ARMO

The State of Kubernetes Open Source Security

October 2022

Table of Contents

Introduction and Key Findings

Introduction & Methodology

Open source software — where the original source code is made available for public use and can be modified and redistributed at will — is becoming increasingly popular across many different areas of business. Developers are reaping the benefits of transparency and visibility into the code that they use, and the ability to contribute and be part of the code's evolution, too.

Kubernetes, also known as K8s, is an open-source system for automating the deployment, scaling and management of containerized applications. It is now ubiquitous for cloud-native environments, becoming a de facto standard for organizations who work on the cloud. According to CNCF research, 96% of organizations are either using or evaluating Kubernetes, more than at any other time since they began collecting data in 2016. As an increasing number of organizations move to Kubernetes, this also means that more and more attackers are making it their target.

With this survey, our goal is to understand how these two trends, increased open-source adoption in general and increased use of Kubernetes in specific, work in tandem. How are companies using open source tools to secure their Kubernetes environments?

Today's DevOps teams are forced to make a difficult choice between two realities. They can attempt to integrate several fragmented open-source tools together, which adds complexity to the monitoring and management of the Kubernetes environment, and requires a significant effort in order to get a single view. Alternatively, they can commit to a proprietary solution that they can't adapt, and where they can't access the code, influence the roadmap or contribute to its future. We asked respondents how they manage the relationship between these two approaches, and what challenges are they facing as a result.

Methodology

To get a deeper understanding of the relationship between open source and K8S security, we commissioned a survey of 200 Kubernetes users in companies that ranged in size from under 100 employees to more than 5,000. The survey was completed by Global Surveyz, an independent survey company, and took place during July and August 2022.

The survey respondents are software developers and stakeholders from cybersecurity teams, DevOps and DevSecOps, 57% from North America, 29% in Europe, and 14% in APAC. The respondents were recruited through a global B2B research panel, and invited via email to complete the survey. The average amount of time spent on the survey was 6 minutes and 49 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key Findings

1 **Over half of companies are using open source for Kubernetes security**

55% of respondents are using open source for K8S security, either as a standalone solution or in a hybrid set up alongside a proprietary solution. Open source is used widely across all areas of security, especially for service meshes where thanks to CNCF-led projects, more oversight and support is available.

2 **Almost a quarter are using 5 or more open source tools**

Respondents highlighted the main challenge for proprietary solutions as a lack of oversight, visibility and control – calling these tools a "black box." Because of these limitations, many turn to open source solutions. However, respondents are forced to onboard multiple open source tools, as no one solution provides it all. On average, companies are using 3.6 open source tools for K8S security, while just 17% are using a single open source tool.

3 **Integration challenges are a major inhibitor of open source technology**

As well as the challenge of handling multiple tools, open source has additional challenges – especially with integration. 62% say that open source is difficult to integrate with other DevOps tools, and 69% admit it's difficult or very difficult to integrate with their existing K8S stack. These problems are exacerbated by the fact that open source by nature usually has limited support and guidance.

4 DevSecOps owns K8S security. But who are they, really?

The majority of respondents agree that K8S security belongs with DevSecOps, but this raises another question – where does DevSecOps live within the org? When we break down responses by role, the majority of Security teams believe they should hold responsibility, while DevOps believe DevSecOps is their own domain. As K8S security matures, the market will need to gain greater clarity around ownership.

5 Scanning and fixing misconfigurations: Perception vs reality

Most organizations have good practices in place when it comes to scanning and fixing misconfigurations and vulnerabilities in K8S. For example, 95% are scanning at least weekly. However, VP/C-level executives appear to have a somewhat skewed perception, with 38% believing scans are completed every few hours, compared to under 20% when more hands-on members of the team voiced their thoughts.

6 Top K8S security challenges center around integration

The top challenges for companies with K8S security can all be tied back to issues with integration. For example, 68% of teams are facing too many alerts which is a common problem when you have more tools than you need, while 62% directly call out fragmented solutions as a top issue in their K8S security. The third challenge is that security is interfering with the business' agility and time to market, suggesting it isn't integrated at early stages, but rather inhibiting progress later in the DevOps lifecycle.

Survey Report Findings

K8S Security – Usage of Open Source vs. Commercial

Over half (55%) of companies are using open source for their Kubernetes security, either alone or to complement their proprietary solution. When looking at regional breakdowns, Europe is adopting open source as a standalone solution in greater numbers than APAC and North America.

It's clear that companies are attempting to have it all, recognizing that they may need commercial solutions for the benefits they offer, but they don't want to lose the visibility, transparency and influence they gain by utilizing open source technology.

As there is no complete end to end open source Kubernetes security solution available, companies are forced to turn to proprietary solutions for official support, to fill the gaps, and to ensure ease of adoption.

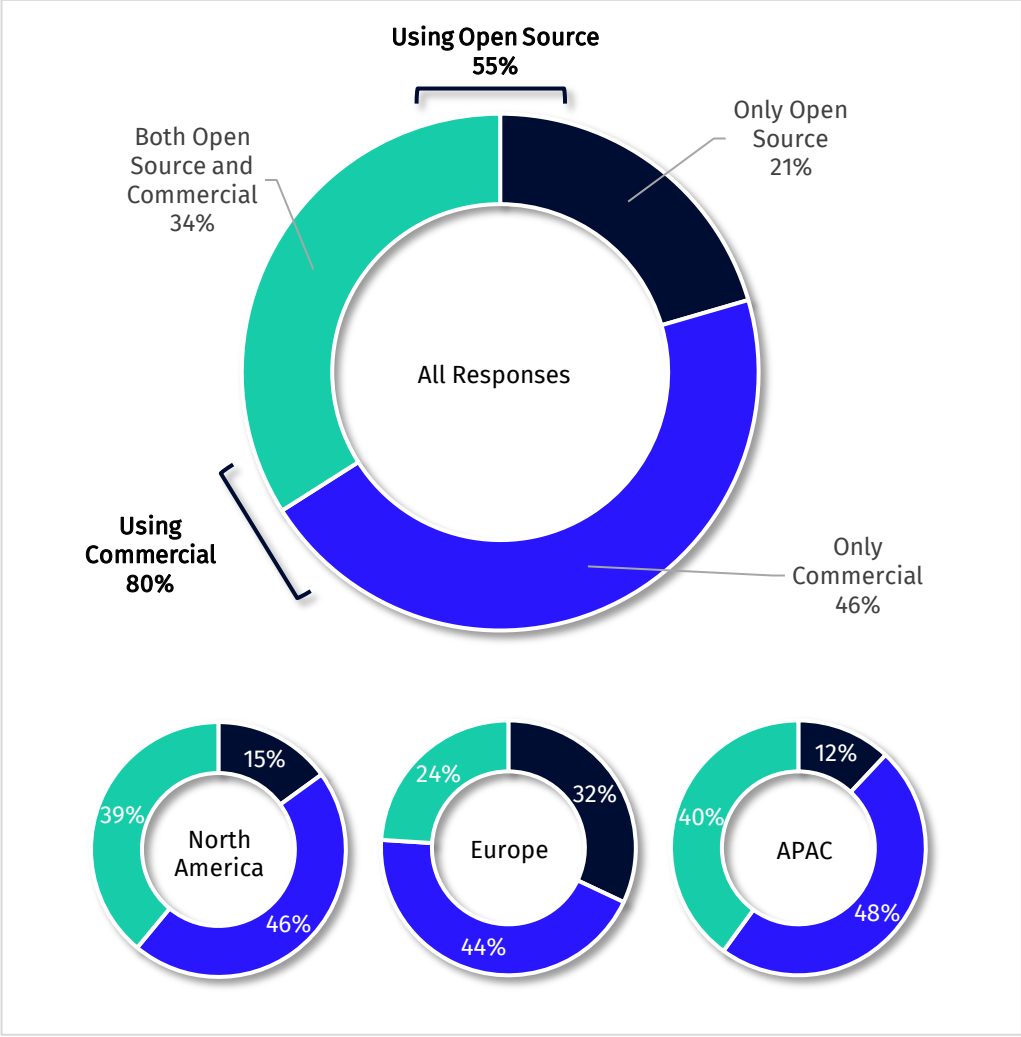

Figure 1: Kubernetes Security – Usage of Open Source vs. Commercial

Open Source vs. Commercial - Preferences for K8S Security Solutions

Given the option to choose, 49% would prefer to use only commercial solutions for K8S security, 14% would prefer to use only open source and 37% prefer a mixture of the two.

This means that 51% would prefer to use at least some open source.

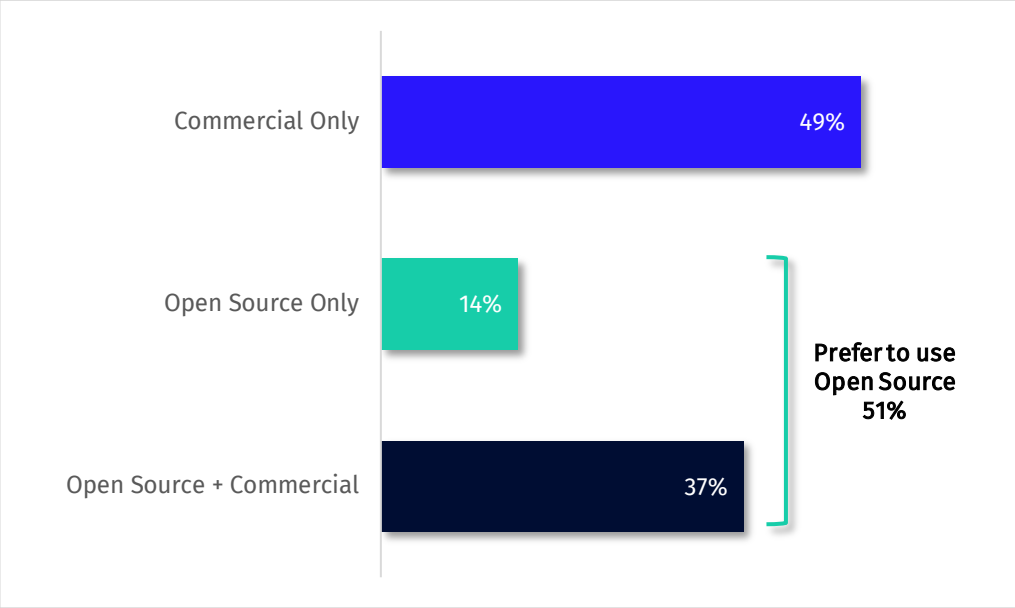

Figure 2: Preferences Towards Open Source vs. Commercial Solutions for Kubernetes Security

Number of Open Source K8S Security Tools in Use

Companies have an average of 3.6 open source tools in use for K8S security.

Overall, just 17% are using a single open source tool. This is because there is no one open source K8s security tool that can do it all! To use open source effectively means using more than one technology and aggregating the integration, management and mitigation of risks across the different tools.

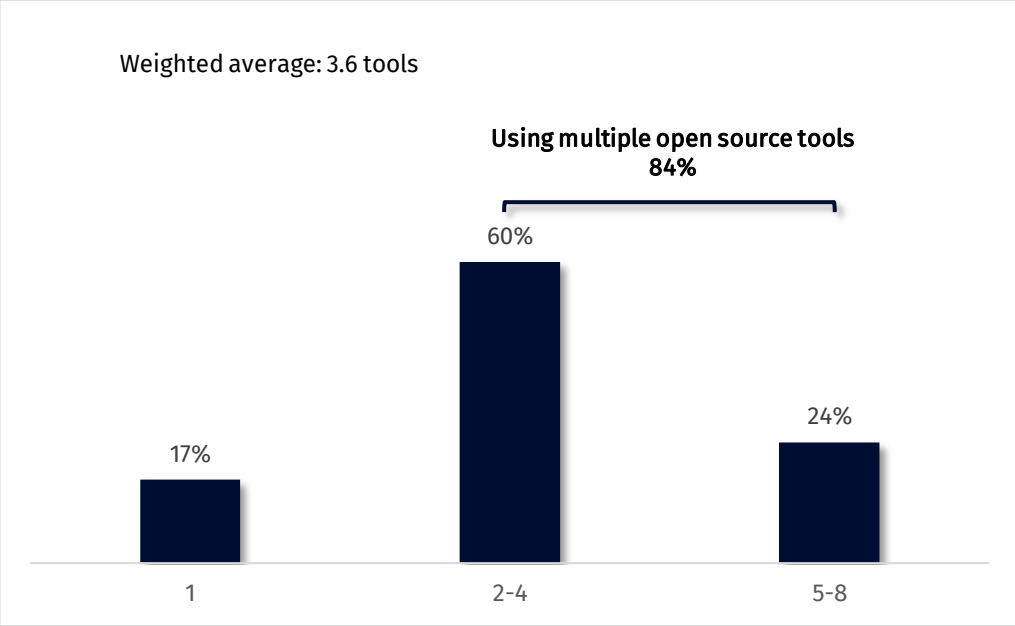

Figure 3: Number of Open Source Kubernetes Security Tools in Use

*Percentages do not add up to 100% due to rounding up of numbers

Open Source is Used Widely for K8S Security

We asked respondents in which areas they are using their Kubernetes security solutions. In all areas, open source is used, either exclusively or in combination with commercial solutions.

The top areas where open source is used are service mesh (32%), network policy/microsegmentation (24%), and misconfiguration scanning (24%). One possible explanation is that several service mesh solutions are CNCF-led graduated projects (such as LINKERD), allowing users to access greater oversight and more support, which may explain their wider adoption rates.

As for proprietary/commercial solutions only, the top areas where this approach is used are vulnerability scanning (51%), secrets protection (51%), and runtime security (51%).

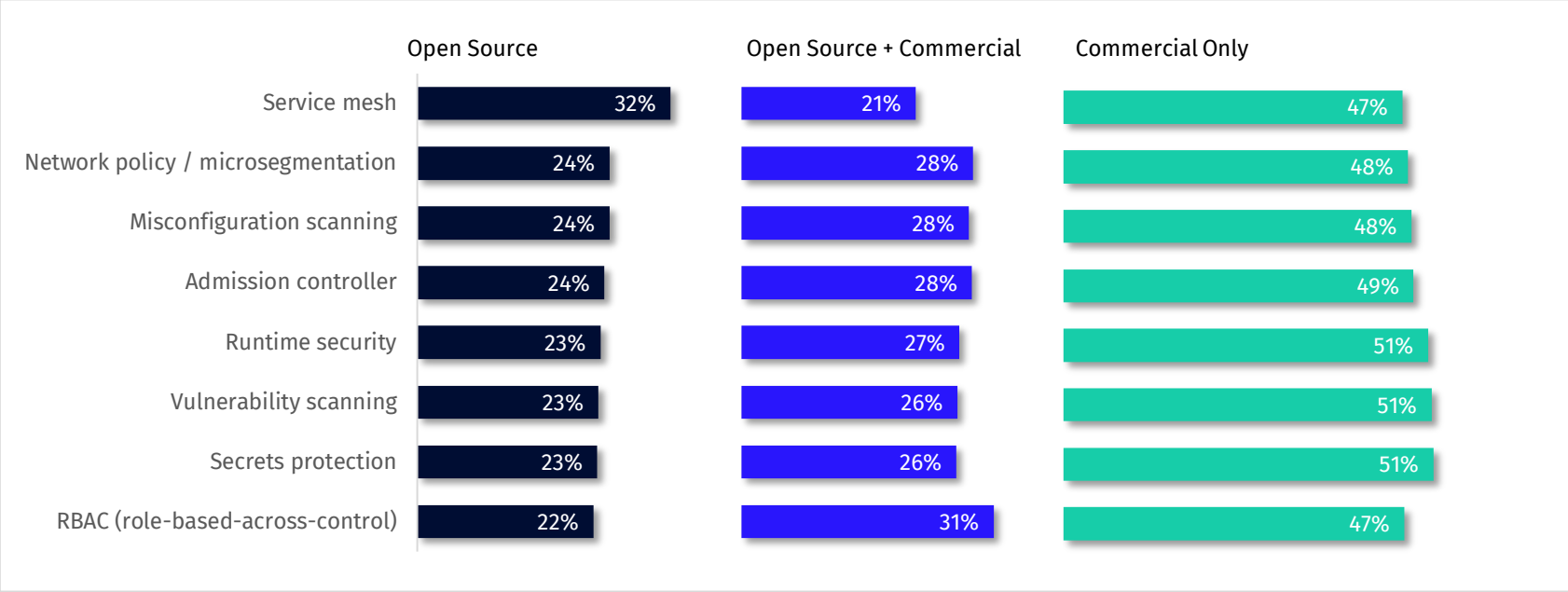

Figure 4: Open Source Usage for K8S Security by Area of Usage

Biggest Challenges Using Proprietary K8S Security Solutions

97% of respondents have challenges when it comes to using proprietary Kubernetes security solutions.

The top challenge with proprietary solutions is that they are a "black box" (69%), where users have zero or limited control and ability to contribute or engage in discussions and lack oversight and visibility into the code and its roadmap.

This is followed by complex pricing, meaning the price is hard to understand or predict (62%), and solutions that are too expensive (47%).

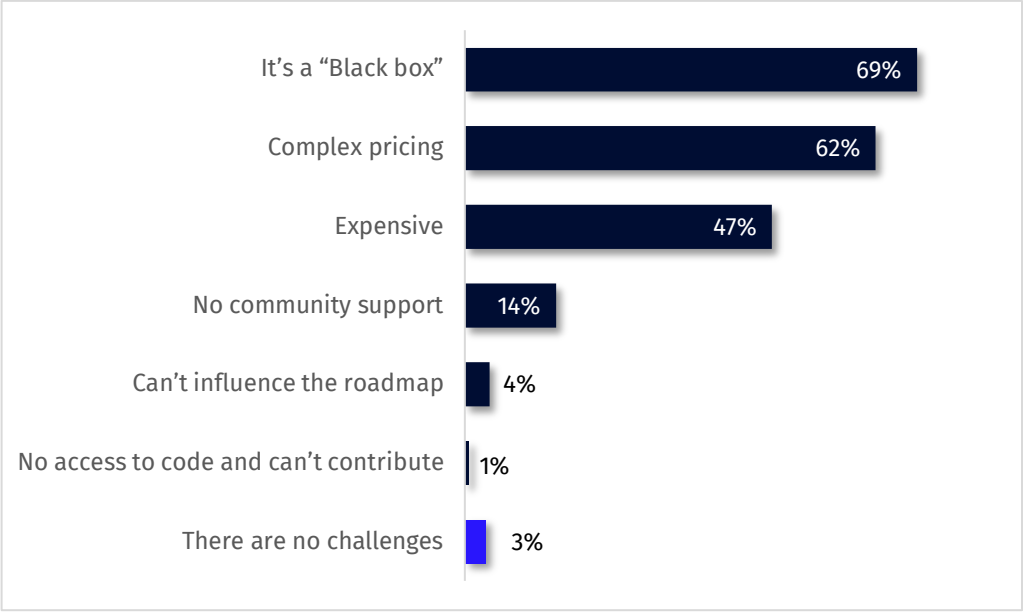

Figure 5: Biggest Challenges of Using Proprietary Kubernetes Security Solutions

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Top Challenges Using Open Source for K8S Security Solutions

95% of respondents admit to having challenges when it comes to using open source solutions for K8S security.

The top challenges are integration with other DevOps tools (62%), managing Kubernetes (51%), and setting up Kubernetes (45%).

For open source Kubernetes security solutions to thrive, they will need to support better integration with the existing DevOps technology stack, as well as be easier to initially set up manage on an ongoing basis.. Without these benefits, open source adoption will continue to be inhibited.

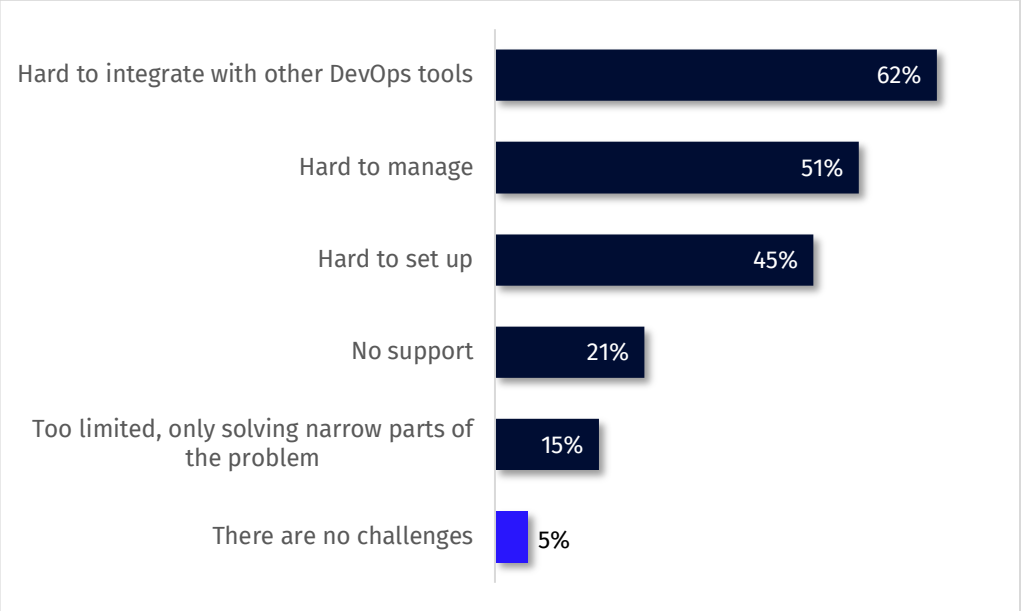

Figure 6: Top Challenges Using Open Source for Kubernetes Security Solutions

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Complexity of Integrating K8S Security Solutions into Existing Stack

69% said it is difficult to integrate Kubernetes security solutions into their existing Kubernetes stack. Only 31% found it easy or requiring a regular level of difficulty to integrate.

This could be partly explained by the use of multiple open source tools as noted above. The more tools that have to work together, the more challenging integration can become.

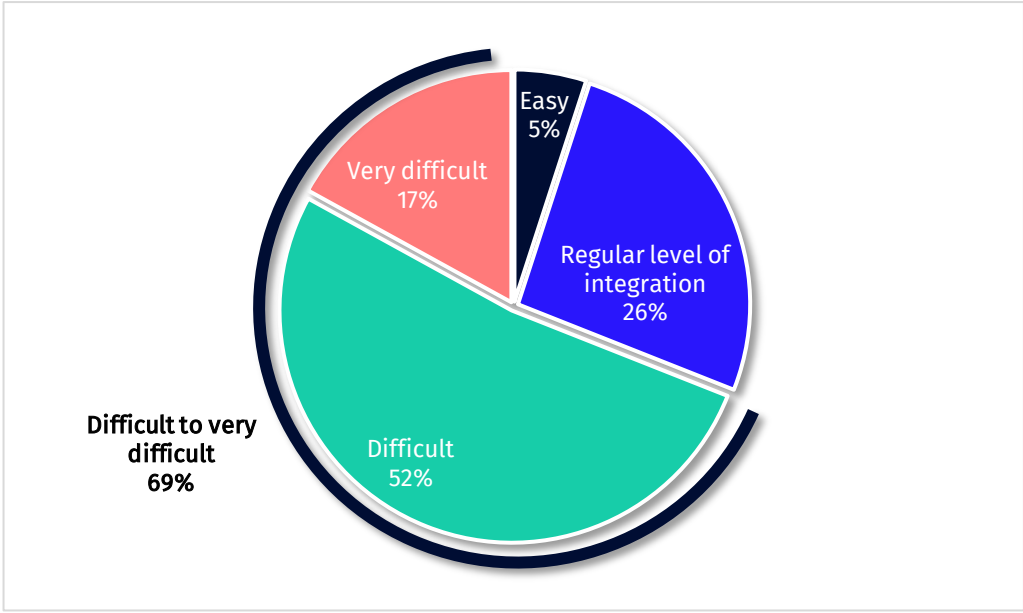

Figure 7: Level of Complexity to Integrate Kubernetes Security Solutions into Existing Stack

Who Owns vs. Who Should Own K8S Security?

Looking at who owns Kubernetes security in their organization vs. who they think *should* own this area of the business, we see DevSecOps (in both cases) take the top spot 58% say DevSecOps currently own this practice, and 63% believe it should.

However, there is still a lack of maturity and understanding for the term “DevSecOps”, and we didn’t ask what the DevSecOps function looks like in each company, for example where it sits in the org chart, or who it reports to. These answers will vary from organization to organization, and while it is likely that DevSecOps will become part of the security function moving forward, it is currently still unclear.

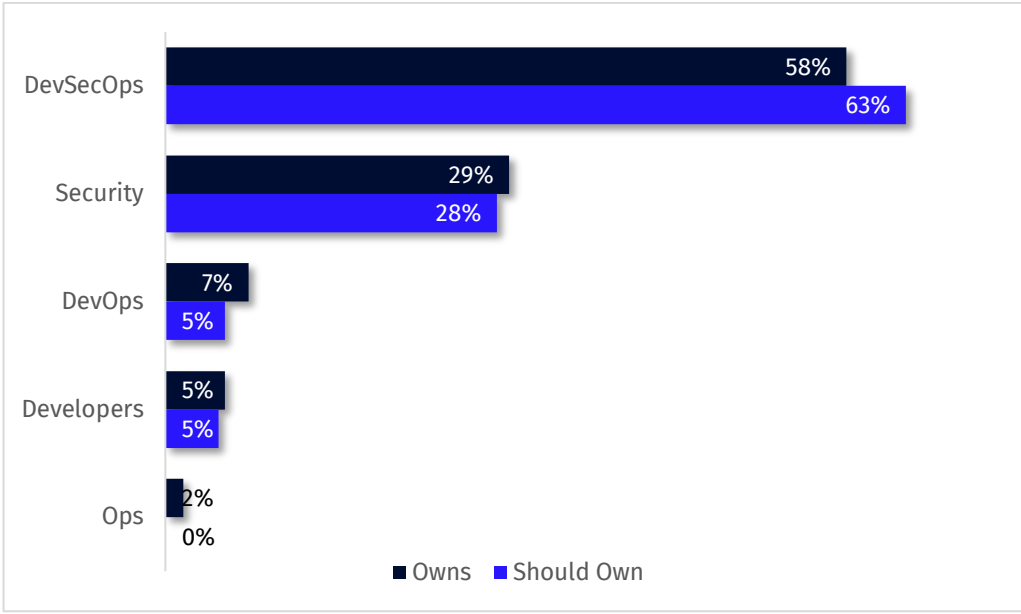

Figure 8: Who Owns and Who Should Own Kubernetes Security?

Ownership of K8S Security in the Organization by Titles

We looked at who currently owns Kubernetes security in the organization today by different titles within the business.

We see gaps between how DevOps, Security stakeholders and IT people see this issue, showing there is a clear issue in terms of Kubernetes security ownership.

Kubernetes security is still a relatively young practice (only a few years old), and over the next few years, the market is likely to decide where it resides within the business, whether that's DevOps or Security.

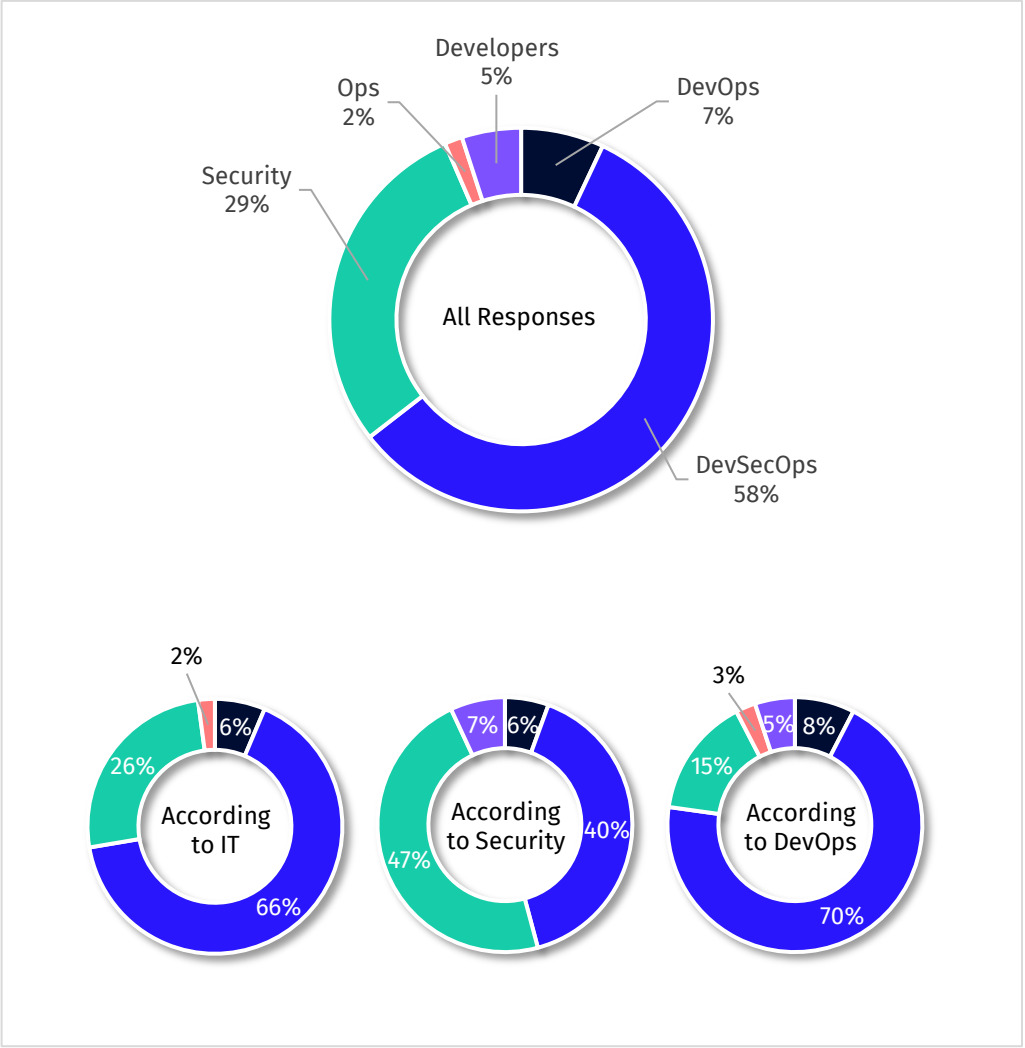

Figure 9: Ownership of Kubernetes Security in the Organization

Level of Confidence in the Organization's K8S Security Expertise

78% are very to extremely confident in their organization's Kubernetes security expertise.

This high number could be a reflection of strict security practices. Perhaps, though, some organizations may be unfamiliar with the complete threat environment for Kubernetes-based security, as it is a relatively new and diverse practice where expertise is hard to come by.

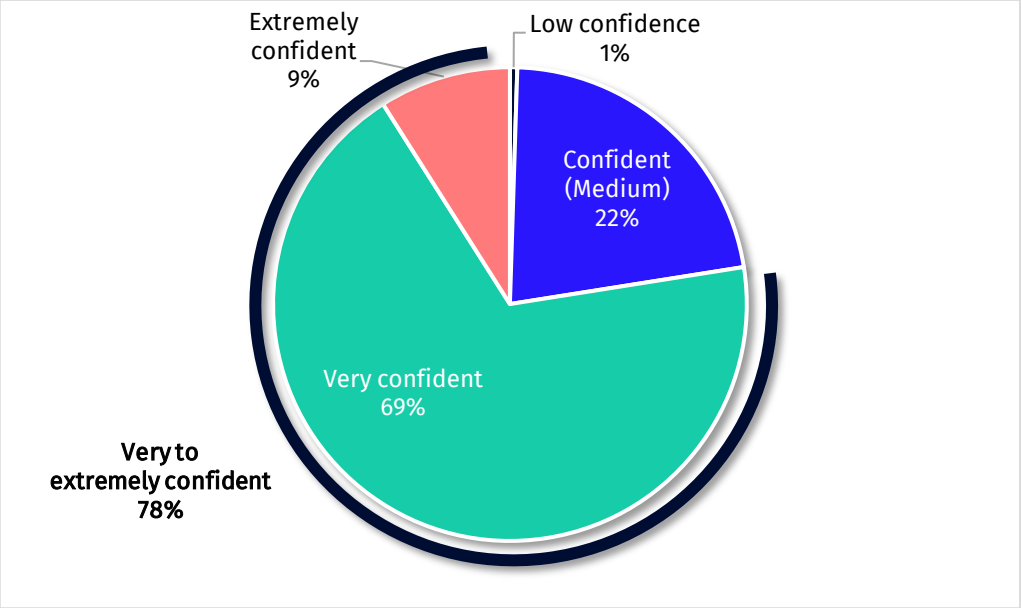

Figure 10: Levels of Confidence in the Organization's Kubernetes Security Expertise

Is K8S an Independent Practice or a Subset of Broader Cloud Security?

97% view Kubernetes security as a subset of broader cloud security rather than its own independent practice.

Kubernetes security is a young and growing practice, and it will be interesting to see whether its unique demands and challenges see it develop into its own independent security practice as it matures.

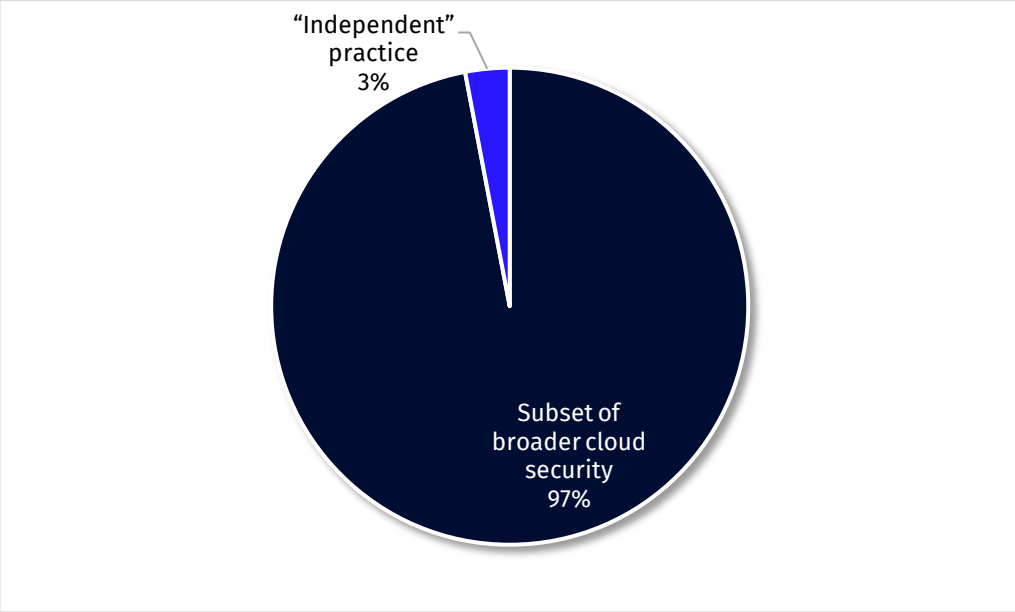

Figure 11: Kubernetes Security Perceptions as an Independent Practice vs. a Subset of Broader Cloud Security

The Biggest Challenges Faced with K8S Security

The top challenges faced with Kubernetes security are too many alerts (68%), solutions that are too fragmented (62%), and that security is interfering with the organization's agility and time-to-market (54%).

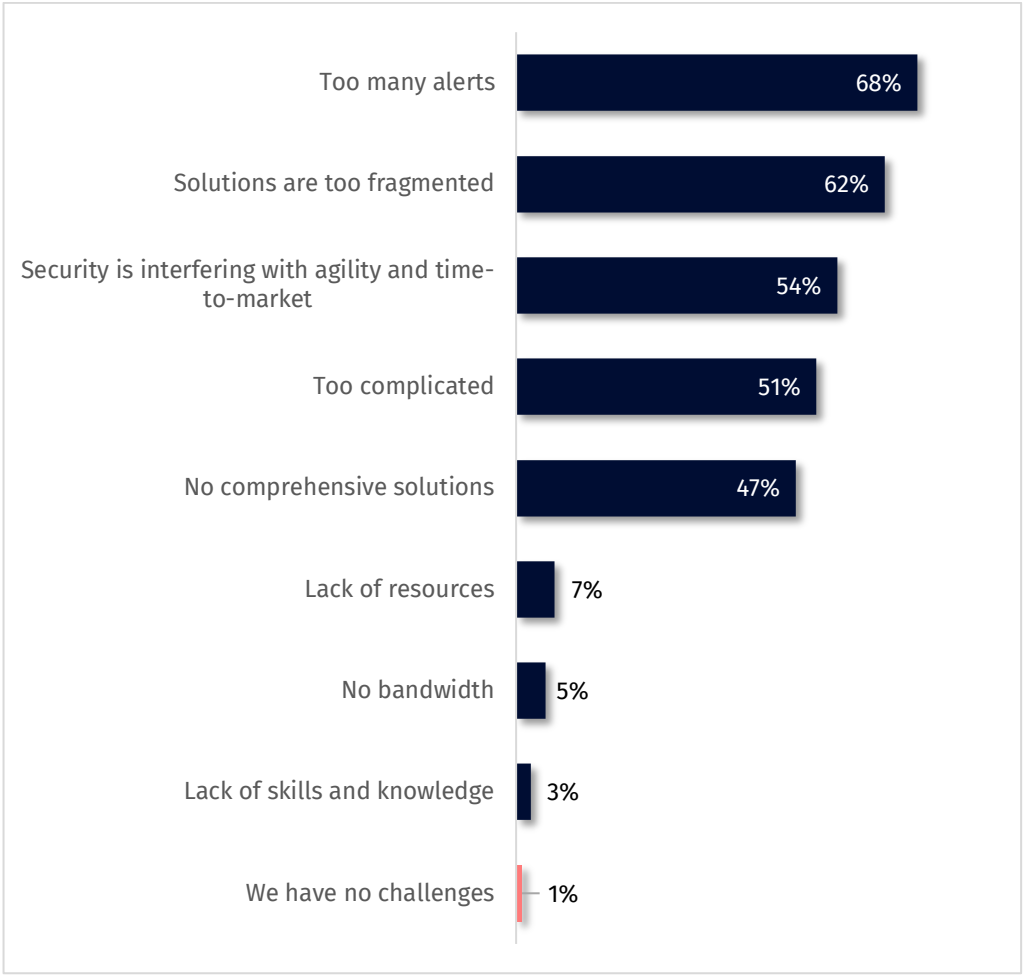

Figure 12: The Biggest Challenges Faced with Kubernetes Security

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Scanning Frequency for K8S Vulnerabilities and Misconfigurations

95% of respondents said they are scanning at least weekly for Kubernetes vulnerabilities and misconfigurations. This means that most organizations are following good security practice and keep good hygiene of their Kubernetes environments.

However, when looking at the breakdown of answers by seniority, we see a striking difference between the perception and reality of VP and C-level executives (figure 14).

These executives overestimate the frequency of scanning with 38% believing it's done every few hours. In contrast, only between 10-19% of those "in the trenches" agree.

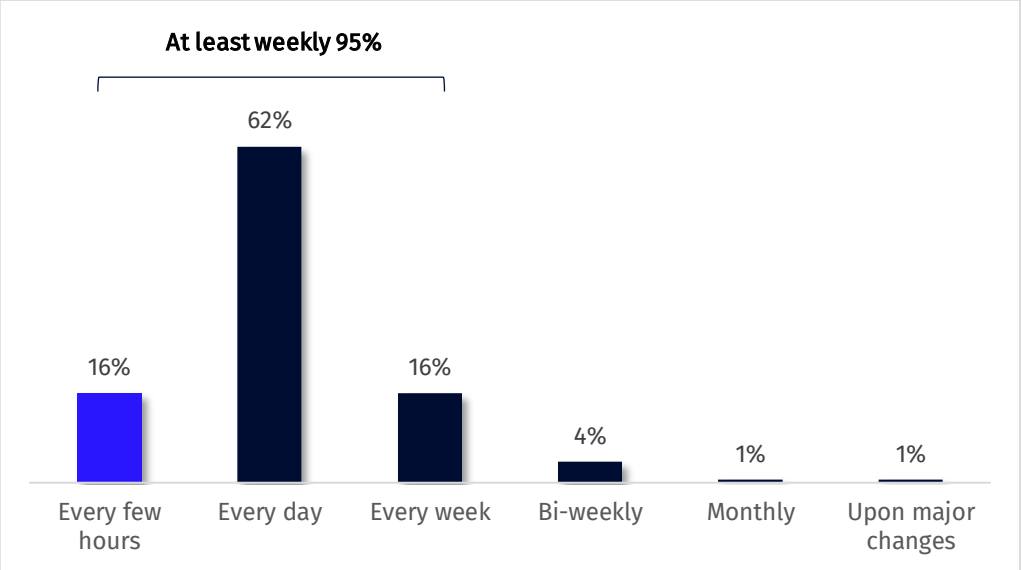

Figure 13: Scanning Frequency for K8S Vulnerabilities and Misconfiguration

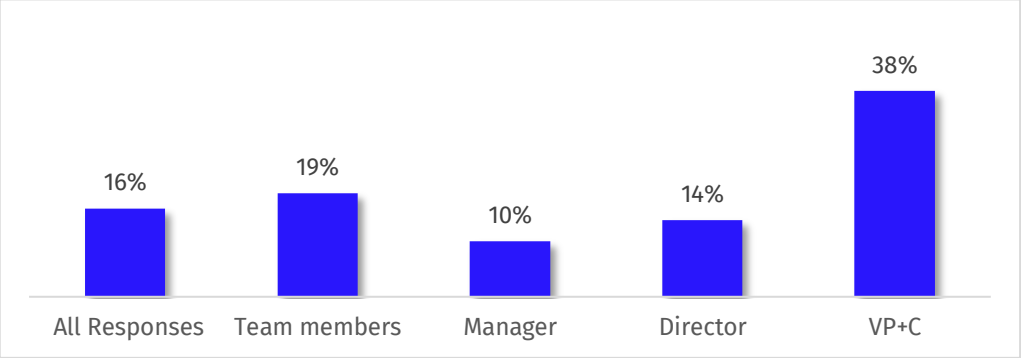

Figure 14: "Every Few Hours" by Job Seniority

Time to Fix Misconfigurations and Vulnerabilities

We asked how often do misconfigurations and vulnerabilities that have been found get fixed? 98% said every week or more frequently.

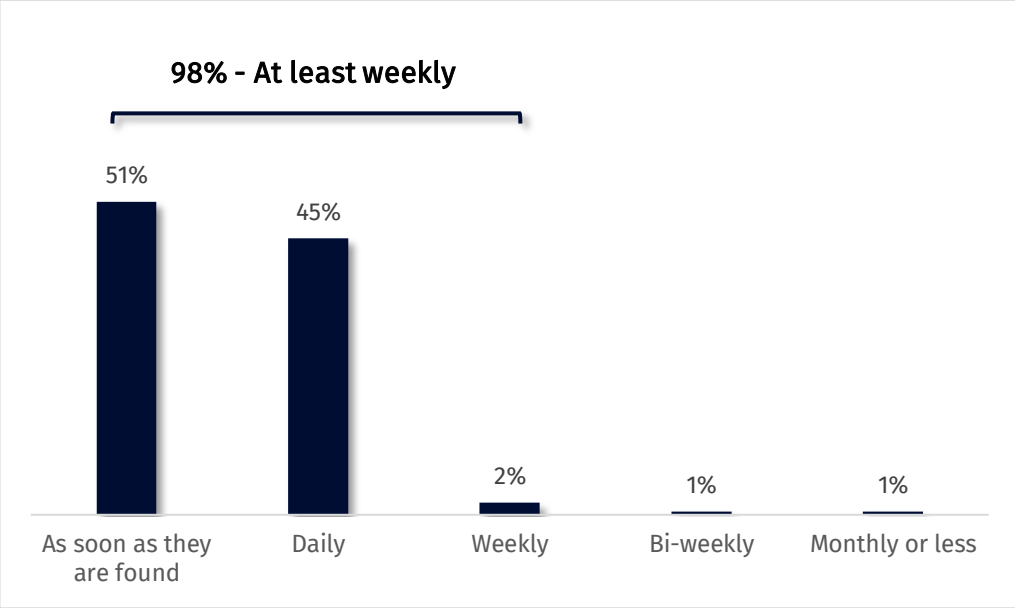

Figure 15: Time to Fix Misconfigurations and Vulnerabilities

Knowledge for Handling K8S Security – Developers vs. Security Teams

We asked respondents if they believe that their developers and security teams are knowledgeable about security in order to effectively handle the security of their organization's Kubernetes environments.

Only 10% consider their developers and security teams to be experts. This is unsurprising as it's still a young practice which is very complex, and it requires expertise that not many have had time to amass.

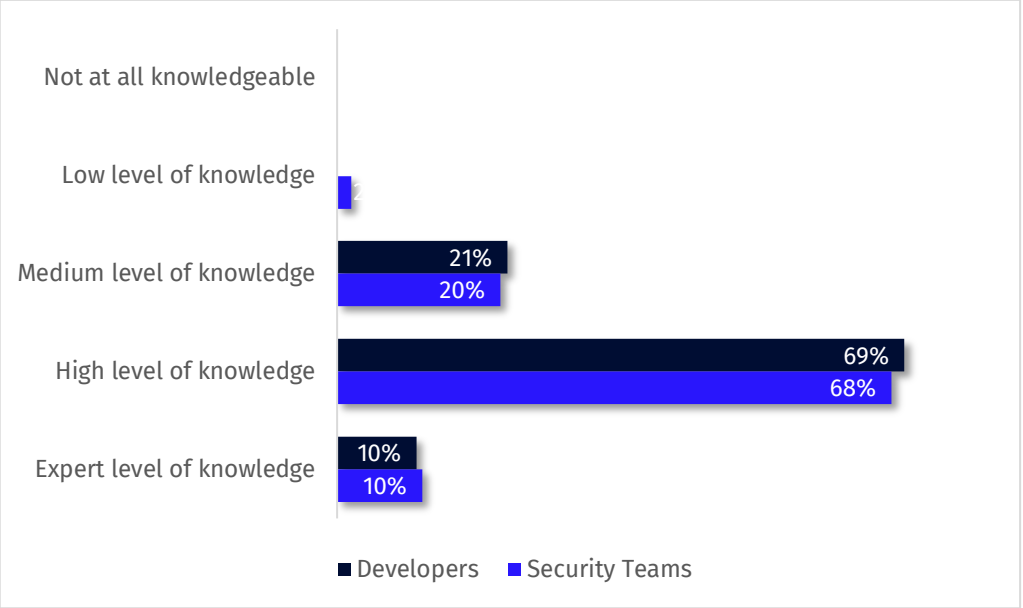

Figure 16: Level of Developers Knowledge About Security for Handling Kubernetes Environments

Top K8S Security Concerns

Top Kubernetes security concerns are identifying potential malware and attacks in the production environment (100%), preventing malware and attacks (100%), and checking their environment for misconfigurations (95%).

It's important to think about runtime security versus security posture. While the first two challenges are related to runtime security for example, misconfigurations are part of maintaining a strong security posture.

Enforcing policies may be currently seen as more of a management issue than a security issue, but it could be a serious security blind spot if it isn't made a greater priority for today's businesses.

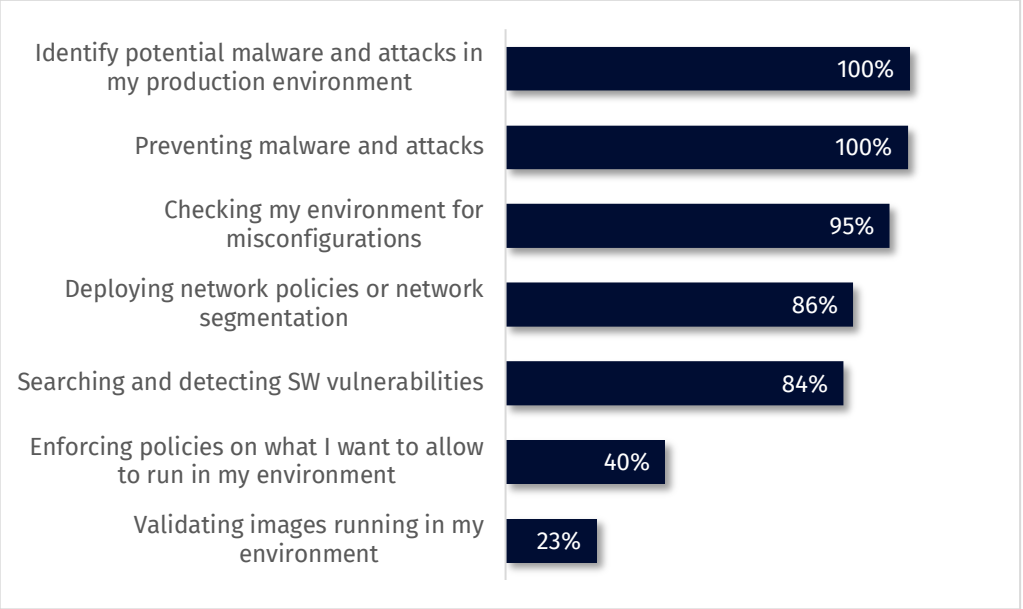

Figure 17: Top Kubernetes Security Concerns

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Roles of K8S Security Tools in Regulation Compliance Requirements

The primary roles of Kubernetes security tools in relation to regulatory compliance requirements are preventing vulnerable containers (71%), producing periodic inventory reports (66%), and verifying least privilege rights (31%).

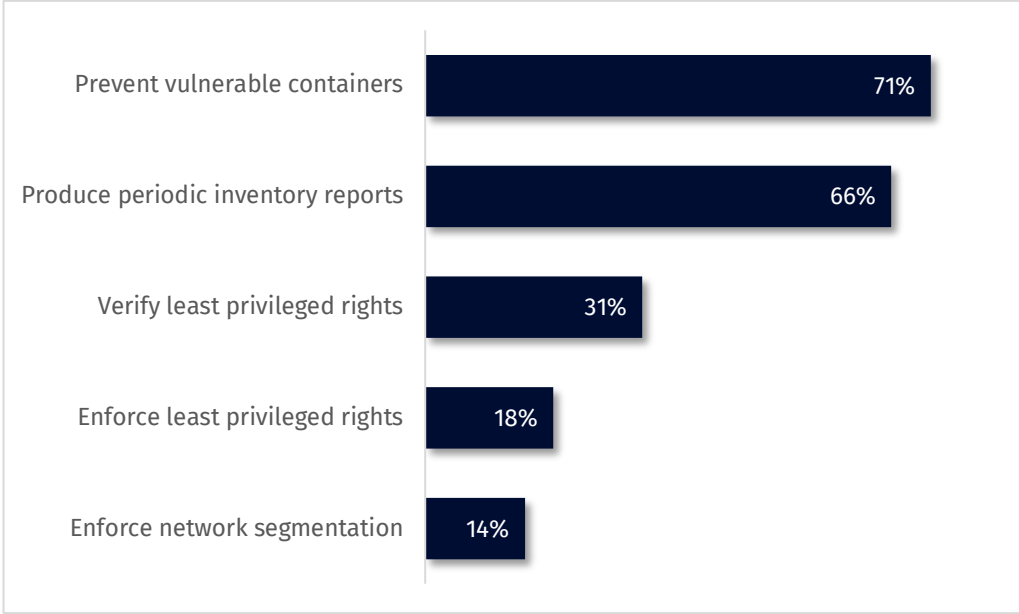

Figure 18: Roles of Kubernetes Security Tools in Regulation Compliance Requirements

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

Demographics

Country, Department, Role, Seniority & Company Size

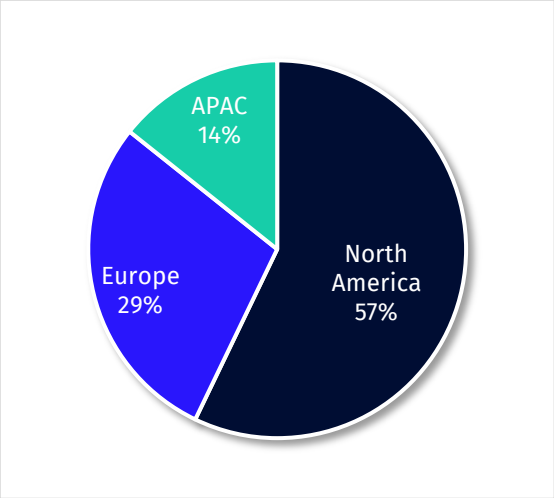

Figure 19: Country

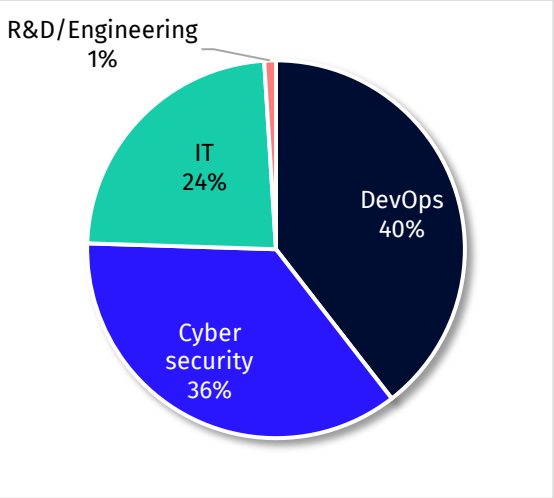

Figure 20: Department

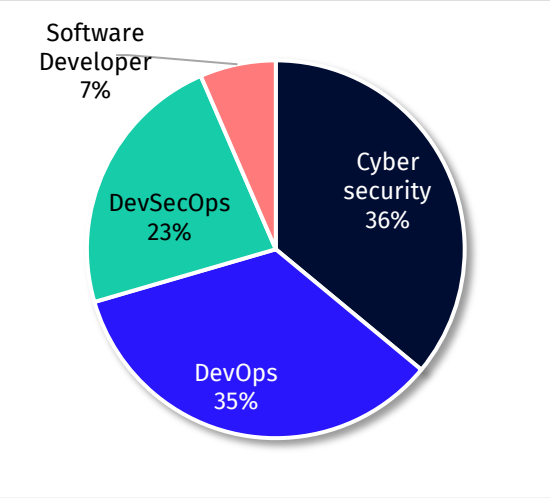

Figure 21: Role

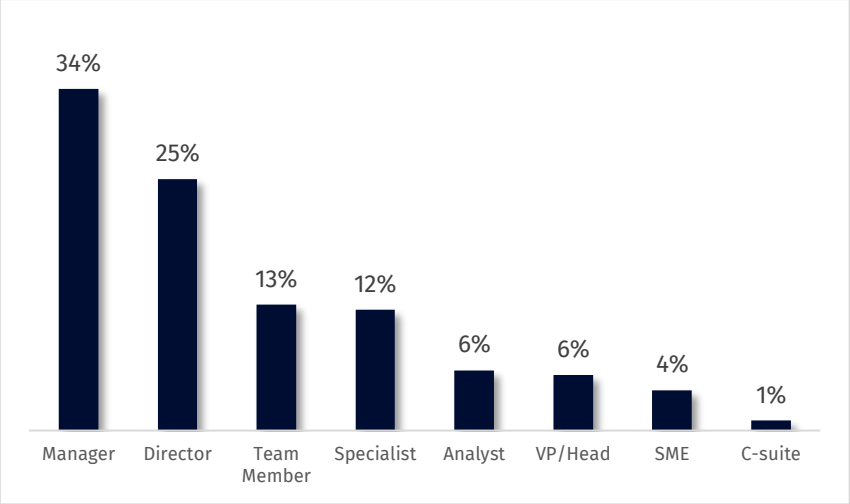

Figure 22: Seniority

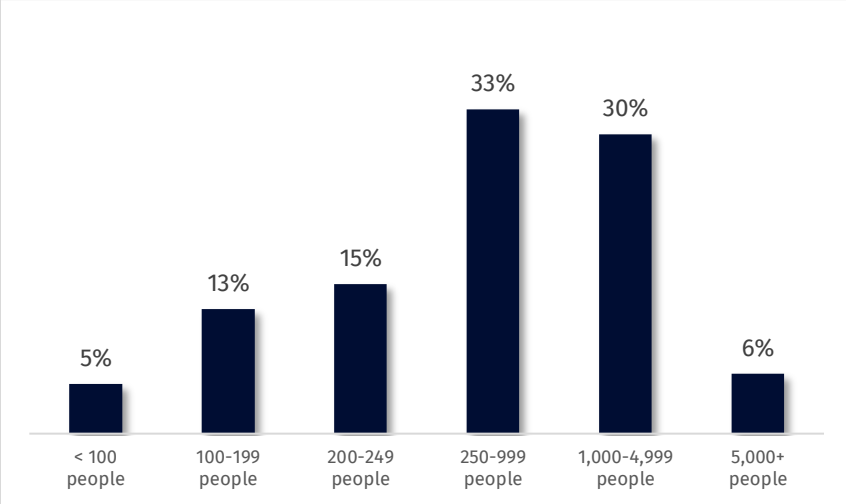

Figure 23: Company Size

About ARMO

ARMO, the creators of Kubescape, is building the first end-to-end open-source Kubernetes Security platform, made for DevOps.

Our patented technology and open-source solutions fit natively within the CI/CD pipeline and existing development tools, assuring DevOps, DevSecOps, and developers that every Kubernetes's cluster, container, and microservice is born and remains secure, from development to production and from configuration to run-time, every time.

Kubescape scans Kubernetes clusters, Manifest files (e.g. YAML, HELM), Code repositories, Container image registries, worker nodes and API servers, detecting misconfigurations according to multiple frameworks (such as the NSA-CISA, MITRE ATT&CK and more), and isolating software vulnerabilities and RBAC (role-based-access-control) violations at early stages of the CI/CD pipeline. It also calculates risk score instantly and shows risk trends over time.

- Join the discussion on Discord - https://discord.gg/DWv4gPgCzU
- Get involved on Kubescape GitHub page - https://github.com/kubescape/kubescape
- Follow us on Twitter - https://twitter.com/armosec
- Sign up for Kubescape cloud (free forever for up to 10 worker nodes) - https://cloud.armosec.io/account/sign-up