ARMO

The State of Cloud Runtime Security, 2025 Edition

Table of Contents

Introduction and Key Findings

Introduction & Methodology

As cloud technologies become the backbone of modern digital infrastructure, they have driven major advances in both cloud development and cybersecurity. The early approach to cloud security, known as "shift left", focuses on integrating security from the start of the development process through a design-first mindset. While this agentless strategy can reduce time and cost, it also requires accepting certain risks and may inadvertently overlook others, leaving potential vulnerabilities that attackers can exploit during runtime. As a result, runtime security, once primarily used for monolithic, on-premises systems, is becoming increasingly critical in cloud environments.

Runtime security for the cloud, however, is quite different, and traditional security measures such as firewalls and endpoint detection and response (EDR) are no longer enough. For best results in what has essentially become 'modern risk management', a new agent-based approach is needed. As a result, eBPF agents (extended Berkeley Packet Filter) – a technology that has been widely adopted in the cloud-native ecosystem – are now on the rise.

As organizations increasingly adopt this technology, they encounter expanded attack surfaces with novel threats that are difficult to manage with traditional runtime security measures. Security teams often struggle to respond promptly to cloud attacks due to a lack of real-time context and visibility. This issue is compounded by the challenges of tool sprawl, escalating cloud security costs, and an overwhelming number of false positives, leaving security teams stretched thin and forced to prioritize which breaches they can realistically defend against.

CADR (Cloud Application Detection Response) is a new paradigm that connects the dots and provides a fully explainable and traceable runtime security story spanning the entire cloud technology stack. It combines multiple detection methods to provide a holistic view of threats across cloud infrastructure, Kubernetes environments, containers, and applications – offering a highly effective solution to runtime security challenges. This approach focuses on continuous, real-time threat detection that can quickly adapt to evolving attack strategies. Unlike legacy security solutions, CADR delivers proactive risk identification and mitigation in cloud-native environments. Its holistic methodology goes beyond simple monitoring, enabling security teams to stay ahead of novel cyber threats.

The aim of this survey was, therefore, to provide CISOs, cloud security architects, SecOps and other senior security stakeholders, with data and insights into current cloud runtime security trends and challenges, with a focus on the benefits of CADR. Some of these challenges include how organizations are currently dealing with attacks on cloud infrastructure and applications, what tools they are using to detect and respond to these attacks, and how siloed tool usage exacerbates the code-to-cloud problem by increasing MTTD and MTTR for cloud-based attacks.

Methodology

To get more insight into the current state of cloud runtime security, we commissioned a survey of 300 SecOps stakeholders and cybersecurity leaders to shed light on their current usage and priorities.

This report was administered online by Global Surveyz Research, an independent global research firm. The survey is based on responses from senior security executives (Directors+), including CISOs, Heads of SecOps, Heads of AppSec, Heads of Product Security, cloud security and security architects. They hailed from companies in the finance, tech, banking and ecommerce industries across the US with at least 1,000 employees; these companies have a SOC (security operation center), use cloud native applications, have most of their infrastructure based on cloud, and deal with cyber-attacks.

The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during March 2025. The average amount of time spent on the survey was 7 minutes. The answers to most of the non-numerical questions were randomized to prevent order bias in the answers.

Key Findings

1 Most SOC teams are overwhelmed by high volumes of security alerts related to potential cloud-based attacks, exacerbated by a less-than-ideal MTTD.

Security teams are overwhelmed by a flood of alerts, most of which lack the context needed to accurately assess and respond to threats. Respondents report receiving an average of 4,080 security alerts per month – or 136 alerts per day – related to potential cloud-based attacks, with the majority (61%) handling between 1,001 and 5,000 alerts monthly (Figure 3). Yet despite this deluge, the average number of true security incidents per year is just 7, meaning it takes an average of 6,994 alerts to uncover one bona fide incident. This "needle in a haystack" challenge is the result of different tools raising "their perspective" of the same event, false positives, and a lack of contextual information – such as asset sensitivity, exploitability, and behavioral baselines – that would help SOC teams quickly zero in on high-risk events. Without context, even benign activity can trigger alarms, stretching resources thin.

Detection times are also lagging. The average time to detect an incident is 4–12 days, with most organizations (71%) taking 1–7 days to identify a cloud-based attack (Figure 5), pointing to an ongoing backlog of alerts and inconsistent monitoring capabilities. The Mean Time to Detection (MTTD) remains too slow for organizations to effectively stay ahead of fast-moving cloud threats. Industries with high-value data and expansive attack surfaces – especially financial services (43%) and eCommerce (39%) (Figure 4) – are among the hardest hit, and would benefit significantly from improvements in alert contextualization and detection speed. Other high-risk sectors, like healthcare and entertainment, should similarly prioritize faster, more accurate cloud threat detection.

2 97% of organization use 3-8 security tools to detect and respond to attacks in the cloud, while 30% miss attacks due to the complexity of correlating alerts. Unsurprisingly, 92% believe that a single, comprehensive, cloud runtime security solution is sorely needed to improve response time.

Nearly two-thirds of organizations (63%) use more than five security tools to detect and respond to cyberthreats in real time within their cloud-native applications and associated infrastructure (Figure 7). This indicates tool sprawl, which impedes the collection and collation of information from different sources into a comprehensive attack story that security professionals can use to respond to incidents quickly and effectively. In addition, most organizations (89%) admit that their current processes for identifying and responding to active attacks in cloud environments result in missed attacks (Figure 6). This suggests that their existing tools aren't targeting runtime security effectively – leaving security incidents undetected – and that perhaps they have an outdated approach to detecting and responding to active attacks in the cloud.

It is no surprise, therefore, that a whopping 92% of respondents believe that a single, comprehensive, cloud runtime security solution that can follow incidents throughout the cloud stack and account for application behavior – would improve their team's response time to cloud-based incidents (Figure 8).

3

While noisy alerts pose a significant challenge to detecting and responding to threats, duplicates and blind spots resulting from siloed teams and fragmented visibility are a major problem too.

The most frequently encountered challenges that organizations face in detecting and responding to cloud-based attacks are alert fatigue (46%) and high volume of false positives (45%), as seen in Figure 11. The lack of contextualized alerts is also the top impediment (53%) for security teams to reduce MTTD and MTTR in their current cloud runtime security setup (Figure 15). In addition, the average time to correlate alerts from different tools during a cloud security incident is 7.7 days, and can take as long as 30 days (Figure 13). Indeed, only 13% of organizations say they successfully correlate alerts across different security tools, indicating there is a significant gap in visibility and response coordination. This finding, therefore, highlights the potential for automation to create a single attack story, and confirms that enhancing alert context and reducing false positives are both key to improving MTTD and MTTR.

Fragmented visibility due to too many separate tools is also a top challenge (44%) – particularly for CISOs and cloud security professionals (Figure 12), because it can impact negatively on their KPIs, such as MTTD, MTTR and incident response rate. These KPIs are relevant to SecOps too, so while it's understandable that AppSec and Security Architecture teams worry less about fragmented visibility – most likely because they have different KPIs – the fact that SecOps don't worry about it as much is somewhat surprising, and suggests that perhaps they're not as worried about fragmented visibility as they should be.

4

92% of SecOps and cybersecurity leaders agree that tools that contextualize alerts into a single attack story can improve their response time to cloud-runtime security incidents.

An overwhelming majority of respondents (92%) either agree (57%) or strongly agree (35%) that tools that contextualize alerts into a single attack story can help reduce their response time to cloud-runtime security incidents (Figure 14). This strong consensus on the benefits of context in improving incident response efficiency is unsurprising, given that most organizations spend an average of 7.7 days on correlating alerts and information from different security tools during a cloud security incident (as seen in Figure 13) – which is less than ideal.

5 38% of SecOps find the Cloud Security team most difficult to work with, reflecting the need to shift to cloud-native approaches to improve visibility, automation, threat detection and collaboration.

The majority of SecOps professionals (38%) struggle to collaborate with the Cloud Security team during security incidents, as seen in Figure 16. This suggests that security processes may be too siloed, resulting in a lack of clear communication channels with other teams. In addition, the fact that 31% of respondents find the Platform team difficult to work with, indicates that infrastructure management and security alignment may not be fully optimized. All of this impedes their ability to meet their MTTD and MTTR KPIs, so to overcome this challenge and mitigate the problem, there needs to be a shift from traditional security models to the more modern cloud-native approaches to improve visibility, automation, threat detection and collaboration.

The fact that most organizations (63%) have a dedicated team in-house responsible for detecting and responding to cloud-based attacks (Figure 17), indicates that they understand that cloud-native attacks are different from traditional security threats, and explains why they choose to invest in a dedicated Cloud Security team rather than scale the traditional Security Operations Center (SOC) team. As the survey results show, however, if Cloud Security teams endeavor to improve their communication and collaboration processes, it would make handling security incidents across the organization far more cohesive and efficient.

Survey Report Findings

Frequency of Cloud-Based Security Incidents Experienced in the Past 12 Months

As cloud becomes more pervasive – the more organizations expand their cloud infrastructure, the more cloud-based attacks they are exposed to, with recent research showing that the total number of reported CVEs has increased by approximately 35% year-over-year—from 28,817 to 38,958. **The survey results corroborate this well-known market trend, with respondents confirming their organizations experienced an average of 7 cloud-based security incidents in the past year** (Figure 1): Most respondents (52%) reported handling 6-10 incidents in the past 12 months, while 33% report 3-5 incidents. Only 15% experienced more than 10 incidents.

In addition, **the more IT infrastructure an organization has on the cloud, the higher the frequency of attacks** (Figure 2): 67% of those who reported between 6-10 incidents are from organizations with more than 81% of their infrastructure in the cloud, and 35% are from organizations with 51% to 80% cloud-based infrastructure.

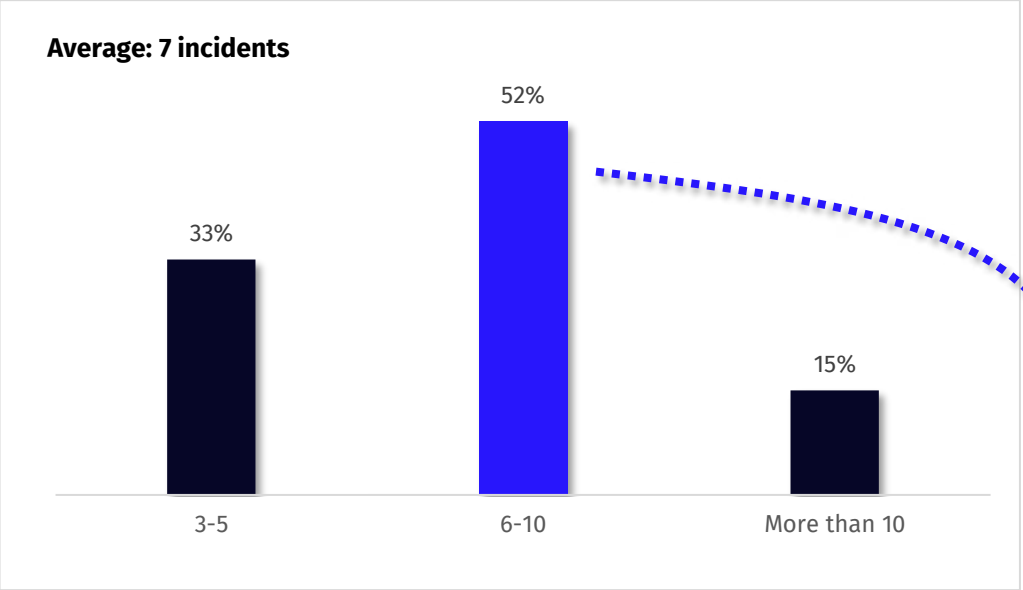

Figure 1: Cloud-Based Security Incidents Experienced in the Past 12 Months

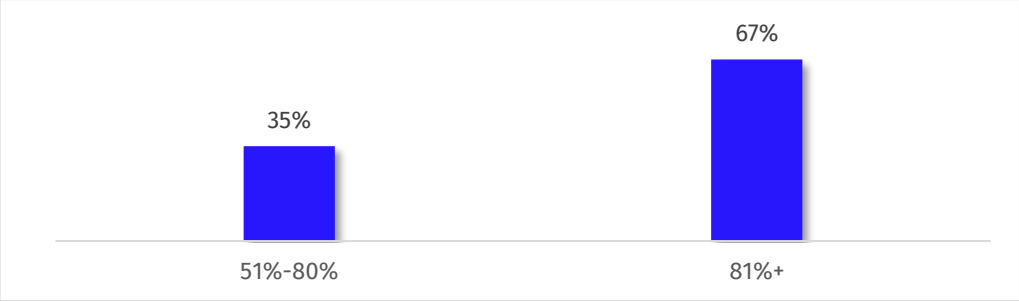

Figure 2: “6 to 10 incidents” by percentage of IT infrastructure in the cloud

Average Number of Security Alerts Related to Potential Cloud-Based Attacks

Most organizations (61%) receive 1,001-5,000 security alerts per month that pertain to potential cloud-based attacks, with an average of 4,080 alerts per month (Figure 3), equating to about 136 alerts per day (that's calendar days, not just business days). In addition, the average detection time per incident is 4-12 days, with most (71%) reporting it takes them 1-7 days to detect a cloud-based attack (Figure 5). This means that SOC teams are typically overwhelmed by a deluge of alerts and an ongoing backlog of security events that they need to investigate and respond to.

Among those that receive 5,001-10,000 alerts per month (29%), **the hardest hit industries include financial services (43%) and eCommerce (39%)** – both of which are prone to high volumes of threats due to the high-value nature of the data they accumulate – followed by technology (24%) and IT (19%), as seen in Figure 4.

While these hardest-hit industries do benefit from the flexibility and scalability that cloud computing offers, they must also be aware that they are being targeted for the resulting large attack surface. Therefore, it would be wise for other sectors that have valuable data, like healthcare, or that use the cloud extensively, like entertainment, to be mindful of these cloud-based attacks as well.

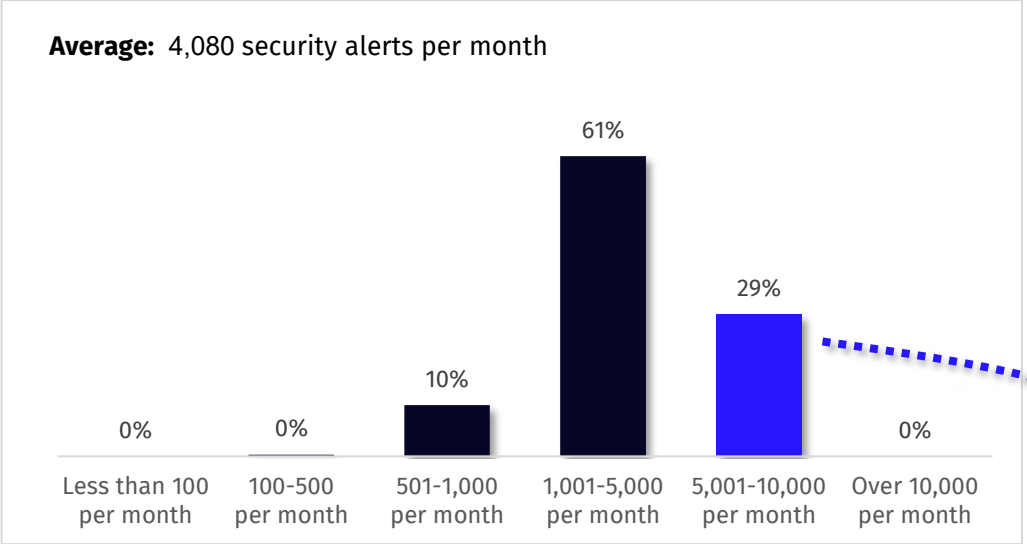

Figure 3: Average Number of Security Alerts Related to Potential Cloud-Based Attacks Received

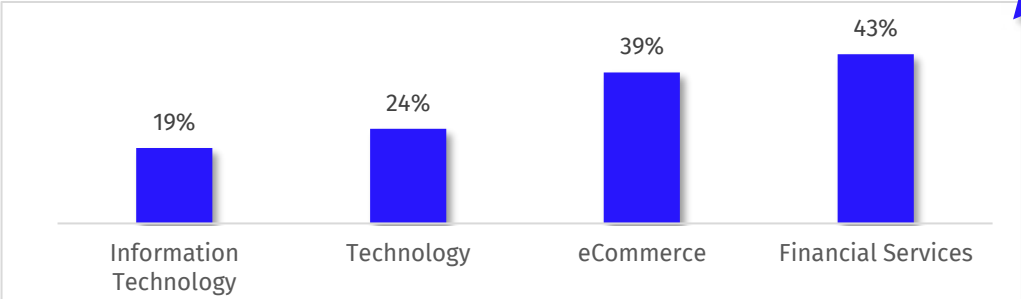

Figure 4: "5,001-10,000 per month" by industry

Time Taken to Detect Cloud-Based Cyber-Attacks in the Past 12 Months

Respondents were asked to share their organization's average detection time of cloud-based cyber-attacks over the past 12 months. **Most reported it takes them 1-7 days to detect a cloud-based attack (71%), with an average of 4 days and an average 'longest detection time' of 12 days – suggesting there are inconsistencies in security posture and monitoring capabilities.**

This indicates that best practices are still emerging in this field, because just as organizations continue to improve, so do the attackers. Organizations must therefore work towards staying ahead of ongoing and new threats, so that rather than taking as long as a week to detect them, they should strive detect them within a far more reasonable 24-hour time frame.

Only a small portion of organizations (22%) identified cloud-based cyber-attacks in less than 24 hours over the past 12 months, and fortunately, almost none reported detection times of more than 30 days (1%).

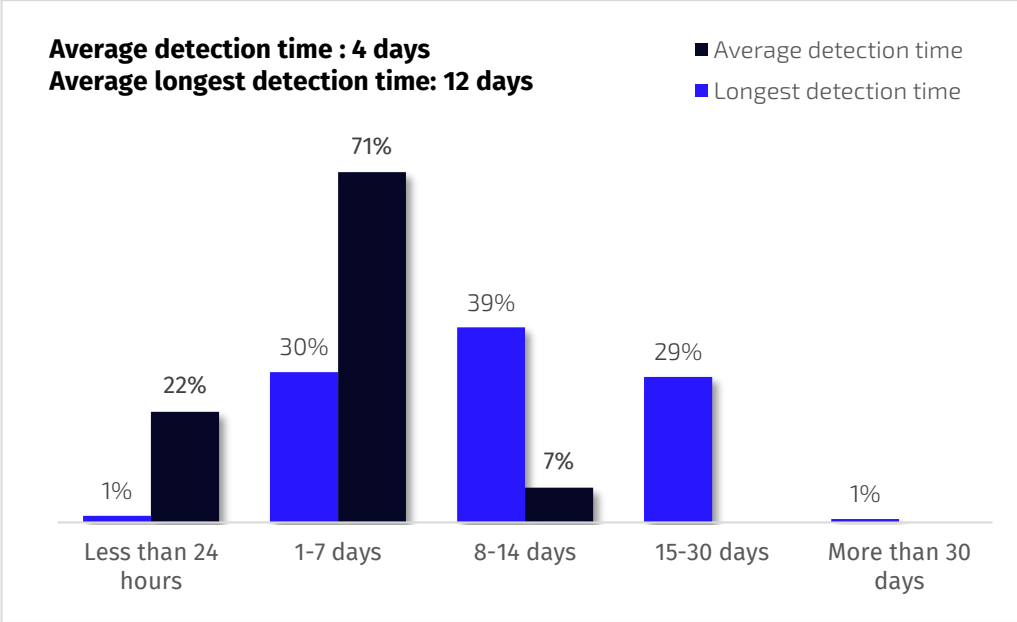

Figure 5: Time Taken to Detect Cloud-Based Cyber-Attacks in the Past 12 Months

Ability to Effectively Detect and Respond to Active Attacks in Cloud Environments

When it comes to detecting and responding to active attacks in cloud environments, most respondents (89%) – or, nine out of ten organizations – admit they are missing active attacks. The reasons cited for this include an overwhelming volume of alerts from their security tools (43%), struggling with correlating alerts from different tools (30%), and false positives generated by current security solutions (16%). The common denominator for these reasons is that they all stem from existing tools, which are likely legacy runtime security tools that weren't designed for cloud environments, or cloud security tools that focus mostly on posture management or just on one layer of the cloud in the stack.

It is also possible that these organizations simply have an outdated approach—trying to apply traditional runtime security processes and measures to the cloud. Those who are using a more current approach to detecting and responding to active attacks efficiently, are using a cloud runtime security solution that can follow the incident throughout the cloud stack, and that can account for application behavior to avoid false positives. That said, only 11% of respondents say they are able to detect and respond to *all* active attacks in their cloud environment, which means that for most organizations this is still a problem.

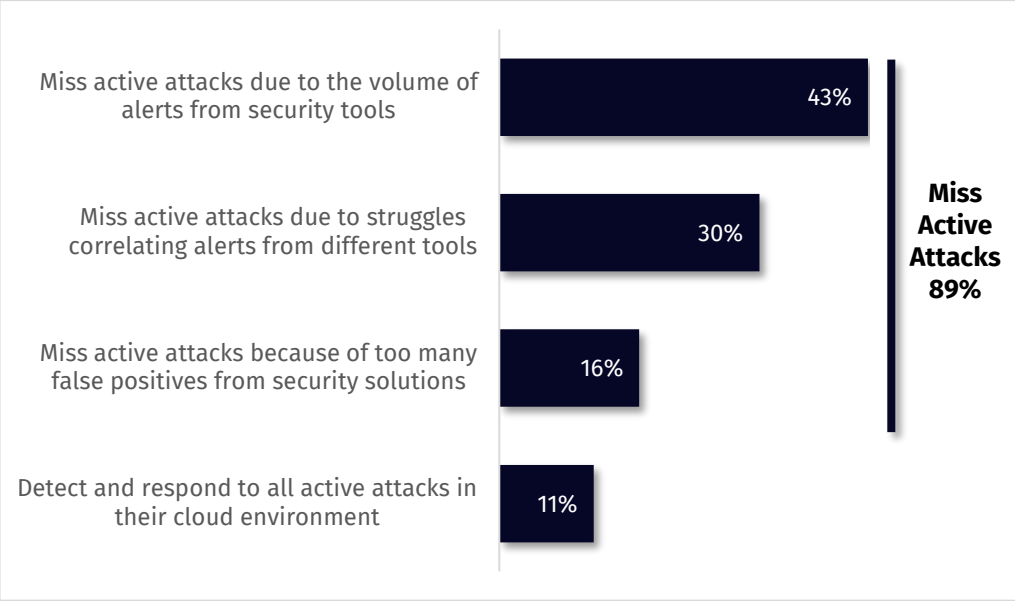

Figure 6: Experience with Identifying and Responding to Active Attacks in Cloud Environments

Cloud Security Tools Used to Detect and Respond to Cyberthreats in Cloud-Native Applications

Most organizations (97%) use between 3-8 security tools to detect and respond to cyberthreats in real time within their cloud-native applications and associated infrastructure. The tools fall into the categories of CDR, ADR, EDR, or CWPP and exclude CSPM and CNAPP. **Nearly two-thirds of organizations (63%) use over five tools,** as seen in Figure 7.

This indicates tool sprawl, which forces security professionals to waste a lot of time on collating data from disparate sources manually, and impedes their efforts to respond efficiently to various incidents. This finding suggests, therefore, that substantial integration is needed behind the scenes to make the process of compiling a coherent attack narrative less demanding for security teams.

It also supports the notion that using a single comprehensive cloud runtime security solution would improve their response time, as seen on the next page (Figure 8).

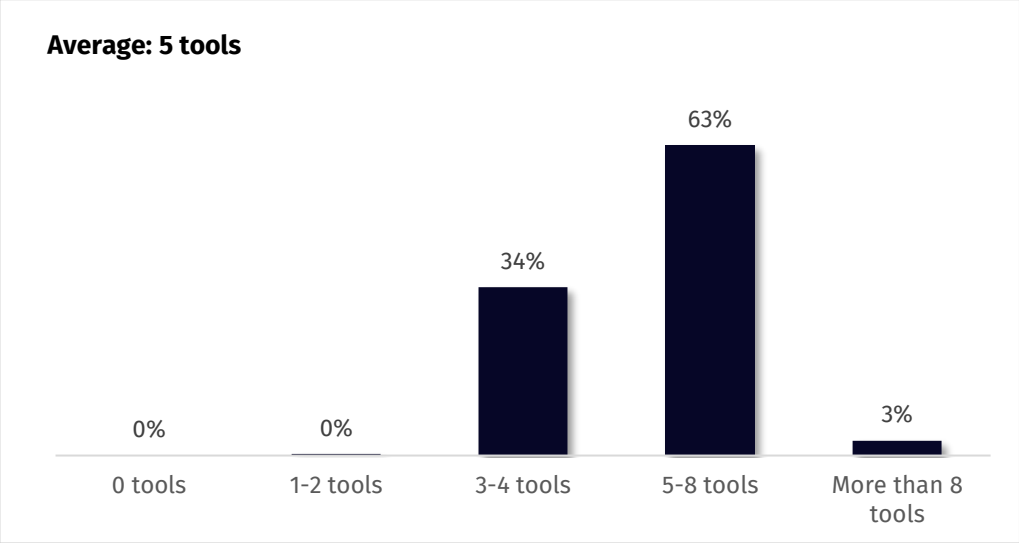

Figure 7: Cloud Security Tools Used to Detect and Respond to Cyberthreats in Cloud-Native Applications

Impact of a Single, Comprehensive Cloud Runtime Security Solution on Response Time to Cloud-Based Incidents

A whopping 92% of respondents believe that a single, comprehensive cloud runtime security solution would either significantly (40%) or somewhat (52%) improve their team's response time to cloud-based incidents (Figure 8). Only a small portion is unsure of the impact (5%) or thinks it would have little impact (3%).

None of the respondents said there would be no impact on response time at all (0%), which is testament to the resounding agreement across the board that a single, comprehensive cloud runtime security solution – as opposed to the current prevalence of tool sprawl, as seen in Figure 7 – is sorely needed.

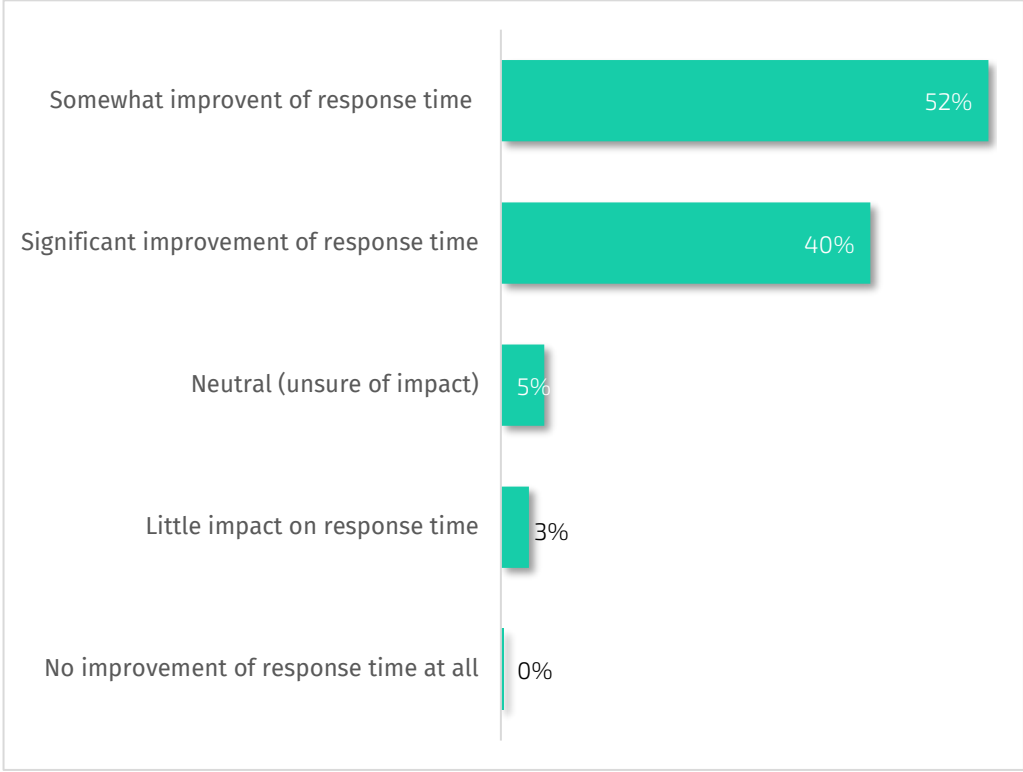

Figure 8: Impact of a Single, Comprehensive Cloud Runtime Security Solution on Response Time to Cloud-Based Incidents

Biggest Challenge in Implementing Threat Detection and Response Solution in Cloud Environments

The biggest challenges in implementing threat detection and response solutions in cloud environments are concerns over performance degradation (28%) and resource consumption (23%), as seen in Figure 9. Citing the presence of a large number of agents already in the system is also seen as a big challenge by 21% of the respondents, most of whom hold roles in SecOps (43%) and AppSec+ Product Security (21%), as seen in Figure 10.

This finding indicates that agents are still regarded as intrusive by many practitioners, with 80% citing an agent-related justification for not implementing a threat detection and response solution. This is interesting, given that many of the runtime solutions that are currently flooding the market are agent-based.

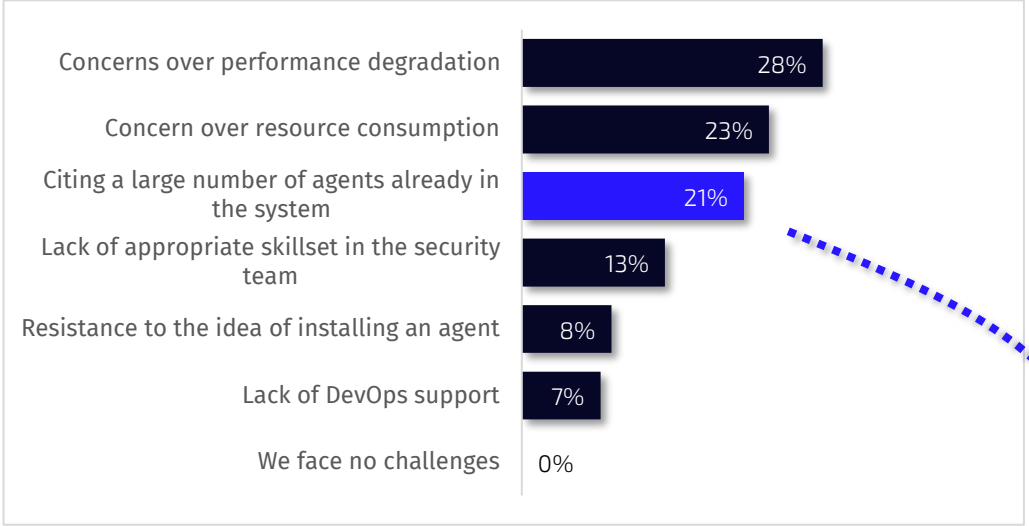

Figure 9: Biggest Challenge in Implementing Threat Detection and Response Solution in Cloud Environments

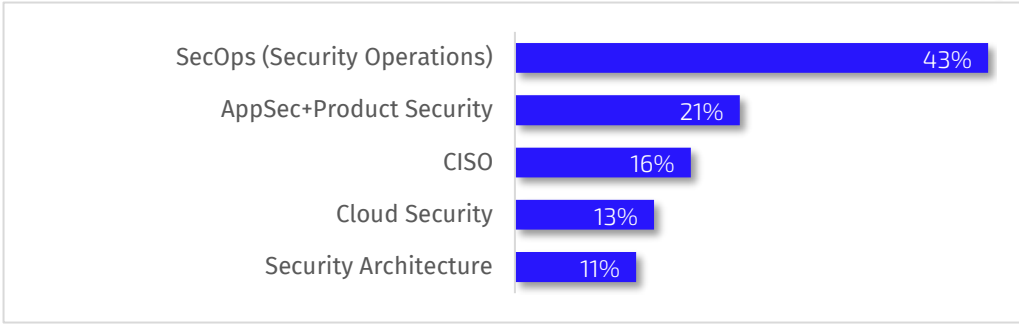

Figure 10: "Citing a large number of agents already in the system" by Role

Challenges Faced in Detecting and Responding to Cloud-Based Attacks

The most frequently encountered challenges that organizations face in detecting and responding to cloud-based attacks are alert fatigue due to high volume of notifications (46%) and high volume of false positives (45%), as seen in Figure 11. Fragmented visibility due to too many separate tools is the third biggest challenge (44%), particularly for CISOs (61%) and those who hold roles in cloud security (57%), as seen in Figure 12.

Other challenges encountered frequently include context correlation due to difficulty in correlating data from different layers (42%), cross-platform alerts due to inability to correlate security alerts across the cloud platform (37%), and slow response to security incidents due to input from multiple teams (34%).

So, while it's clear that noisy alerts pose a significant challenge for security teams around detecting and responding to threats, it is also apparent that duplicates and blind spots resulting from fragmentation of teams and tools are a major problem too.

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

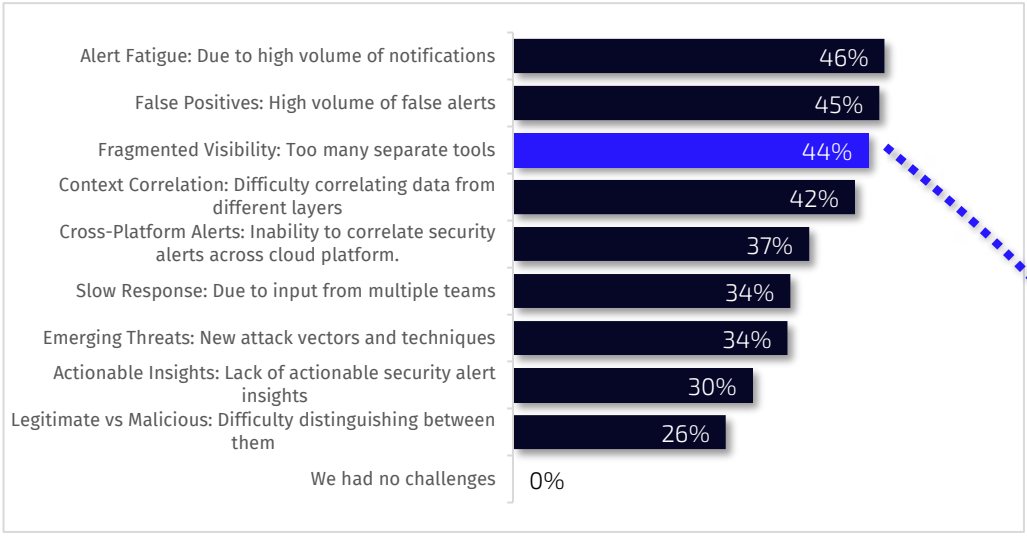

Figure 11: Challenges Faced in Detecting and Responding to Cloud-Based Attacks

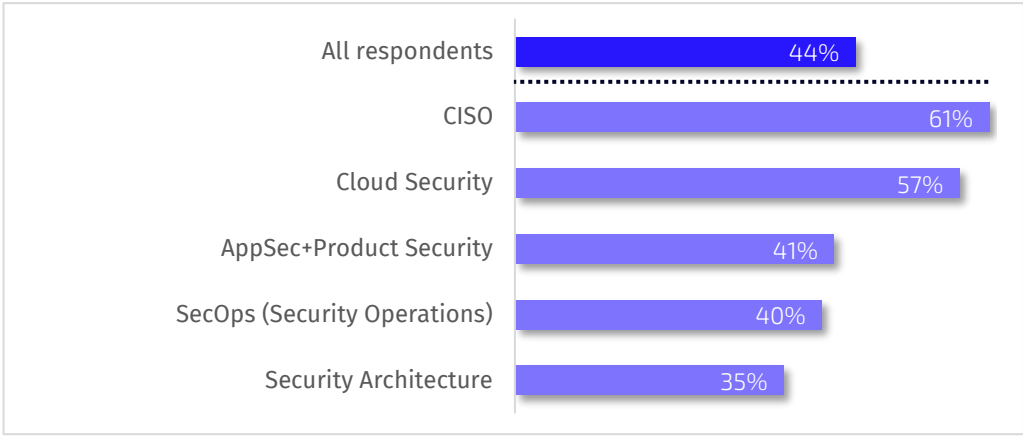

Figure 12: "Fragmented visibility" by Role

Time Spent Correlating Alerts and Information from Different Security Tools During Cloud Security Incidents

All of the respondents estimate that they spend anywhere between 12 hours to 30 days on correlating alerts and information from different security tools during a cloud security incident, with a significant majority (74%) spending 1-7 days on this task.

A small portion of respondents estimate that they spend 12-24 hours on correlating alerts (13%), and an equally small portion spend 7-30 days (13%), making **the overall average of time spent on correlating alerts 7.7 days**. Notably, no respondents reported spending more than 30 days on this task.

Given that only 13% of organization are successfully correlating alerts across different security tools, this finding indicates that there is a significant gap in visibility and response coordination. Many organizations rely on multiple security tools but struggle to integrate and unify their data, leading to missed threats and slower incident response. The inability to correlate alerts effectively means that security teams spend more time manually investigating incidents, increasing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) – highlighting the potential for automation to create a single attack story.

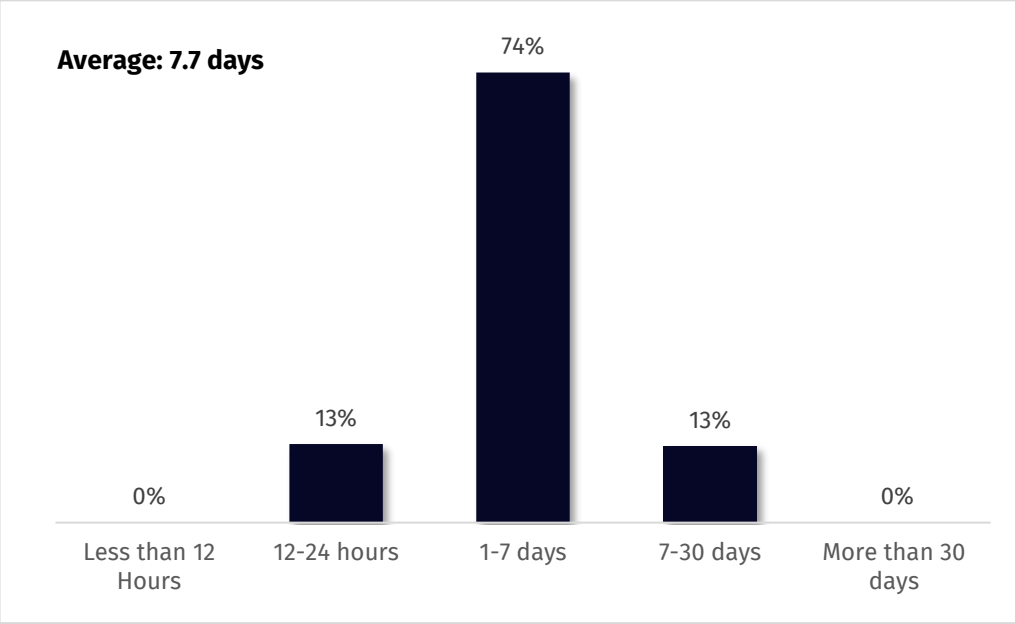

Figure 13: Time Spent Correlating Alerts and Information from Different Security Tools During Cloud Security Incidents

Impact of Contextualizing Alerts into a Single Attack Story on Response Time to Cloud-Security Incidents

An overwhelming majority of respondents (92%) either agree (57%) or strongly agree (35%) that tools that contextualize alerts into a single attack story can help reduce their response time to cloud-runtime security incidents. Only a small portion of respondents are neutral (7%) or disagree (1%) with the notion that contextualizing alerts can improve response time.

This strong consensus on the benefits of context in improving incident response efficiency is unsurprising, given that most organizations spend an average of 7.7 days on correlating alerts and information from different security tools during a cloud security incident (as seen in Figure 13) – which is less than ideal.

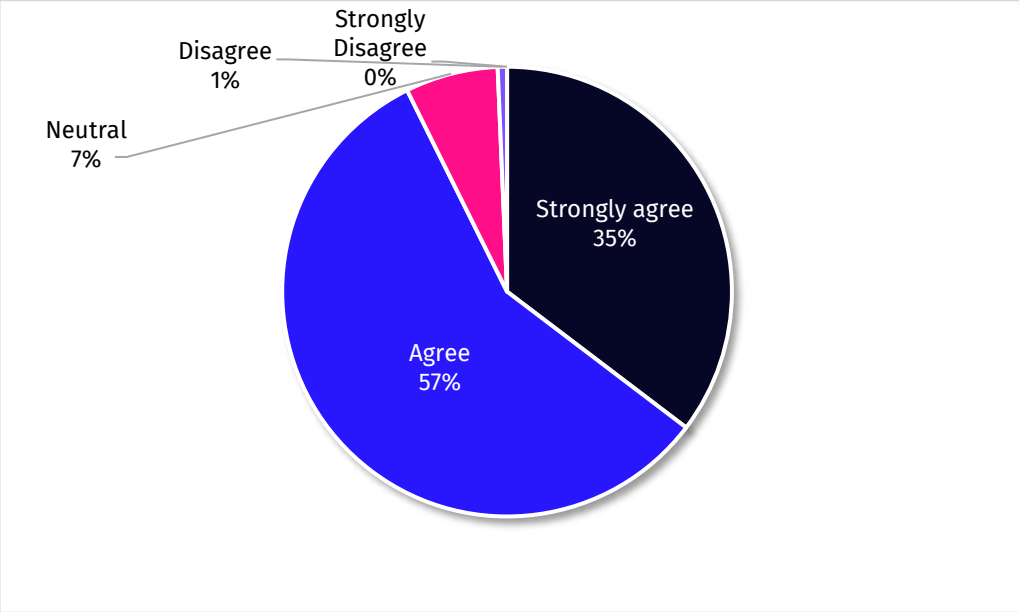

Figure 14: Impact of Contextualizing Alerts into a Single Attack Story on Response Time to Cloud-Security Incidents

Challenges in Reducing MTTD and MTTR in Current Cloud Runtime Security Setup

When asked about factors that impede their efforts to reduce MTTD and MTTR in their current cloud runtime security setup, respondents cited challenges around context, integration, coordination, automation and visibility.

The most significant challenge reported by 53% of respondents is the lack of contextualized alerts, followed by the overwhelming number of false positives (47%) and integration issues with existing security tools (45%). Other challenges include difficulties coordinating information flow between teams (42%), insufficient automation in response workflows (42%), a constantly evolving threat landscape (39%), and limited visibility into runtime environments (37%).

Notably, no one claimed they have no challenges at all, which reflects the level of difficulty faced by security teams as they endeavor to improve detection and response time to security incidents in the cloud.

This finding therefore confirms that enhancing alert context is key to improving MTTD and MTTR, followed by a desperate need to reduce false positives.

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

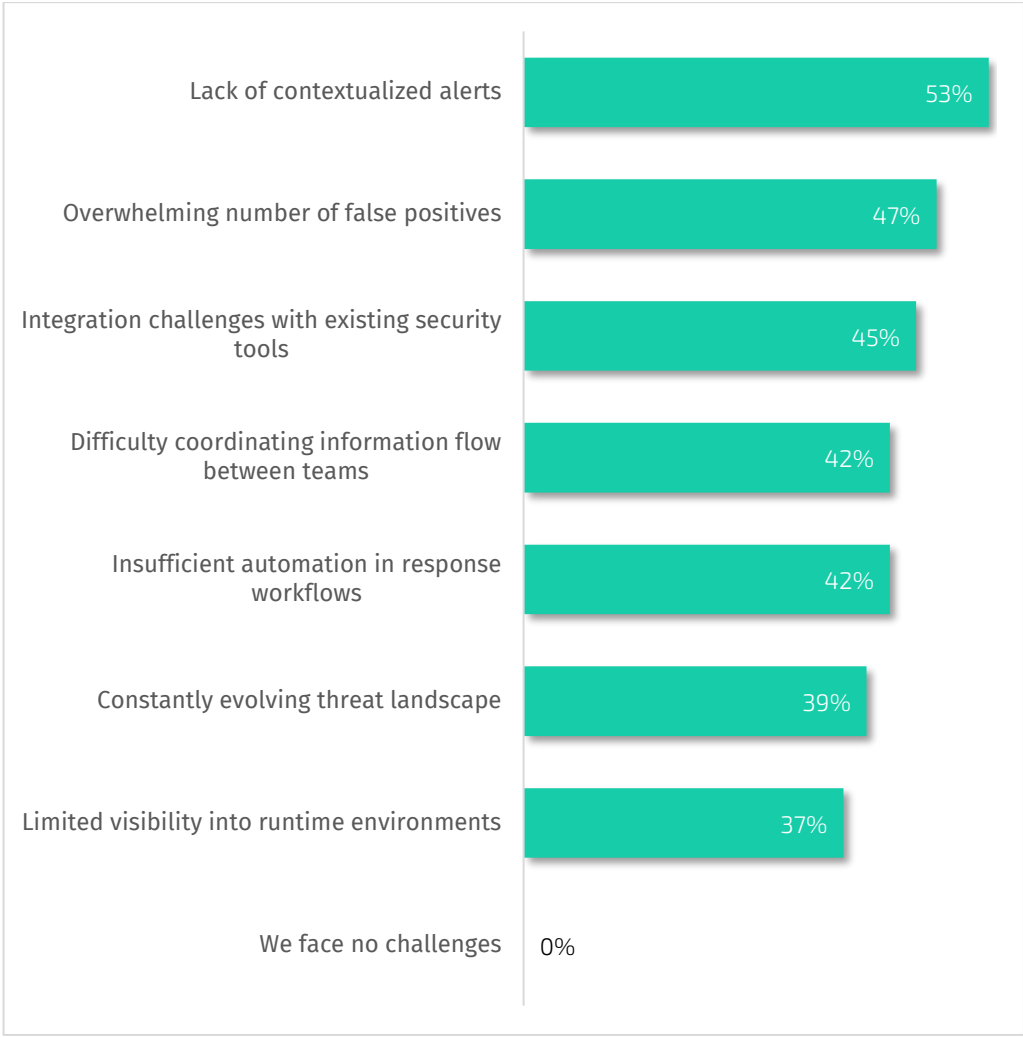

Figure 15: Challenges in Reducing MTTD and MTTR in Current Cloud Runtime Security Setup

Most Difficult Team to Work with During Security Incidents

The majority of respondents (38%) say that the Cloud Security team is the most challenging to collaborate with during security incidents, followed by the Platform team (31%), DevOps (13%) and Developers (10%). The AppSec team appears to be the least challenging to work with (8%), indicating that application security processes are more streamlined and embedded within development cycles.

This finding sheds light on collaboration challenges in cloud security: The fact that 38% of respondents struggle to collaborate with the Cloud Security team suggests that security processes may be too siloed, resulting in a lack of clear communication channels with other teams; and the fact that 31% of respondents find the Platform team difficult to work with, indicates that infrastructure management and security alignment may not be fully optimized.

In other words, SecOps – particularly SOC team responders – often face communication gaps with modern cloud-native teams, largely due to organizational silos. These silos can hinder their ability to meet key performance indicators like MTTD and MTTR. Bridging this gap calls for a shift toward cloud-native security models that enhance visibility, streamline automation, improve threat detection, and foster stronger cross-team collaboration.

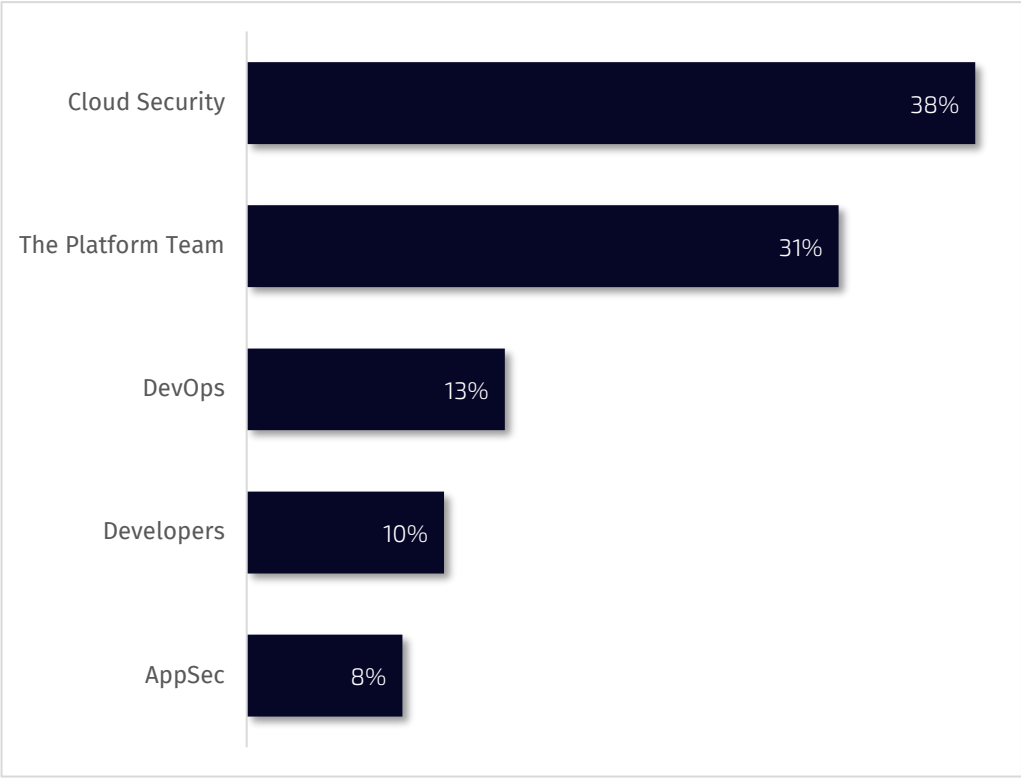

Figure 16: Most Difficult Team to Work with During Security Incidents

Teams Responsible for Detecting and Responding to Cloud-Based Attacks

The survey reveals that most organizations (63%) have a dedicated team in-house which is responsible for detecting and responding to cloud-based attacks (Figure 17). The fact that they favor a dedicated team in-house for this purpose demonstrates that they understand that cloud-native attacks are different from traditional security threats. This is likely the reason they choose to invest in a dedicated Cloud Security team rather than enlarge and upskill the traditional Security Operations Center (SOC) team, especially given that SOC personnel say that the Cloud Security team is the most difficult to work with during security incidents, as seen in Figure 16.

Only a third of respondents (31%) reported that detecting and responding to cloud-based attacks is handled as part of the SOC team, while a small portion (6%) rely on a managed SOC service (MDR).

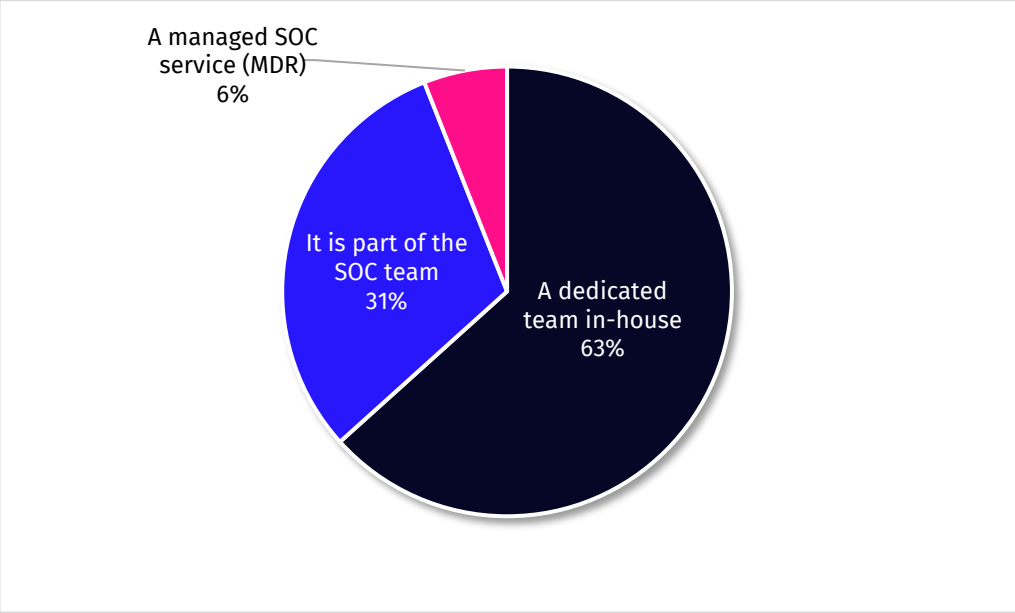

Figure 17: Teams Responsible for Detecting and Responding to Cloud-Based Attacks

Current Size & Future Growth Plans of the Team Dedicated to Threat Detection and Response to Cloud Runtime Attacks

The size of the team dedicated to threat detection and response to cloud runtime attacks tends to be influenced by a balance between operational needs (which, in this case, is typically 24/7 on-call rotations) and budgetary constraints. **The fact that 69% of organizations currently have teams of five or more (as seen in Figure 18) reflects the increasing challenges of cloud-native security in runtime.** The average team size is 5.1 members, with the largest proportion (53%) having teams of 5-6 members. Smaller teams of 3-4 members make up 30%, while 16% have teams with 7 or more members, and only 1% have a team of 2 members.

Logically, as the number of attacks grows, so does the number of responders needed. But with the correct solution in place – which provides explainability (i.e., observability and context) and enables automated responses – it is feasible that the sweet spot for the team size can remain small, rather than keep growing.

The data reveals, however, that **92% of the organizations surveyed are, in fact, planning to expand their teams: 53% will do so in 2025, while 39% will do so at a later date** (Figure 19). This indicates that the majority organizations are focused on team growth for enhanced cloud security.

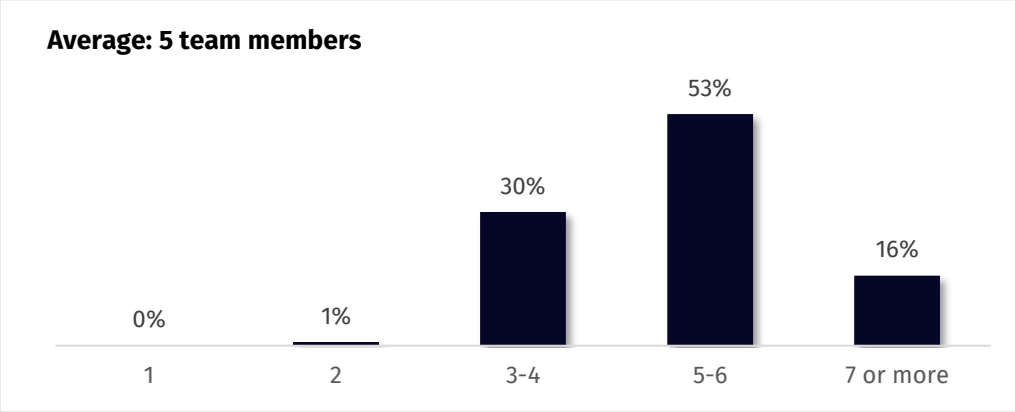

Figure 18: Size of the Team Dedicated to Threat Detection and Response to Cloud Runtime Attacks

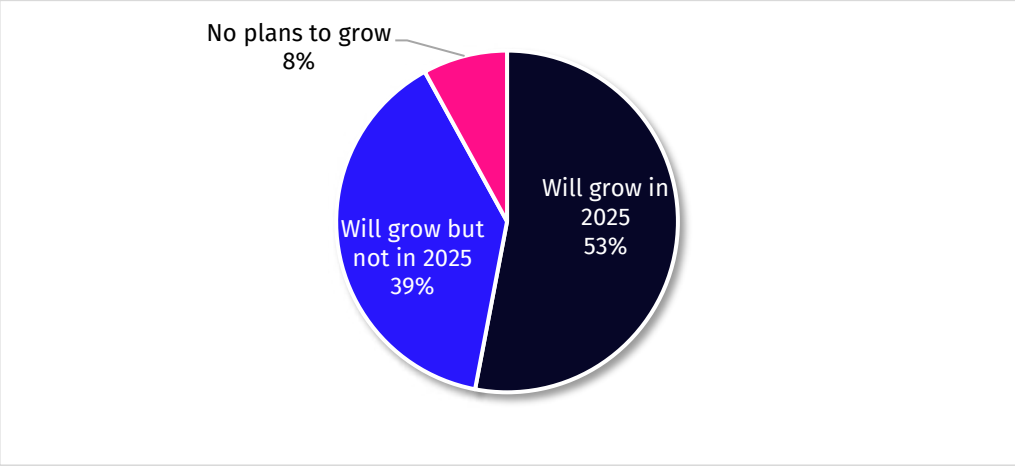

Figure 19: Plans to Grow the Team Dedicated to Detecting and Responding to Runtime Attacks

Demographics

Industry, Role, Job seniority, Company size

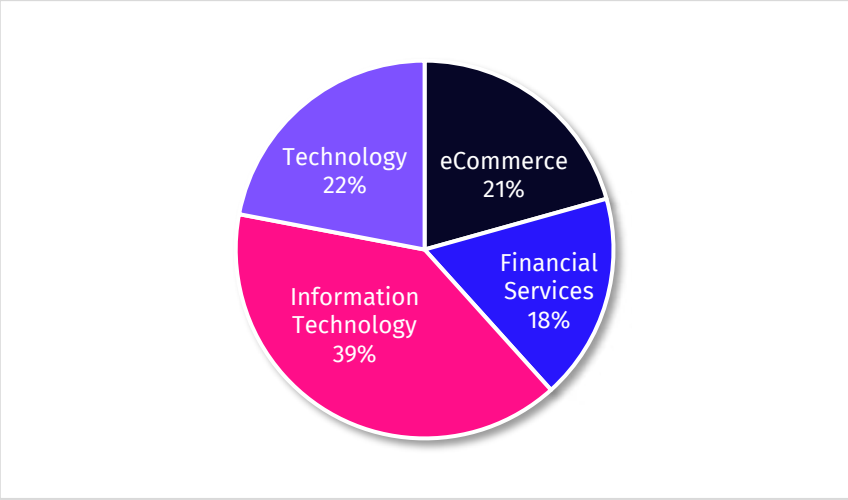

Figure 20: Industry

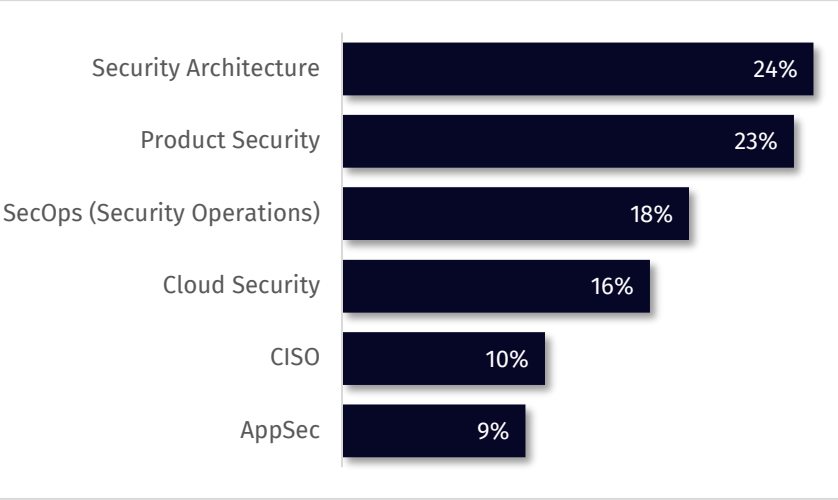

Figure 21: Role

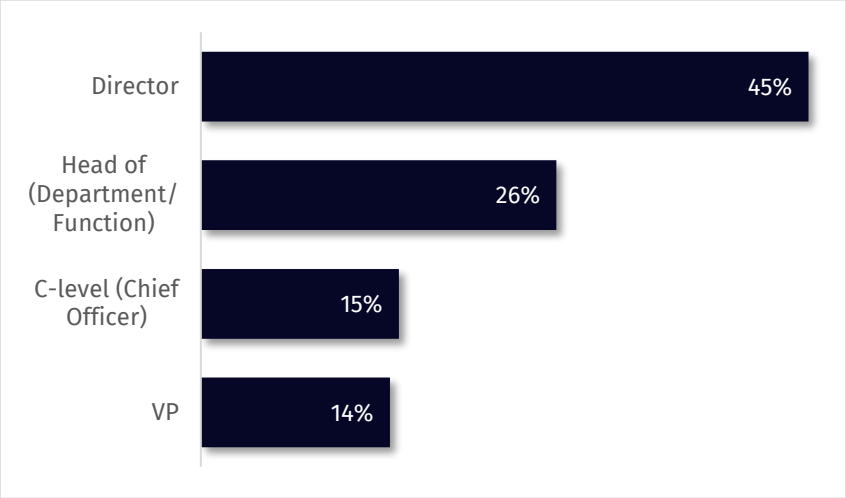

Figure 22: Job seniority

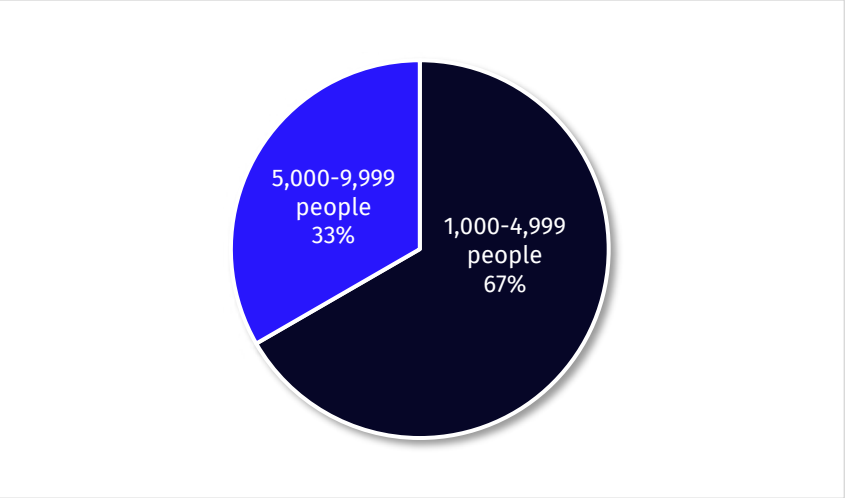

Figure 23: Company size

Technologies/Approaches Used, Cyber Attack Frequency Change, Cloud-Based IT Percentage

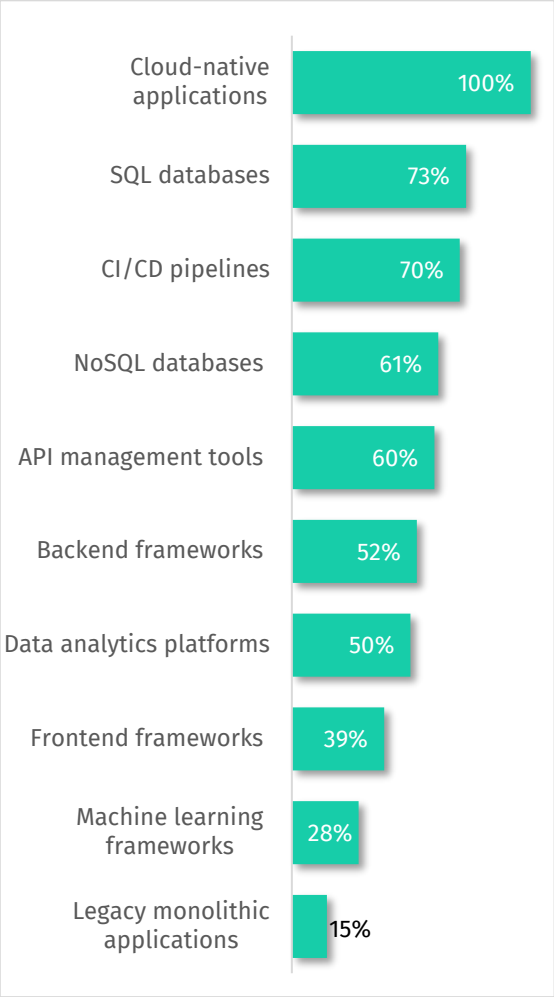

Figure 24: Technologies/Approaches Used

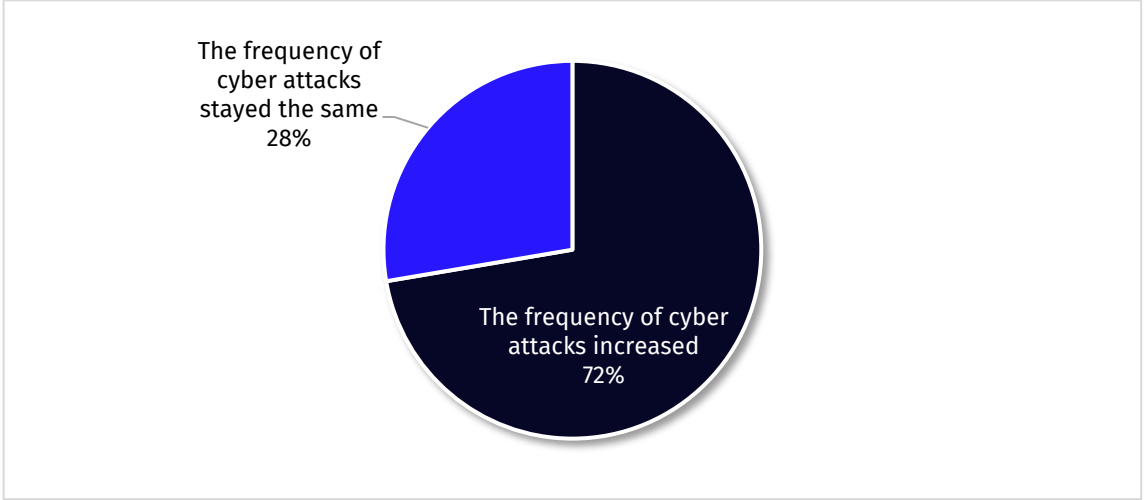

Figure 25: Cyber Attack Frequency Change (Last 12 Months)

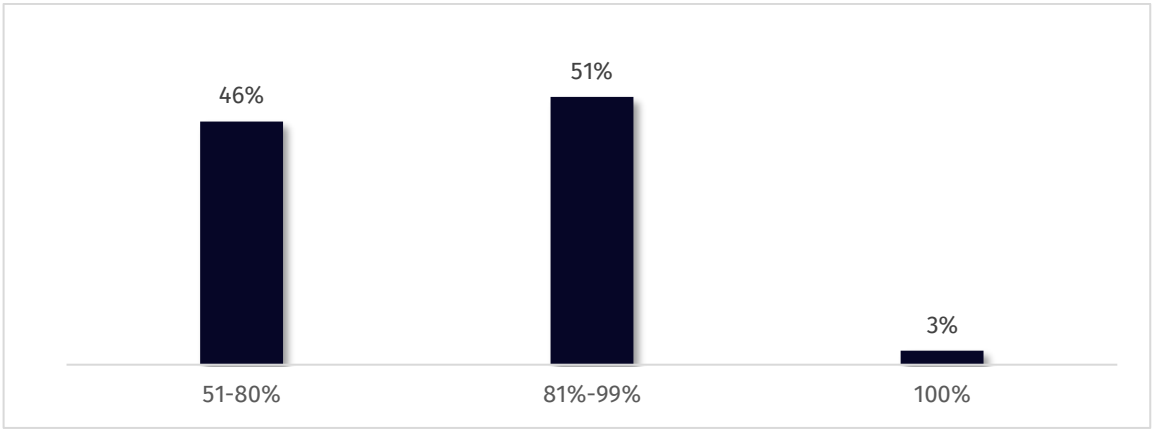

Figure 26: Percentage of Cloud-Based IT

About ARMO

ARMO is a Cloud Runtime Security company. It is the first open-source based, runtime-powered platform for detecting and responding to cloud application behavior.

ARMO Platform reduces the risk of cloud attacks by using runtime insights to minimize cloud attack surfaces. It detects and responds to cyberattacks in real-time, and provides clearly explainable attack stories without overwhelming teams with alerts. ARMO Platform helps DevOps, security, and platform teams by filtering out unnecessary alerts, freeing them up to focus on the most important threats and address real risks.

ARMO Platform has multiple deployment options: It is available as a SaaS and can be deployed on-premises (including in air-gapped environments).

ARMO's open-source project, Kubescape, is the fastest-growing CNCF cloud security solution – used by over 25,000 companies, and in more than 100,000 high-scale cloud environments worldwide.

Watch ARMO in Action

For more information, please visit us: