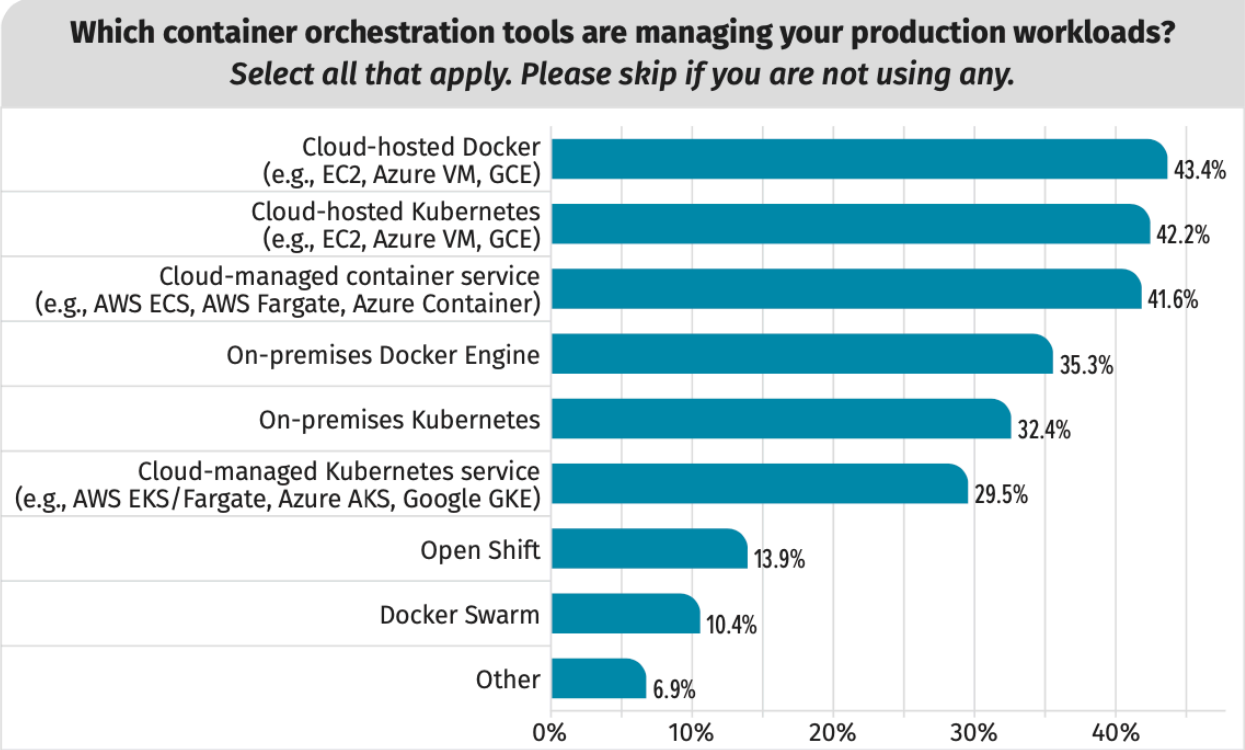
Continuous Integration Tools

Organizations are shifting to cloud native & cloud hosted Continuous Integration (CI) solutions:



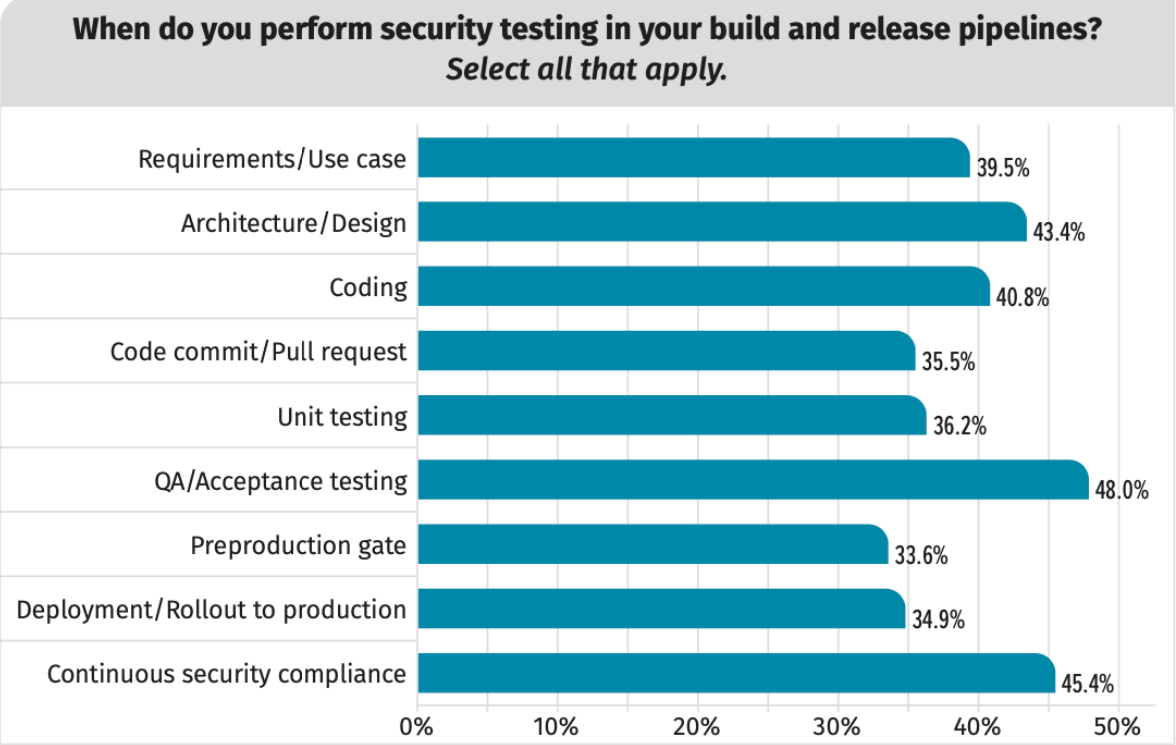
Container Orchestration Tools

- Organizations are avoiding the complexity and overhead involved with installing, managing and hardening Docker and Kubernetes services.



Security Testing Phases

- Less than 40% of organizations shift security reviews into upfront requirements & design.



3. Shift Right Analysis

Top 5 Shift Right Controls

- Configuration Security Monitoring
- Vulnerability Scanning
- Container Image Scanning
- Web Application Firewalls (WAF)/Next Gen WAF
- Network Detection & Response/Network Traffic Analysis

Security Testing Responsibility

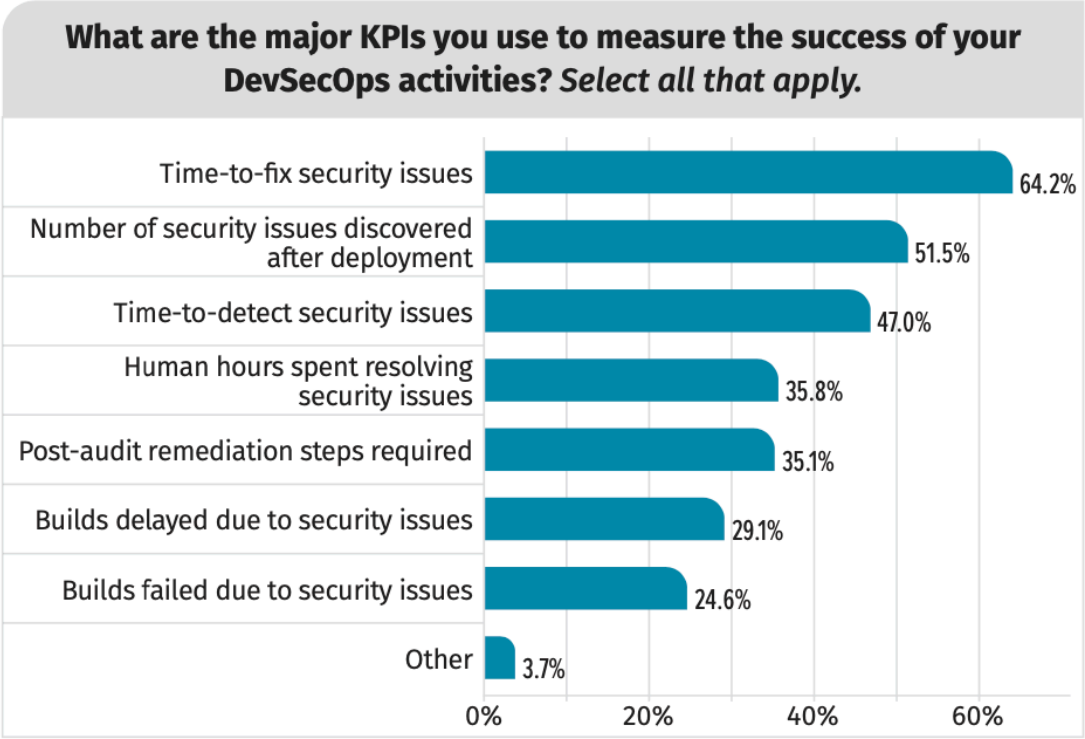
- Security teams (internal & external) still conduct most testing.
- Security testing cannot scale at the velocity of DevOps.
- Development and cross-functional teams must contribute more.

Role	Managing	Conducting	Accepting	Corrective Actions
Business unit owner	39.3%	12.6%	52.6%	26.8%
Commercial application vendors	17.4%	23.4%	19.4%	33.3%
Cross-functional teams in DevOps or DevSecOps	28.8%	38.1%	29.4%	39.2%
Development team	28.8%	38.1%	36.8%	63.3%
External security consultants	8.5%	42.8%	13.2%	9.2%
Internal security team	50.1%	65.4%	34.1%	22.6%
Quality assurance	17.9%	33.4%	28.8%	18.1%
Security architect	42.1%	38.8%	28.8%	24.1%

Measuring Program Success

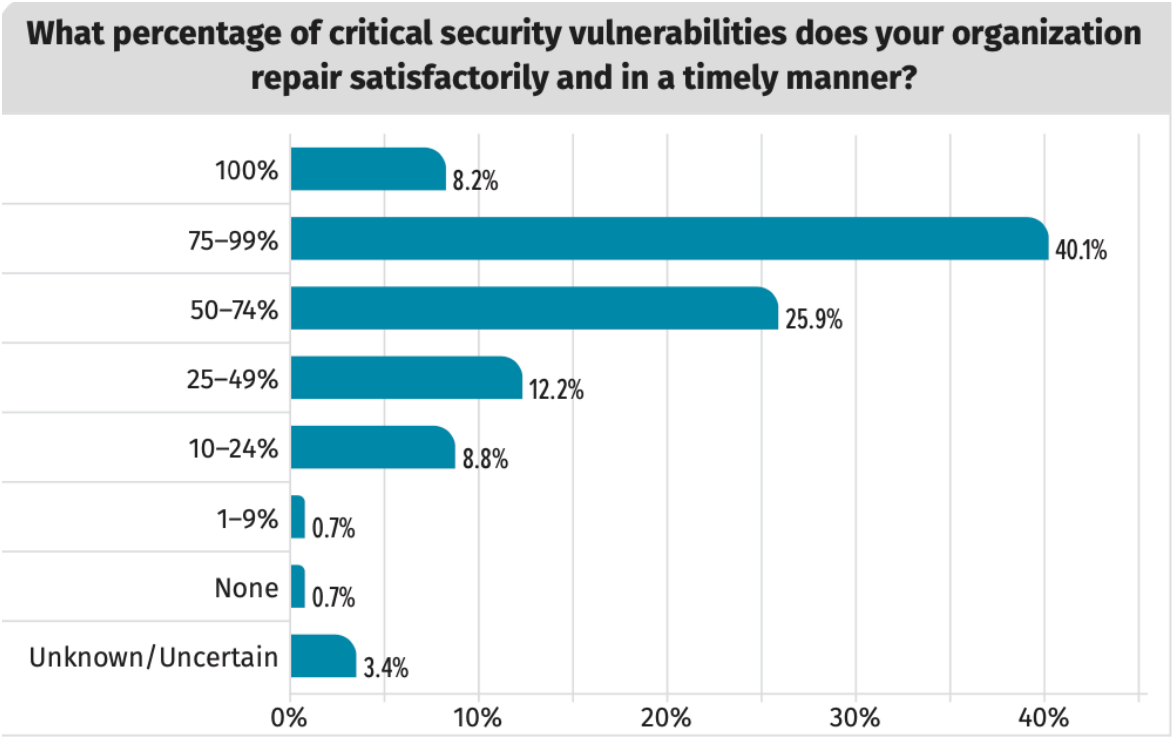
Top DevSecOps Key Performance Indicators:

- Time-to-fix
- Security issues found after deployment
- Time-to-detect



Mean Time To Recover (MTTR)

- Less than half of organizations are repairing critical vulnerabilities satisfactorily and in a timely manner.

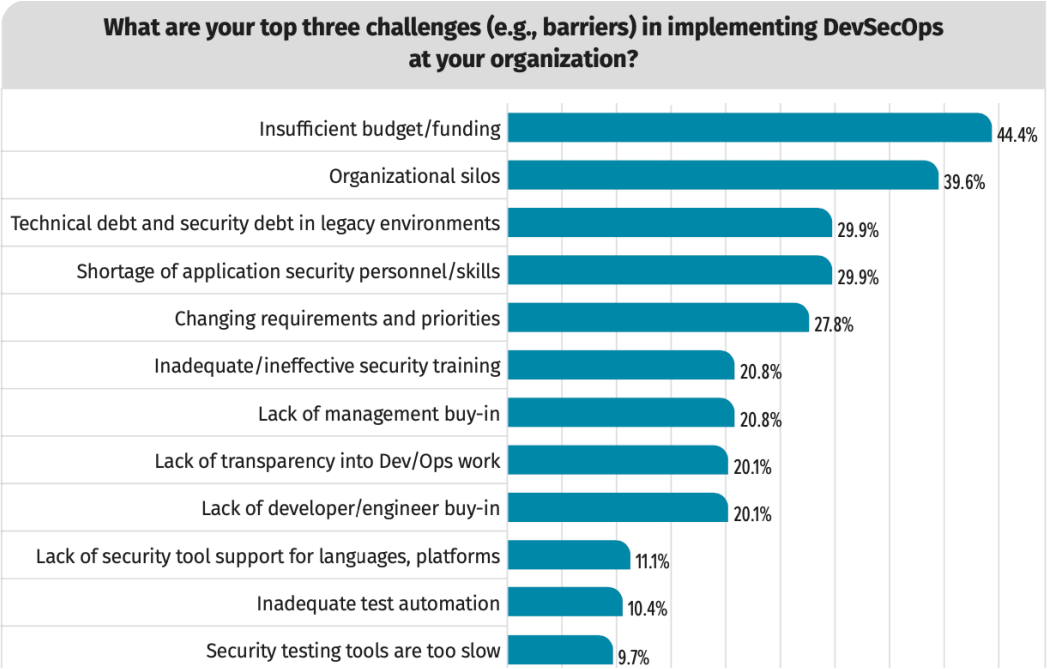


4. Moving Forward

Organizational Challenges

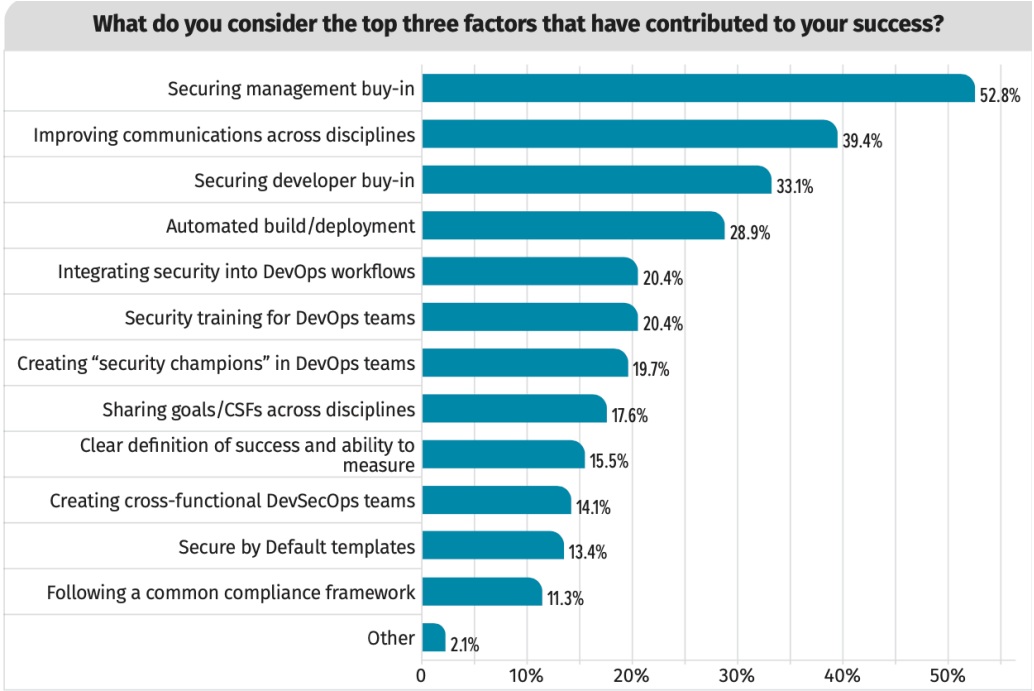
Major challenges are fundamentally organizational:

- Insufficient budget
- Shortage of security skills and security training
- Organizational silos
- Lack of buy-in from management and development teams



Top Success Factors

- Securing buy-in from managers and developers
- Improving communications across disciplines
- Moving into the cloud can help organizations become more agile and secure.



Conclusions

Shift right in order to improve success shifting left:

Automation & Tooling

Create a control plane for enforcing security and compliance.

Help security and compliance move at the speed of DevOps.

Cloud Platforms

Test Coverage

Collect attack data to identify real risks that need to be defended.

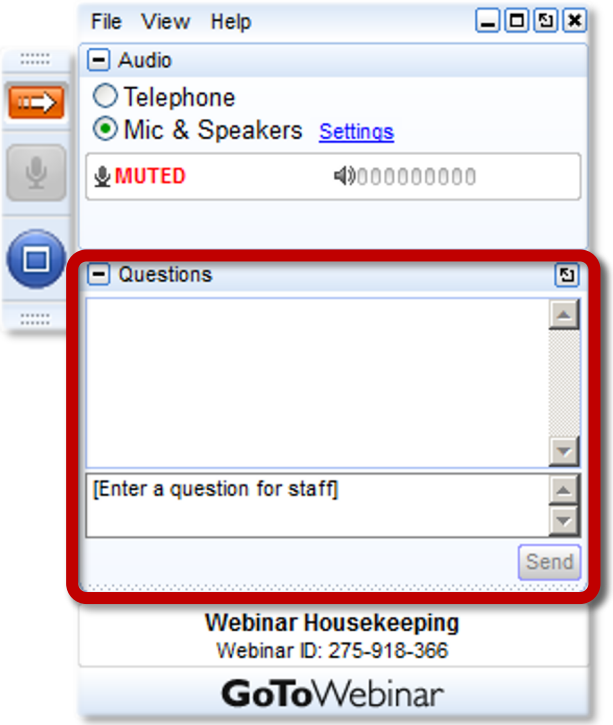
Understand gaps in testing and controls, and shift left to improve process design and tooling.

Production Weaknesses

Q&A

Please use **GoTo**Webinar's Questions tool to submit questions to our panel.

Send to "Organizers" and tell us if it's for a specific panelist.



Acknowledgments

Thanks to our sponsors:

And to our attendees, thank you for joining us today!