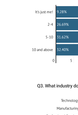
logz.io

The 2018 DevOps Pulse

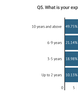
Full Report

Q1. What is your role in the company?

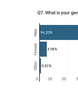


Q2. What is the size of your team?

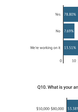
Q3. What industry does your company belong to?



Q4. What is the size of your company?

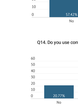


Q5. What is your experience level?

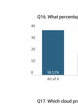


Q6. Where in the world do you work?

Q7. What is your gender? (Optional)



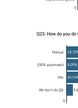
Q8. Do you feel your company has fair opportunities for all genders?



Q9. Do you consider your work environment/culture to be diverse?

Q10. What is your annual salary?

Q11. What is the size of your infrastructure? (number of servers/instances)



Q12. What architecture are you using to build your application?

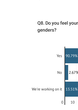
Q13. Are you using serverless in your application logic?

Q14. Do you use containers?

Q15. Do you use container orchestration services, and if so, which?

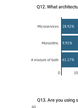
Q16. What percentage of your infrastructure is based in the public cloud?

Q17. Which cloud provider are you using? (check all that apply)

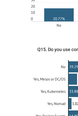


Q18. Does your company rely on open source technology, and if so, how heavily?

Q19. Does your company contribute to open source?

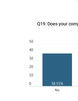


Q20. How frequently does your team deploy code into production?



Q21. Do you have a continuous integration (CI) strategy in place?

Q22. Do you have a continuous deployment (CD) strategy in place?



Q23. How do you do QA in your organization?

Q24. Which metric monitoring tools do you use? (check all that apply)

Q25. What's your most common use case for log analytics? (check all that apply)

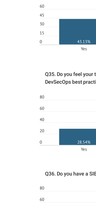
Q26. How do you distribute alerts in your organization?

Q27. How long does it take your team to identify and troubleshoot a production issue?

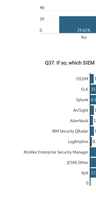
Q28. Who implements security and handles security incidents in your organization?

Q29. Do you have a team of security analysts?

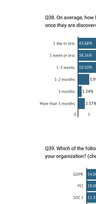
Q30. Do you have difficulty finding qualified talent to fill roles on the security analyst team?



Q31. If so, which factors contribute to the security skills gap in your organization? (check all that apply)



Q32. Does your organization practice DevSecOps?



Q33. Does your organization use any of the following DevSecOps strategies? (check all that apply)

Q34. Do you feel there are enough tools available to successfully implement DevSecOps?

Q35. Do you feel your team has adequate knowledge of DevSecOps best practices?

Q36. Do you have a SIEM system in place?

Q37. If so, which SIEM system do you use?

Q38. On average, how long does it take to resolve a security incidents once they are discovered?

Q39. Which of the following compliance certifications are important to your organization? (check all that apply)

Q40. Are you GDPR-ready?

Q41. On a scale of 1-5, how worried is your organization about a potential attack or breach? (one being not worried, and five being extremely worried)

Q42. Which types of attacks do you feel most concerned about?

Q43. How confident do you feel in your / your teamates ability recover from a security exploit?

Q44. What would help you / your team feel more confident responding to security issues? (check all that apply)

Conclusion

DevOps teams are still struggling to bring security into the mix. The majority of DevOps professionals report that they are not practicing DevSecOps and that there is a lack of knowledge and tools to help in this area.

We believe this will change in the near future.

To facilitate this, these organizations will be able to make use of a growing number of DevSecOps best practices, as well as specified tooling. Automated security, code dependency scanning, threat assessments and developer training are just some of the methodologies that we expect to see increasingly in practice by the end of 2018.

logz.io