Secure DevOps and Misconfigurations

cloud security alliance®

Acknowledgments

Author:

Hillary Baron

Contributors:

Frank Guanco
Sean Heide
Alex Kaluza
Shamun Mahmud
John Yeoh

Designers:

Claire Lehnert
AnnMarie Ulskey

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Table of Contents

Survey Creation And Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA is also tasked with educating various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys help gauge the maturity of information security technology at various points in the industry, as well as the rate of adoption of security best practices.

Trend Micro commissioned CSA to develop a survey to add to the industry's knowledge about secure DevOps and misconfigurations and to prepare this report of the survey's findings. Trend Micro financed the project and co-developed the initiative by participating with CSA in the development of survey questions addressing secure DevOps. The survey was conducted online by CSA from July 2021 to September 2021 and received over 900 responses from IT and security professionals from a variety of organization sizes and locations. The data analysis was performed by CSA's research team.

Goals of the study

The goal of this study was to better understand the current state of DevSecOps in a variety of areas. Key areas of interest include:

- Public cloud workloads now and in the future
- Cloud security challenges and misconfigurations enterprises face
- Enterprises journey toward implementing DevSecOps approach
- Training and education methods for improving cloud security

Executive Summary

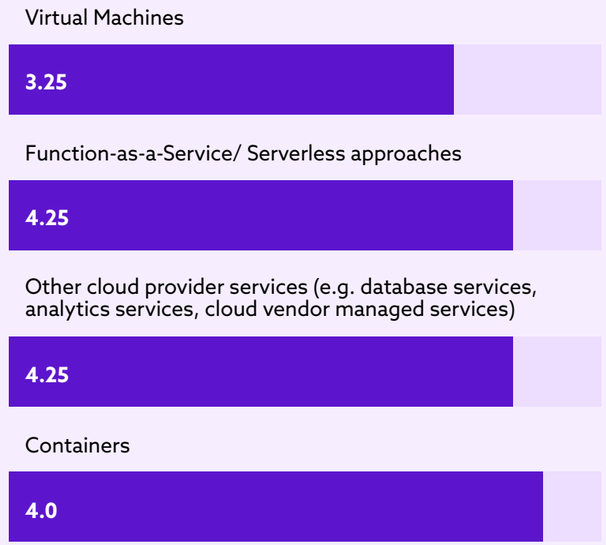
Secure DevOps, DevSecOps, and "shifting left" have become increasingly popular terms in cybersecurity. With the rapid increase both in volume and speed to delivery of applications, attacks on applications have also increased in both volume and complexity. Combine this with the shortage of cybersecurity professionals and lacking security skillsets, cybersecurity teams are already stretched to their limits. This has given rise to a DevSecOps approach, however, DevSecOps isn't a silver bullet, organizations still face misconfigurations and other security challenges, struggle with implementing DevSecOps approach, and insufficient security skillsets

Key Finding 1

Movement toward a DevSecOps approach

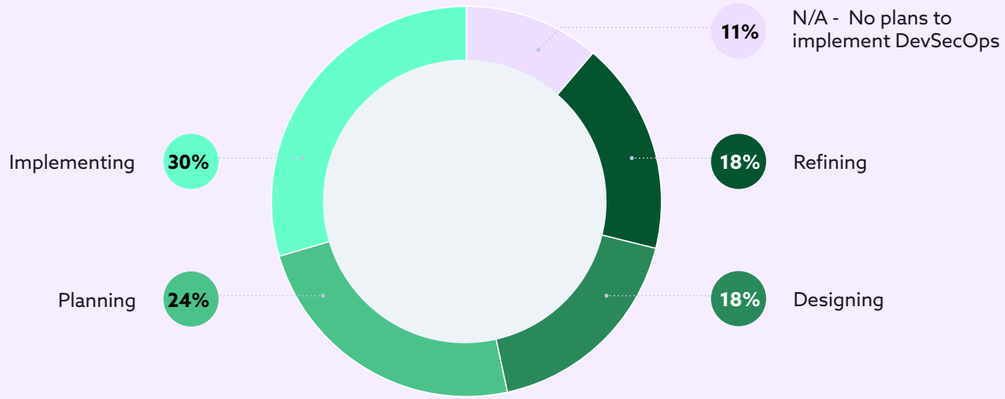
There are clear indications that organizations are moving toward a DevSecOps approach. The first indication is the increase in the variety of cloud workloads including containers and serverless that is expected over the next year. The increased use of these types of workloads indicates that there is a trend toward DevSecOps.

Predicted changes to the type of workloads used in public cloud over the next 12 months



The second indication is that nearly 90% of organizations are in some phase of the journey toward DevSecOps. Just under half of the organizations are either implementing or refining their DevSecOps approach. Of those who haven't yet reached the implementation phase, 48% expect to reach the implementation phase within a year. All of these indicate an explicit trend toward the use of a DevSecOps approach.

Current phase in DevSecOps implementation journey

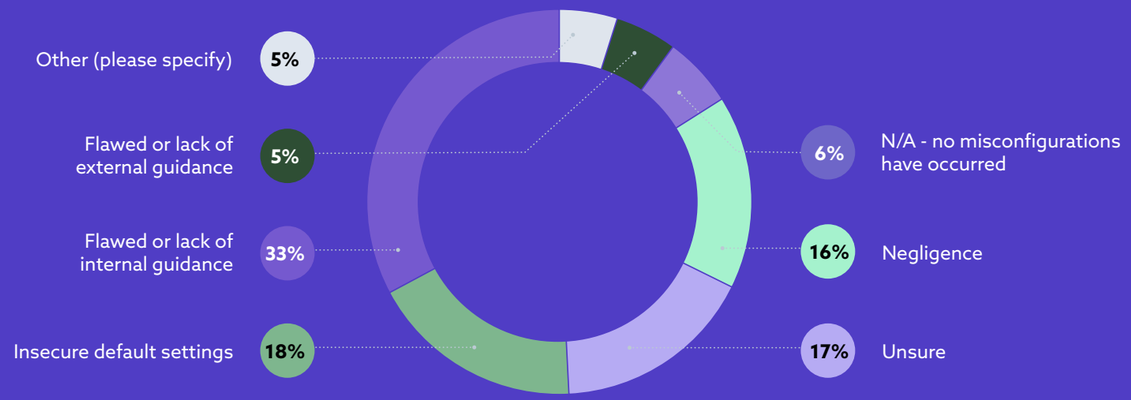


Key Finding 2

A third of misconfigurations blamed on flawed or lack or internal guidance

Although there is a movement toward DevSecOps, misconfigurations still occur. On average, organizations are moderately confident in their ability to defend against misconfigurations. This is encouraging, but still leaves room for improvement. The primary reason cited for these misconfigurations was flawed or lacking internal guidance (33%). This indicates that the guidance organizations are developing internally is ineffective for preventing misconfigurations. The use of other guidance such as industry frameworks could help organizations deal with this issue.

Primary cause of misconfigurations in organizations



Key Finding 3

Organizations are struggling with IAM and PAM

Despite misconfigurations repeatedly being rated as a top concern year after year, organizations are moderately confident with their ability to defend against them. What organizations are least confident about are issues of privilege access management and identity, authorization, and access challenges. In a previous survey, privilege and permission management was rated as a top IAM security challenge for organizations. This could speak to the complexity of implementing native cloud service provider solutions, third-party solutions, in-house solutions, or some combination. All often require a multi-year effort from organizations to properly implement.

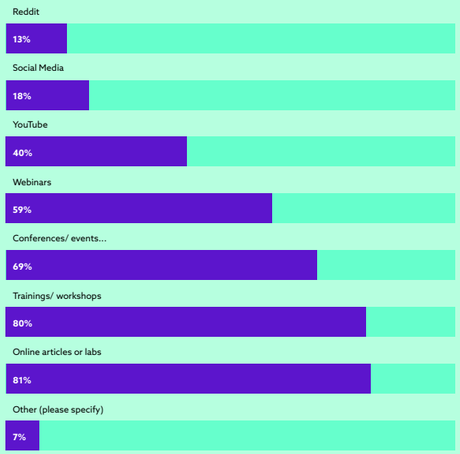
Items ranked by confidence to defend against them

Key Finding 4

Online articles and training are the top ways security professionals learn more about cloud security, tools, and vendors.

Cloud security is a fast moving industry with a shortage of experts. Keeping up with the latest best practices and trends often requires security professionals to seek out knowledge. The most common method to learn more about cloud security, tools, and vendors was through online articles or labs (81%) and training or workshops (80%). Conferences or industry events were also common (69%). Social media and entertainment platforms are used much less frequently despite their overall popularity. This indicates that security professionals still have a preference for traditional methods of learning.

Resources used to learn more about cloud security, tools, and vendors

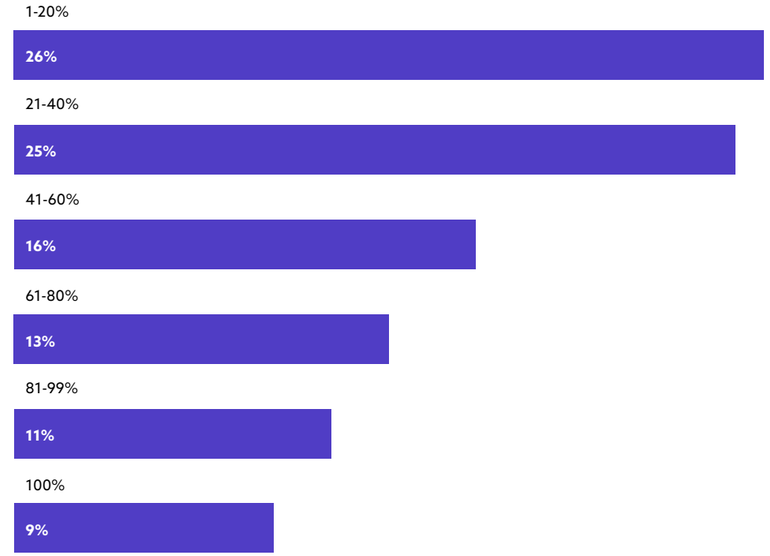


Public Cloud Workloads

Current cloud workloads

At the time of the survey, 51% of organizations were running 40% or less of their workloads in the cloud. Approximately 40% of organizations have between 41-99% of their workloads in the public cloud. This leaves 9% which have 100% of their workloads in the public cloud.

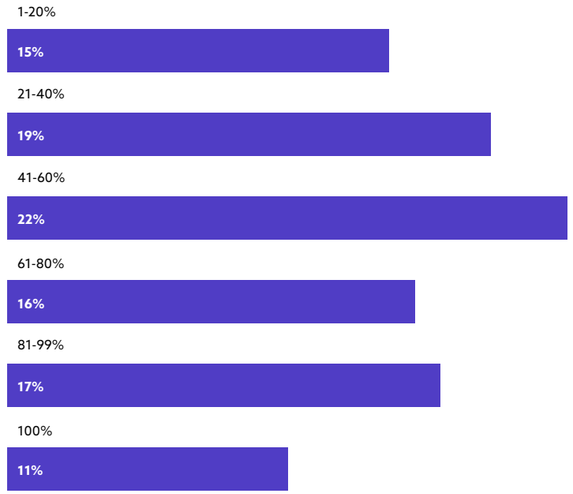
Percentages of workloads run in the public cloud



Future cloud workloads

There is a notable shift expected with more workloads in the public cloud. Approximately 55% of organizations will have between 41-99% of their workloads in the public cloud, up from 40% of organizations.

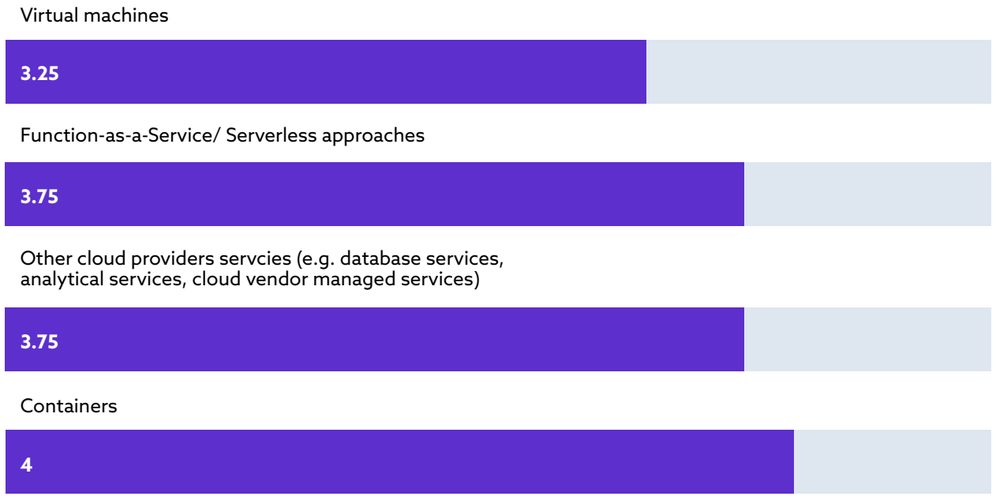
Percentage of workloads in the public cloud in 12 months



Changes in workload types

Over the next 12 months, respondents expect the following to increase in the use of container platforms, function-as-a-service/serverless approach, and cloud provider services. The use of VMs is also expected to remain about the same. A similar trend was found in a previous survey1, indicating this is a trend that can be expected year-over-year.

Predicted changes to the type of workloads used in public cloud over the next 12 months



Security Challenges

Important frameworks

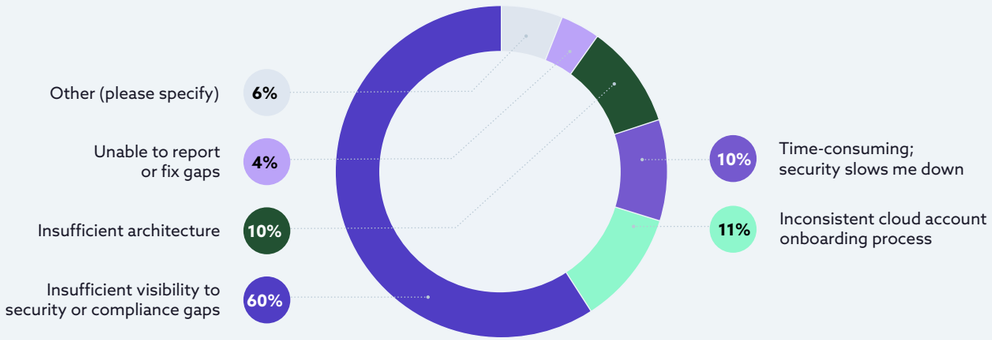
The most important frameworks for organizations is the National Institute of Standards and Technology's Cybersecurity Framework (78%), followed by CIS Security Foundations Benchmarks (67%) and CSA's Cloud Controls Matrix (66%). Many organizations find multiple frameworks important to their security strategy.

Important frameworks for organizations

Top challenges for maintaining security and compliance

Insufficient visibility to security or compliance gaps is the top challenge for security professionals by a significant margin (60%). Visibility is an issue that has plagued security professionals for many years and is not easily solved.

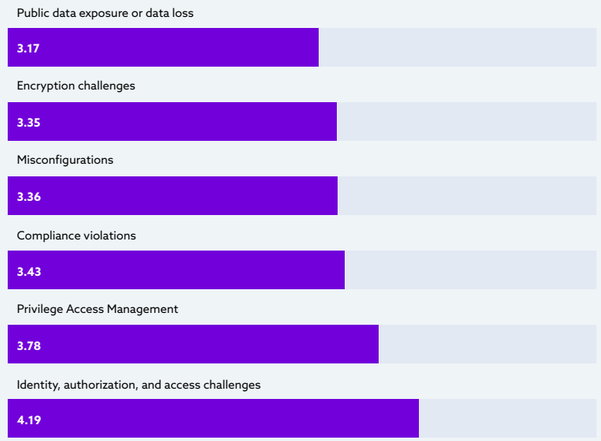
Top challenge when maintaining cloud security best practices and compliance



Confidence to defend the organization

Organizations are least confident about issues of privilege access management and identity, authorization, and access challenges. In a previous survey, privilege and permission management was rated as a top IAM security challenge for organizations[1]. This could speak to the complexity of implementing native cloud service provider solutions, third-party solutions, in-house solutions, or some combination. All often require a multi-year effort from organizations to properly implement.

Items ranked by confidence to defend against them



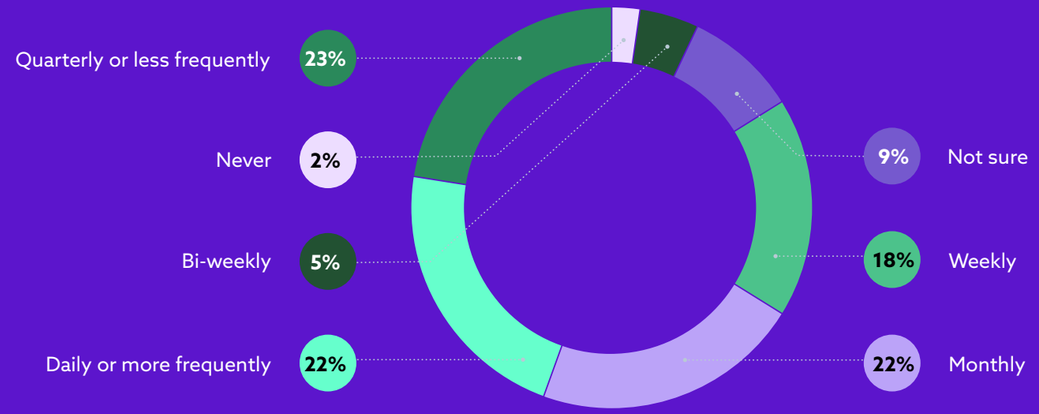
[1] *The 2020 State of Identity Security in the Cloud.* CSA (2020).

Misconfigurations

Review cloud infrastructure vulnerabilities and/ or misconfigurations

Among organizations, there is no clear pattern with regard to the frequency of reviewing cloud infrastructure for vulnerabilities or misconfigurations

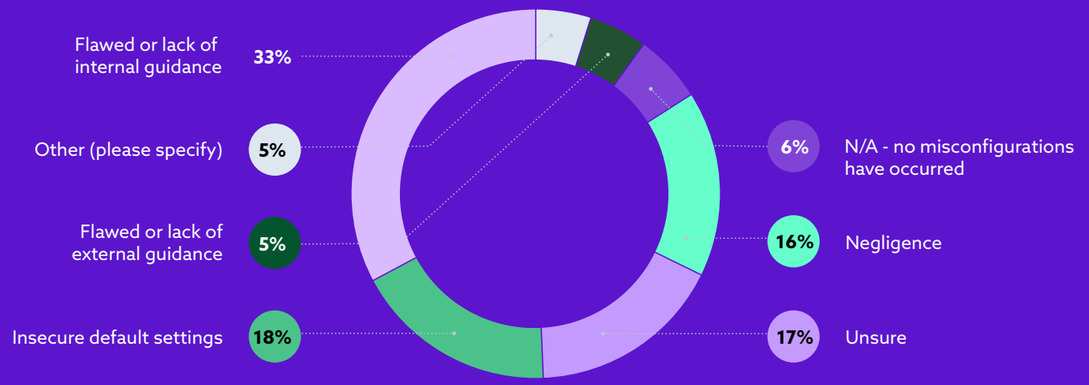
Frequency of reviewing cloud infrastructure for vulnerabilities and/ or misconfigurations



The primary cause of misconfigurations

Flawed or lack of internal guidance is the most common contributor to misconfigurations. This indicates that attempting to develop materials internally can benefit from outside resources or guidance.

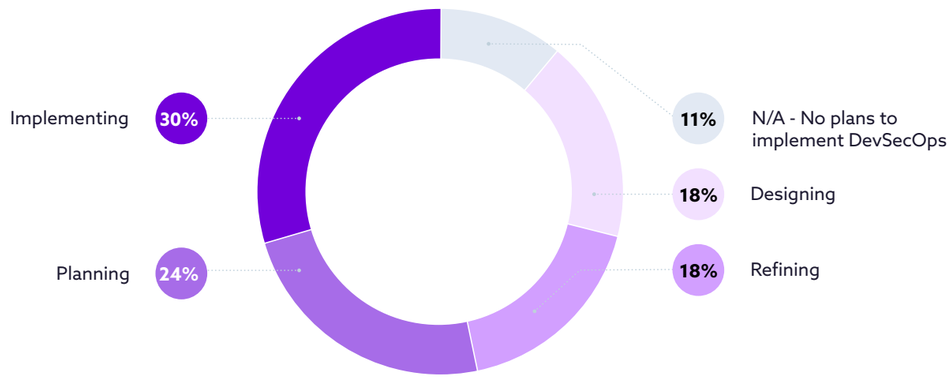
Primary cause of misconfigurations in organizations



DevSecOps

Stage of DevSecOps journey

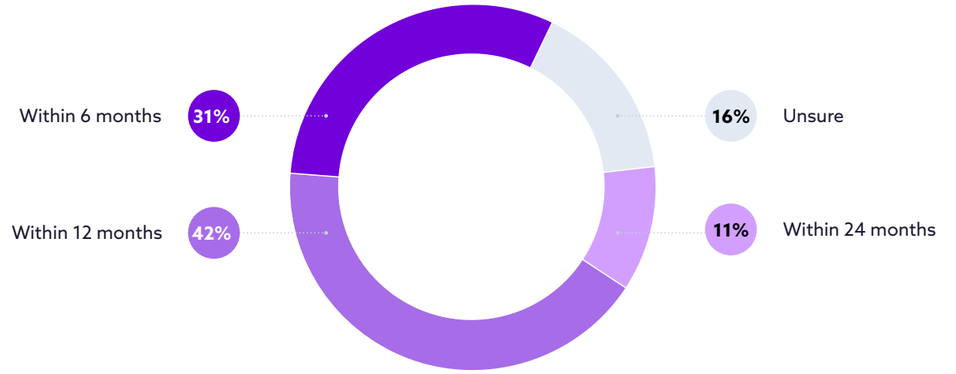
Most organizations are already in the process of implementing DevSecOps in their organization. Nearly half are already implementing or refining their approach. Only 11% of organizations don't plan to implement DevSecOps.



Timeline to reach the implementation phase

Of the organizations that haven't reached the implementation stage of their DevSecOps journey, 73% expect to reach this phase in one year's time.

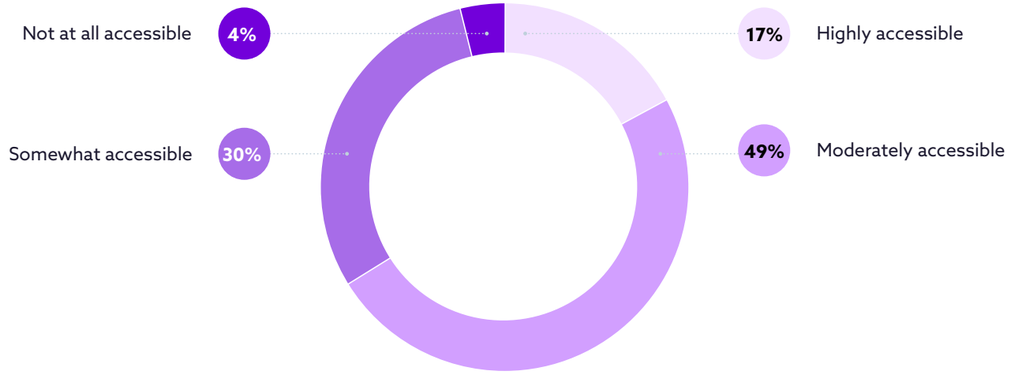
Predicted timeline for reaching implementation phase in DevSecOps journey



Accessibility of DevSecOps implementation resources

Security professionals find that overall DevSecOps best practices resources are moderately or highly accessible. Still about a third of security professionals are struggling to find resources.

Accessibility of resources for DevSecOps best practices

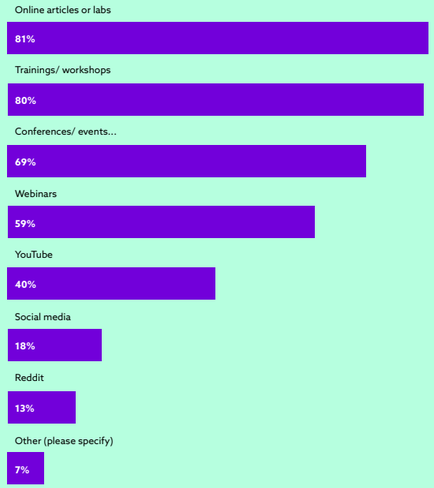


Training and Education

Finding resources to learn about cloud security, tools, and vendors

Security professionals still prefer traditional methods for learning about cloud security, tools, and vendors using social media and entertainment sites such as YouTube and Reddit to a much lesser extent.

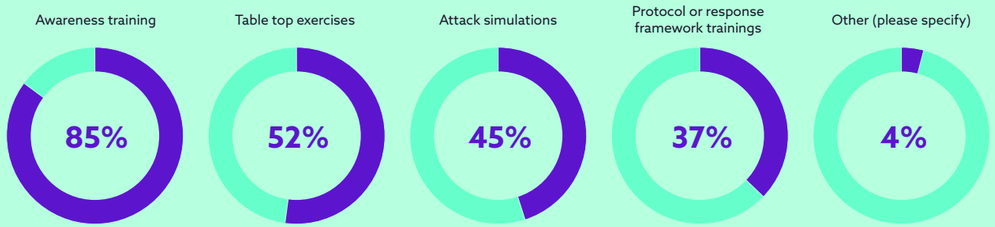
Resources used to learn more about cloud security, tools, and vendors



Methods of training to an event response or crisis incident

Organizations use a variety of methods to address crisis incidents and event responses. The most commonly used strategy is awareness training (85%) followed by tabletop exercises (52%), then attack simulations (45%), and finally protocol or response training (37%)

Methods for addressing crisis incident education



About the Sponsor

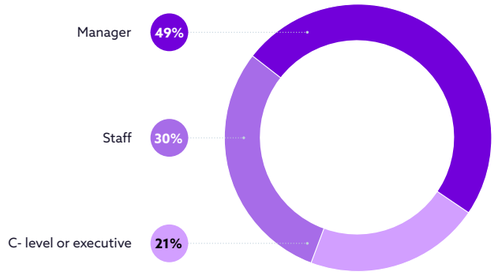
With over two decades of expertise in Endpoint, Messaging and Web Security, Trend Micro provides individuals, and organizations of all sizes, with smarter security solutions that protect against a wide range of insidious threats and combined attacks including viruses, spam, phishing, spyware, botnets and other Web threats, such as data-stealing malware. Trend Micro develops, delivers, and supports proactive cloud-based solutions designed to safeguard critical information and protect personal and corporate reputations. As an industry leader in security intelligence, Trend Micro's mission is to secure the exchange of digital information by providing the most flexible and customizable Internet Content Security solutions available.

TREND MICRO™

Sponsors are CSA Corporate Members who support the findings of the research project but have no added influence on the content development or editing rights of CSA research.

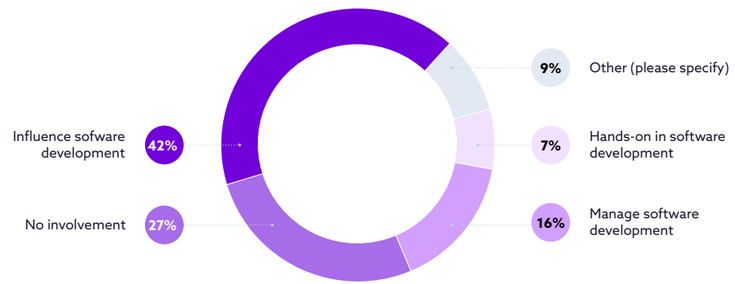
Demographics

This survey was conducted from July 2021 to September 2021and gathered over 900 responses from IT and security professionals from a variety of organization sizes, industries, locations, and roles.

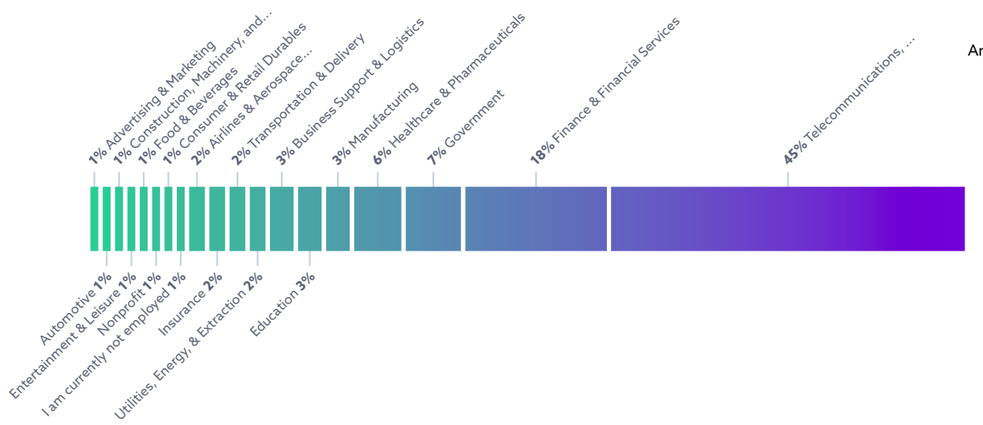


Which of these best describes your current job level?

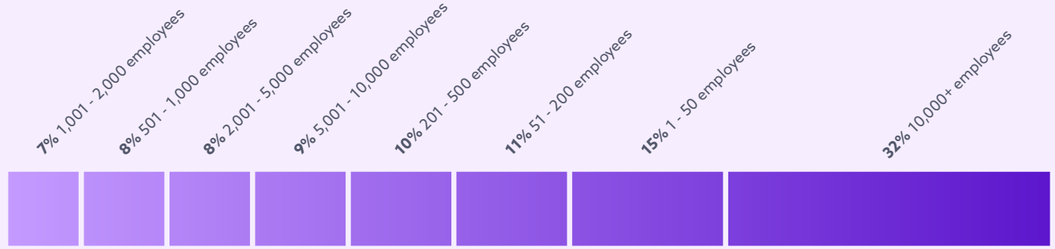
What is your usual role when it comes to software development within your organization?



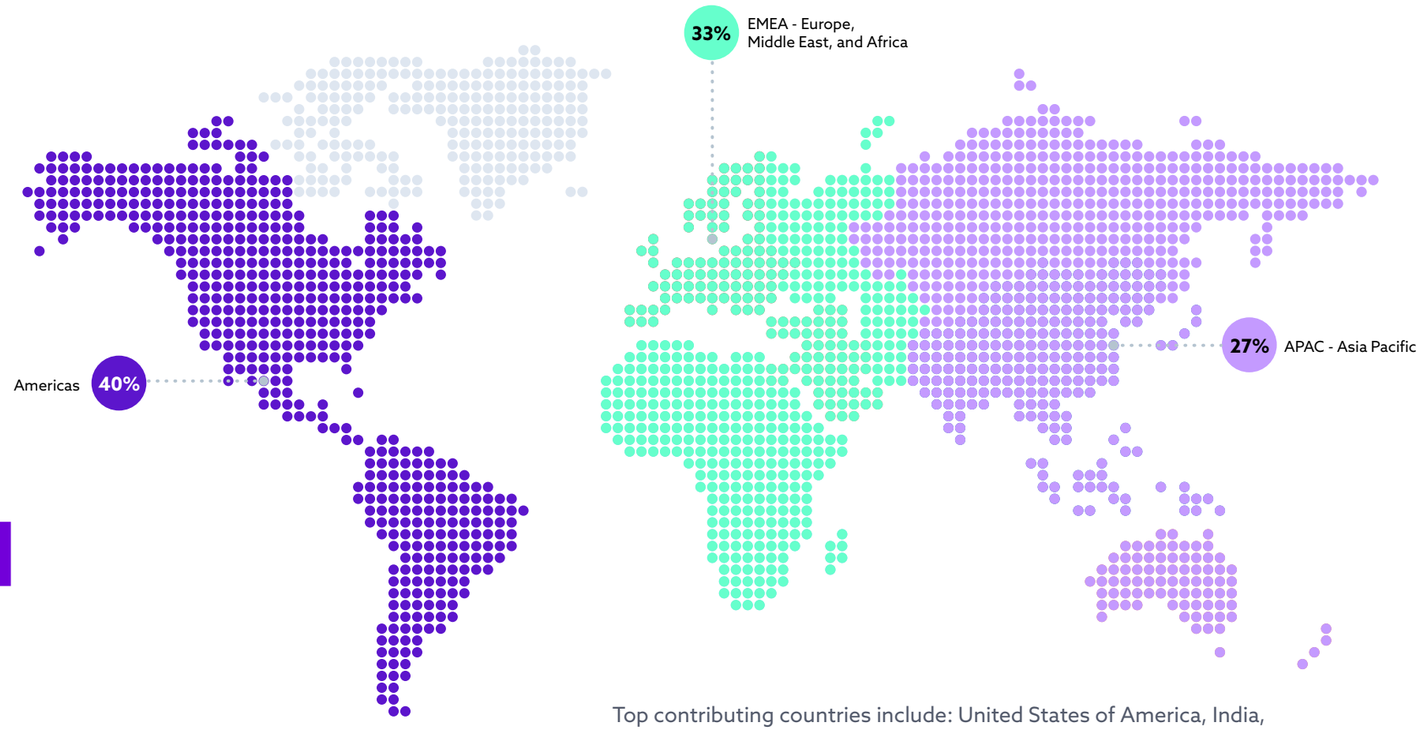
Which of the following best describes the principal industry of your organization?



What is the size of your organization?



What region of the world are you located?



Top contributing countries include: United States of America, India, United Kingdom, Singapore, Australia, Netherlands, Spain, Germany, Italy