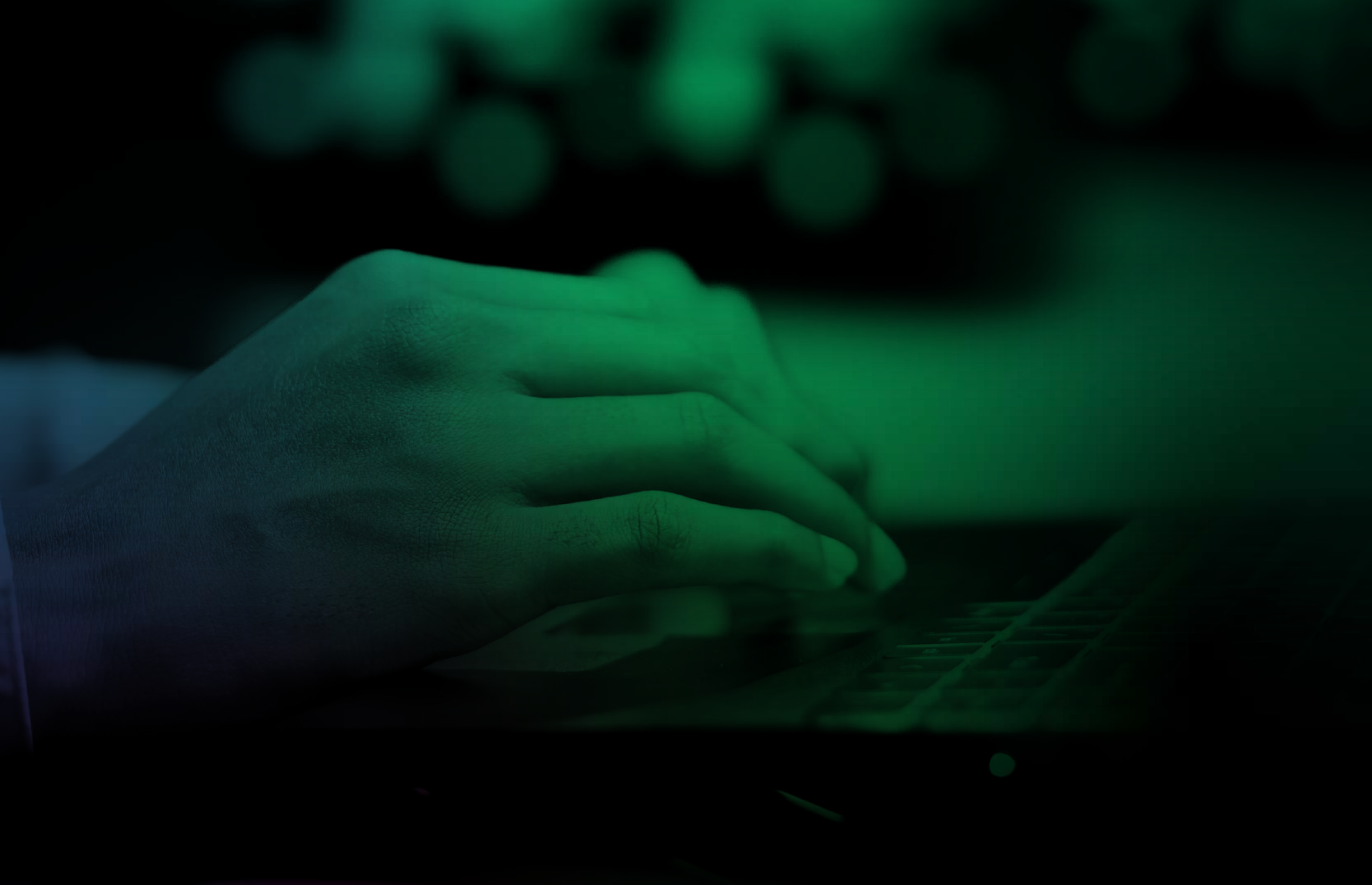
mesoform

# Mesoform;
# State of the Union 2023

Unveiling the interplay of DevOps, SRE, and Cybersecurity from 2023 in Mesoform's state of the union



# Table of Contents

# INTRODUCTION

*We know this is a vast coverage of IT and as a result, the state of the union is a large document to consume. So as guidance we recommend to use it for reference and digest by first reading the document's main introduction and two primary section intros. Then work out which specific sub-sections you're interested in from the contents and go from there; finishing with the section summary and final conclusions since these will give you insights into any other specific areas that may be of interest.*

In the ever-evolving landscape of technology, achieving seamless collaboration between Development and Operations (**DevOps**) and Site Reliability Engineering (**SRE**) has become a cornerstone for organisational success.

Mesoform's State of the Union embarks on a comprehensive exploration of the union of the intricate threads that bind DevOps and SRE principles and their interplay with the ever-growing concern of cybersecurity. Beginning with an examination of Organisational and Team Culture, we scrutinise the impact of flexible work arrangements, the delicate balance between cultural practices and security, the indispensable role of leadership, and the catalysing force of diversity in fostering innovation.

Transitioning into Cloud Usage, the report then unravels the strategic choices made by high-performing teams, shedding light on the transformative benefits of loosely-coupled architecture and the strategic utilisation of cloud infrastructure.

Delving into the Impact of Software Delivery Performance and Operational Performance, the narrative navigates through the critical landscape of supply chain security, the integration of security measures into continuous integration pipelines, and the evolving metrics defining software delivery performance.

It then explores the non-linear impact of Site Reliability Engineering Practices, the resilience of Platform Teams through Platform Engineering, the strategic insights unveiled by recent research, and the crucial choices organisations face in adopting platform engineering principles. Conclusively, the journey leads into the realm of cybersecurity, dissecting the OWASP Top Ten Project, vulnerability exploitation, and the mitigation strategies crucial for defending against emerging threats.

# DEVOPS AND SRE

To begin with, we start by looking at reports focused on DevOps and site-reliability engineering. Studies, for example, which used the Supply Chain Levels for Secure Artefacts (SLSA) framework and the National Institute for Standards and Technology's Secure Software Development Framework (NIST SSDF) to explore technical and non-technical aspects related to software supply chain security. It was a study performed by Google and showed one of the main industry focus was on securing the software supply chains and the importance of good application development security practices.

Other studies, like those done by Puppet for their State of DevOps Report 2023, provided insightful data and trends regarding the adoption of DevOps practices across various industries and highlighted the continued importance of collaboration, automation, and continuous delivery in driving successful software development and deployment strategies.

**An important finding to note is that general consensus showed that despite the prevalence of DevOps practices across organisations, nearly 80% remain in the middle of their DevOps journey, experiencing varying degrees of success at the team level but little across the entire organisation.**

Another of the key findings of all of the surveys was that organisations that prioritise establishing security practices in their development processes experienced various additional benefits. Firstly, such teams reported reduced developer burnout, which is crucial for maintaining a healthy and productive work environment.

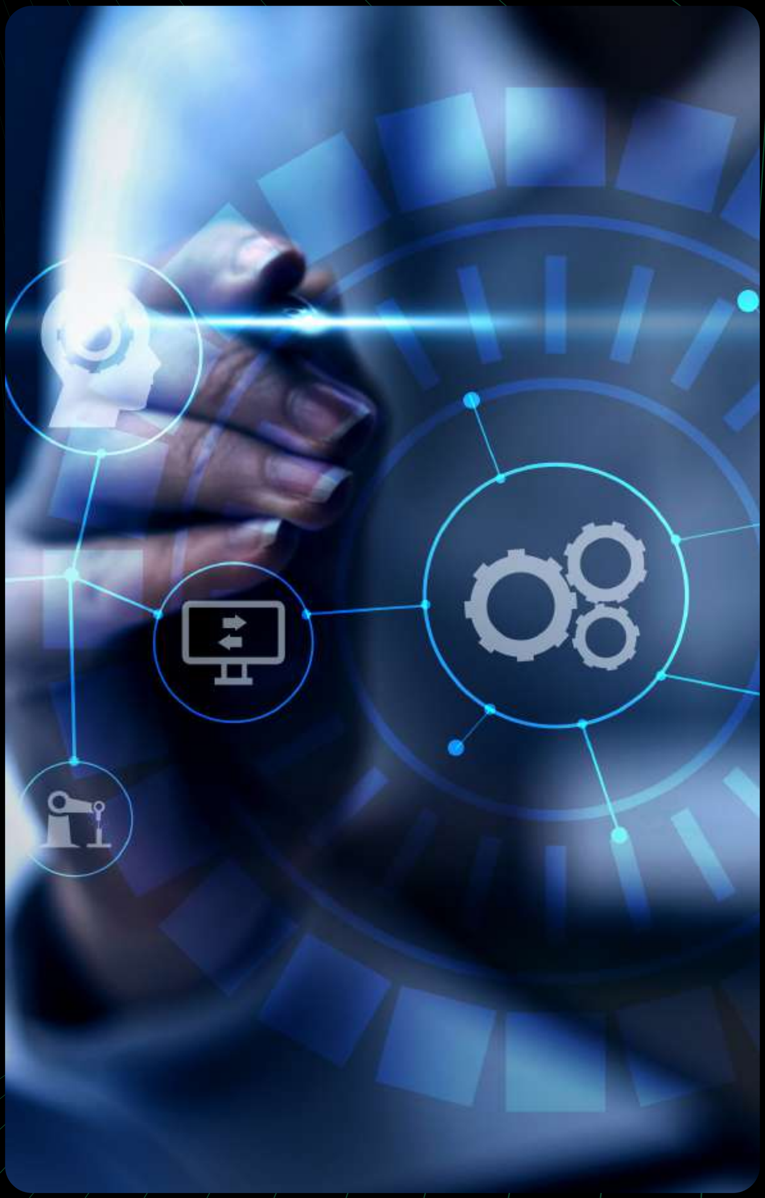
Teams with low levels of security practices were found to have 1.4 times greater odds of experiencing high levels of burnout compared to teams with high levels of security practices. These teams were also significantly more likely to recommend their team to others. Indicating that employees in organisations with strong security practices are more satisfied and content with their work environment, leading to a higher likelihood of recommending it to potential employees or colleagues.

Furthermore, the studies highlighted that security practices, particularly those related to SLSA, positively correlated with both organisational performance and software delivery performance. In other words, **organisations that placed an emphasis on securing their software supply chain experienced improved overall performance and efficacy in delivering software products.**

However, it was noted that the full potential of these security practices could only be realised when combined with strong continuous integration capabilities. Continuous integration allows for the automation and frequent integration of code changes into the main development branch (where software release, in some form or another are done). This helps catch security vulnerabilities early in the development process.

Interestingly, the results emphasised that the biggest predictor of an organisation's application-development security practices was not technical but cultural. Organisations with high-trust, low-blame cultures that emphasised performance were 1.6 times more likely to adopt emerging security practices compared to organisations with low trust and high blame cultures that focused on power or rigid adherence to rules.

Lastly, analysis shows early evidence suggesting that pre-deployment security scanning was effective in identifying vulnerable dependencies. By detecting and addressing these vulnerabilities before deployment, organisations could reduce the number of security issues in their production code, leading to more secure software products.



Overall conclusions underline the importance of securing the software supply chain and the various benefits that organisations can achieve by adopting good application development security practices. Cultural aspects, such as trust and blamelessness, were highlighted as significant factors in driving the adoption of security practices, complementing technical measures like the SLSA framework and continuous integration capabilities.

# Organisational and Team Culture

In the fast-evolving landscape of the Information Technology (IT) industry, the relentless pursuit of innovation and efficiency has revolutionised the way businesses operate. Amidst this digital transformation, the well-being of IT teams has emerged as a critical aspect that directly impacts their performance and overall organisational success. Burnout, a state of chronic emotional and physical exhaustion, has become a pressing concern in IT workplaces. As companies strive to optimise their IT operations, it is crucial to understand the relationship between burnout and good DevOps and security practices to foster a resilient and productive workforce.

**Several key variables were identified as impactful factors on organisational performance. These variables can be categorised into the following areas:**

- **High-Trust and Low-Blame Cultures**: Organisations with cultures that foster high levels of trust and promote a blameless environment tend to have higher organisational performance. In such cultures, individuals feel more comfortable taking risks, learning from mistakes, and collaborating effectively.

- **Supportive Teams:** Organisations that provide adequate funding and leadership sponsorships to support their teams tend to experience higher levels of organisational performance. This support enables teams to carry out their tasks efficiently and effectively.

- **Team Stability and Positive Perceptions:** Teams with stable compositions and positive perceptions about their own teams, such as the likelihood of recommending their team to others, are associated with higher organisational performance. This suggests that cohesive and satisfied teams contribute to better outcomes.

- **Flexible Work Arrangements:** Companies that offer flexible work arrangements tend to see high levels of organisational performance. Such arrangements can enhance employee satisfaction, work-life balance, and productivity.

# How to Measure Company Culture

- Employee Surveys
- Exit Surveys
- Focus Groups

- Business needs scorecard (BNS)
- Organisational culture assessment instrument (OCA)
- Behavioural observation scale (BOS)
- 3rd party culture measurement tools

## Flexible work arrangements

Flexible work models have a significant impact on employee well-being and team dynamics. Industry research confirms that organisations with flexible work arrangements experience decreased employee burnout and an increase in the likelihood of employees recommending their teams as great places to work. Last year's studies not only replicated these findings but also shed light on additional factors contributing to burnout.

Stable teams and flexible work arrangements were found to be associated with reduced burnout among employees. Furthermore, Net Promoter Score (NPS) was measured to indicate whether employees would recommend their teams to others. The results showed that team NPS was positively influenced by perceived leadership buy-in. In alignment with the burnout findings, a generative culture, stable team structures, and flexible work arrangements were associated with employees being more inclined to recommend their teams to friends or colleagues.

## Cultural practices and security

By reducing barriers to following security practices, organisations can make it easier for developers to prioritise security alongside other development tasks. This involves creating a culture that values security efforts, implementing the right infrastructure to support security processes, and integrating security into the development workflow.

Companies that adopted good security practices were shown to have various positive outcomes as a result. Such as a lower chance of security breaches, service outages, and performance degradation. Additionally, organisations with established security practices reported less burnout among team members and increased satisfaction with their workplace.

**Companies which performed best in these areas generally did so by focusing on both cultural and technological aspects. Below are some of the key factors of top performing organisations:**

## Cultural Factors

Organisations with a generative **culture**, characterised by cooperation, risk-sharing, and learning from mistakes, are more likely to establish and embrace security practices. This culture encourages software engineers to be proactive about supply chain security, rewards security efforts, and reduces perceived risks of reporting potential security issues.

## Technological Factors

Infrastructure plays a crucial role in supporting security practices. Having systems for source control, continuous integration (CI), and continuous delivery (CD) makes tasks like vulnerability scanning and manual code reviews easier to conduct. CI/CD systems ensure consistent scanning and analysis of code commits, enhancing the security process.

## Flexibility in Work Arrangements

Supporting flexible work arrangements, such as remote work, can positively impact security practices.

## Cloud Use

Embracing cloud services, whether public or private, can contribute to better security practices.

## CI/CD Usage

Implementing **CI/CD** is a significant driver of security practices. CI/CD provides the integration platform for many security measures and enables faster and more efficient security scanning.

## Organisational Size

Larger organisations tend to have higher security scores, possibly due to having more resources and mature security practices.

# 9 Data Security Best Practises to Protect Data Privacy from 2023

- ✓ Identify and Categorise Sensitive Data
- ✓ Define a Data Usage Policy
- ✓ Track Who Has Access to Sensitive Data Protect Data Physically
- ✓ Document Your Cybersecurity Policies
- ✓ Adopt a Risk-Based Data Protection Strategy
- ✓ Employee Security Training
- ✓ Implement Multi-Factor Authentication
- ✓ Use Data Encryption

## Leadership is critical

The perceptions of leadership buy-in was another significant finding and showed that employees working in such environments were less likely to expect major errors, indicating a positive outlook on their organisations. Employees were asked to predict the level of support their teams would receive over the next year. Higher perceived leadership buy-in, reflected in financial support, resource allocation, and sponsorships, was correlated with high-performing organisations.

This led to a number of key points to consider:

→ Effective leadership plays a vital role in the success of DevOps initiatives. Leaders who understand the value of DevOps and its impact on organisational outcomes are more likely to provide the necessary resources, support, and buy-in from stakeholders.

→ They create a culture that encourages collaboration, experimentation, and continuous improvement. Strong leaders also champion the adoption of DevOps practices, facilitate knowledge sharing, and empower their teams to make decisions autonomously.

→ By fostering an environment of trust and psychological safety, leaders can unleash the full potential of their teams, resulting in higher performance and innovation.

## Diversity is important

As with wider society, cultural diversity points showed significant importance last year whereby representative representations of employees from underrepresented groups revealed some disparities. Diversity encompasses various dimensions, including but not limited to gender, race, ethnicity, age, educational background, and professional experiences; and employees from these groups reported spending more time on unplanned work, irrespective of their organisation's performance level. Additionally, they reported higher levels of burnout compared to employees from non-underrepresented groups.

Research consistently shows that teams with diverse members tend to be more high-performing and achieve better business outcomes. They bring together different perspectives, knowledge, and problem-solving approaches, fostering creativity and innovation. They are more likely to challenge assumptions, identify blind spots, and generate a wider range of ideas and solutions.

Furthermore, diverse teams can better understand and serve a diverse user base, leading to improved customer satisfaction and market competitiveness.

Therefore team leads should be vigilant about workload distribution to ensure fair allocation among team members because creating an inclusive environment where diverse voices are heard and valued is essential for leveraging the full potential of team members and driving success in DevOps.

These findings highlight the crucial need to create healthy and inclusive work environments at both the organisational and team levels. While we continue to emphasise the importance of culture, we acknowledge that transforming or improving an organisation's culture is a challenging endeavour. Our recommendation is for organisations to first understand their employees' experiences and then invest resources in addressing culture-related issues as part of their DevOps transformation efforts.

## Cloud Usage

Something which is abundantly clear and has been for a number of years - High-performing businesses use cloud infrastructure. What studies have shown last year, is that companies with software initially built on and for the cloud tend to have the highest organisational performance. Using cloud platforms, whether private, public, hybrid, or a mixture of clouds, is associated with better organisational performance than relying solely on on-premises servers.

Furthermore, organisations that use multiple public clouds are 1.4 times more likely to have above-average organisational performance than those that don't. Embracing multiple public cloud providers allows teams to leverage different capabilities and practices, which can contribute to improved performance.

Cloud usage was also shown to have a positive impact on supply chain security practices, such as implementing Supply Chain Levels for Secure Artefacts (SLSA). Cloud providers often offer building blocks and encourage automation, leading to enhanced security practices that, in turn, contribute to higher organisational performance.

## High-performing teams use cloud infrastructure

Feedback from respondents of the surveys showed some clear characteristics and behaviours of high performing teams in relationship to their usage of Cloud computing:

- High-performing teams are significantly more likely to use cloud infrastructure for their applications than low-performing teams.
- High-performing teams recognise the advantages of utilising cloud infrastructure for their applications. Cloud infrastructure provides scalability, flexibility, and cost-effectiveness, allowing teams to easily adapt to changing requirements and handle increased workloads.
- By leveraging cloud services, such as virtual machines, storage, and databases, teams can quickly provision resources, optimise performance, and enhance overall productivity.
- The cloud also enables collaboration among team members, regardless of their physical locations, fostering effective communication and seamless workflow.

## The Benefits of Loosely-Coupled Architecture

Loosely-coupled architectures are commonly observed in software deployed to the cloud and adopting microservices, managing numerous services. However, it's important to note that loose coupling goes beyond merely counting the number of services in a system. Components in such architectures can be independently deployed, allowing teams to develop, test, and deploy their services without the burden of extensive coordination between teams.

In practice, loose coupling is not restricted to a specific architectural style; rather, it denotes the ability to make changes in one part of the system without affecting other parts. This flexibility allows organisations to divide their work among different teams, enabling individual teams to make progress without relying heavily on coordination with other teams.

Teams that prioritise building software with loosely-coupled architectures experience several advantages, impacting various aspects of their performance. Loosely-coupled systems contribute to strong stability, reliability, and throughput in software delivery. Additionally, teams adopting this architectural approach are more likely to recommend their workplace to others.

The research from last year indicates that teams requiring deep integration testing with other services before deploying their software may not have fully achieved loose coupling. These teams could benefit from improving interfaces and isolation between systems, with improved "testability" of services being a crucial aspect of achieving loose coupling.

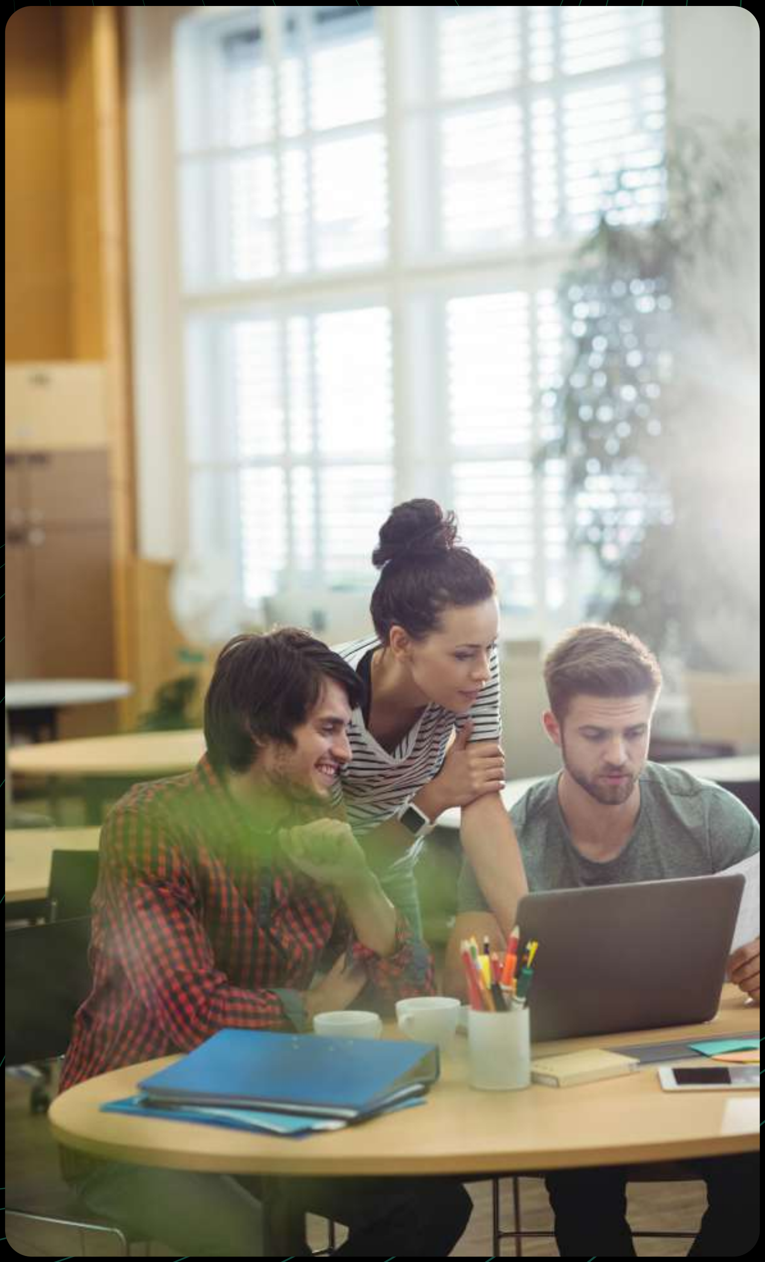
On the contrary, cohesive and stable teams that adopt a loosely-coupled architecture are more likely to follow software development practices that encourage continuous improvement. For example, Site Reliability Engineering (SRE) practices, such as setting reliability goals and regular reviews to revise reliability targets, align well with loose coupling and further support organisational performance.

Loosely-coupled architectures also facilitate the scaling of teams within an organisation, as independent teams can increase their size without being overly dependent on other teams' coordination.

However, surprisingly, last year's research revealed that loosely-coupled architecture might contribute to burnout on teams, contrary to previous findings. The analysis suggests that stable teams with strong information flow typically experience lower levels of burnout. More research is needed to definitively understand this finding.

Furthermore, when security requirements are defined and controlled by a centralised security organisation, it may be challenging for teams to decouple their software from other teams. Therefore, shifting security concerns to the team most responsible for the application can yield significant benefits.

In conclusion, loose coupling of software services not only impacts technical aspects but also influences the socio-technical aspects of software development. Loosely-coupled architectures lead to loosely-coupled organisations, fostering a more distributed and scalable approach to development. **It is crucial for organisations to understand the potential benefits and challenges associated with loose coupling and consider its impact on overall performance and culture.**



## Essential Cloud Characteristics

Analysis of the reports emphasises the importance of cloud computing five essential characteristics, as defined by the National Institute of Standards and Technology (NIST).

Those characteristics are defined as:

- **On-demand self-service:** Consumers can provision computing resources as needed, automatically, without human intervention from the provider.

- **Broad network access:** Capabilities are widely available, and consumers can access them through various clients such as mobile phones, tablets, laptops, and workstations.

- **Resource pooling:** Provider resources are pooled in a multi-tenant model, with dynamic allocation and reassignment of physical and virtual resources based on demand.

- **Rapid elasticity:** Capabilities can be elastically provisioned and released to rapidly scale outward or inward with demand, allowing for unlimited provisioning at any time.

- **Measured service:** Cloud systems automatically control and optimise resource usage by leveraging metering capabilities for transparency and reporting.

The results confirm that organisations exhibiting these five characteristics of cloud computing experience better software delivery and operational performance. Furthermore, these characteristics set processes in motion that positively affect organisational performance as well.

The results also highlight that teams are increasingly adopting the five characteristics of cloud computing, with Resource Pooling seeing the largest increase of 14%, followed by a 5% rise in Rapid Elasticity, which was already the second most-used feature in the previous year.

## Multi-cloud

However, according to the Accelerate State of DevOps 2022 report, the use of hybrid and multi-cloud (and private) environments was having a negative impact on software delivery performance indicators like Mean Time to Restore (MTTR), lead time for changes, and deployment frequency, unless the respondents had high levels of reliability. This suggests that when teams have strong reliability practices in place, the negative impact of using hybrid and multi-cloud setups on software delivery performance can be mitigated. Tools which help close the gap and standardise experiences across different cloud providers will go a long way to ensuring reliability in both development practices, CI/CD and app performance.

The conclusion of the surveys emphasises the significance of reliability in technology teams and its impact on organisational success. Reliability goes beyond merely shipping code or delivering quality code; it involves ensuring that the services provided remain available, performant, and consistent with users' expectations over time.

# Impact of Software Delivery Performance and Operational Performance

High software delivery performance is beneficial for organisational performance only when operational performance is also high. Simply delivering quickly may not matter if the service cannot meet users' reliability expectations. **Organisations should focus on both speedy delivery and reliable operations to achieve optimal results.**

The research reveals that companies excelling in both inner and outer loop development have a significant advantage in shipping code faster and with higher reliability. Among the various capabilities contributing to high performance, version control, continuous integration (CI), continuous delivery (CD), and loosely-coupled architecture play a crucial role.

High-performing teams that meet reliability targets demonstrate 1.4 times higher usage of continuous integration compared to other teams. Continuous Integration, also known as CI, is an essential aspect of the outer loop development process. It involves automatically building an artefact and running a series of automated tests for every code commit. This process provides rapid, automated feedback to developers, enabling them to operate with increased confidence in their code. CI plays a pivotal role in efficiently moving code from a developer's workstation to production.

Furthermore, the study highlights that more organisations are adopting continuous delivery practices, with 11% of respondents reporting that they deploy on-demand or multiple times per day, but 69% between once per week and once per month; and respondents who make higher-than-average use of all the mentioned capabilities (version control, CI, CD, and loosely-coupled architecture) enjoy a remarkable 3.8 times higher organisational performance compared to those who do not prioritise these technical capabilities.

# Why Supply Chain Security Matters

Supply chain security is a critical aspect of software development and has become a major focus for many organisations in the industry. Initiatives like Supply Chain Levels for Software Artefacts (SLSA) and the NIST Secure Software Development Framework (SSDF) aim to enhance the security of software production processes and prevent malicious software updates.

Research has revealed some key findings regarding the adoption and impact of supply chain security practices:

→ **Adoption has already started:** SLSA and SSDF practices are seeing moderate adoption, but there is still room for improvement and wider implementation.

→ **Healthy organisational cultures lead the way:** Organisational culture plays a significant role in driving software development security practices. Higher trust and "blameless" cultures are more likely to embrace SLSA and SSDF practices compared to lower-trust cultures.

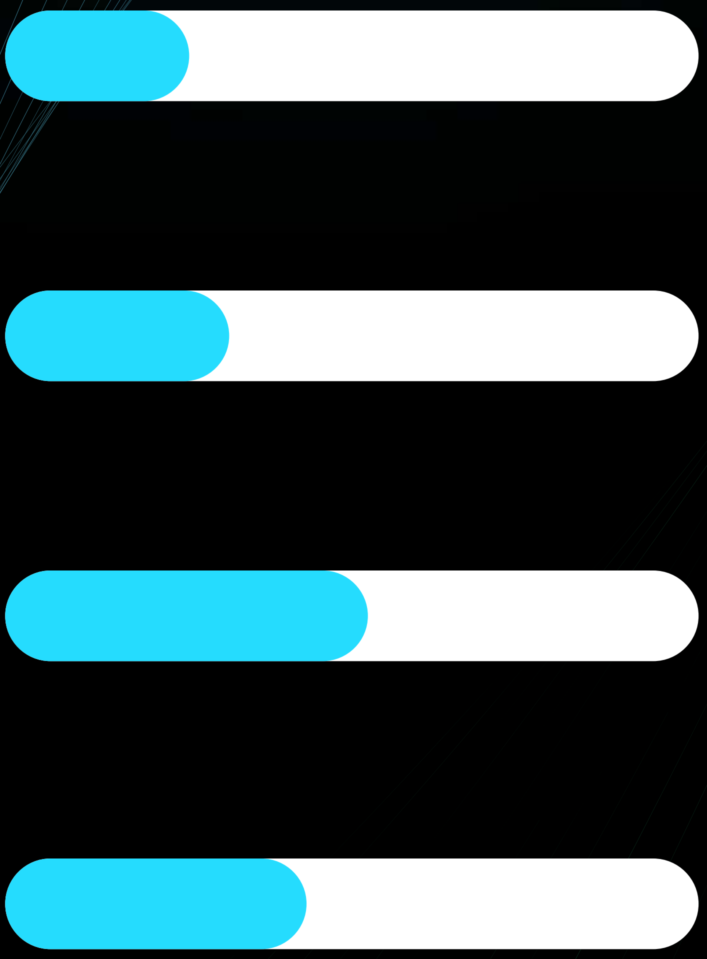
→ **Integration is crucial:** The adoption of technical aspects of supply chain security heavily relies on the use of continuous integration/continuous delivery (CI/CD) systems, which serve as integration platforms for many supply chain security practices.

→ **Unexpected benefits:** Implementing better security practices not only reduces security risks but also leads to additional advantages, such as reduced burnout among employees.

The impact of security practices on software development was assessed. While there are ongoing efforts to monitor vulnerabilities in software and third-party components, some security processes are perceived to slow down the development process. This indicates a need for improvement in security tooling and approaches to strike a balance between security and development speed.

Overall, the software industry is making strides in enhancing supply chain security, but there is still work to be done. **Organisations should prioritise security practices, foster healthy cultures, and leverage CI/CD systems to ensure secure and efficient software development processes.**

# High performers who meet reliability targets are...



**33%** more likely to use version control

**39%** more likely to practice continuous integration

**46%** more likely to practice continuous delivery

**40%** more likely to have systems based on a loosely-coupled architecture

## Developing from the trunk

Trunk-based development is a software development practice that involves continuously merging code changes, on “feature branches”, into the main trunk (the main copy of the code), avoiding long-lived feature branches. This practice complements continuous integration and has been proven to accelerate software delivery velocity over the years. Interestingly, research from last year showed a shift in demographics, indicating that experience matters when implementing trunk-based development. Respondents with less experience overall demonstrated less positive results in trunk-based development, experiencing decreased software delivery performance, increased unplanned work, higher error-proneness, and a higher change failure rate. On the other hand, individuals with 16+ years of experience who adopted trunk-based development witnessed increased software delivery performance, decreased unplanned work, reduced error-proneness, and a lower change failure rate.

## Software Supply Chain Security and Continuous Integration

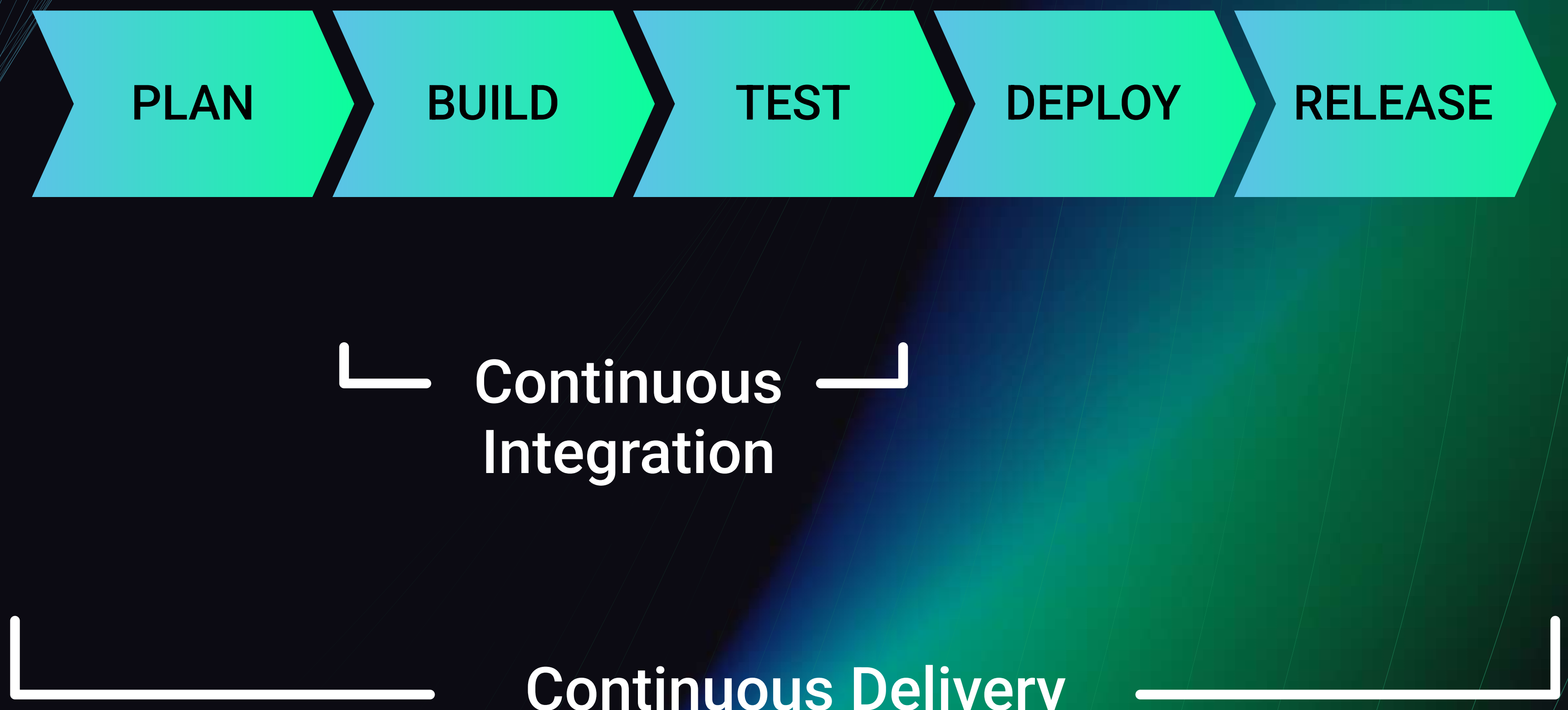
Implementing software supply chain security controls, such as those recommended by the SLSA framework, positively affects software delivery performance when continuous integration capabilities are firmly established in the supply chain.

Without continuous integration in place, security controls and software delivery performance might conflict with each other.

Continuous delivery (CD) is a software development practice enabling teams to deploy software to production at any time and ensuring it remains deployable throughout its lifecycle. It establishes a fast feedback loop that checks the quality and deployability of the system and prioritises fixing issues blocking deployment. Research consistently confirms that CD is a predictor of higher software delivery performance, especially when combined with other DevOps capabilities. Teams that adopt version control and continuous delivery are 2.5 times more likely to achieve high software delivery performance. However, CD may lead to more time spent on rework or unplanned work due to iterative changes driven by tighter feedback loops.

Additionally, interactions of CD were examined with other DevOps capabilities, such as trunk-based development and loosely-coupled architecture. Interestingly, it was found that when these capabilities are used together with CD, there might be a negative impact on a team's performance. Teams combining loosely-coupled architectures and CD are 43% more likely to anticipate higher error proneness. This suggests potential friction for teams striving to improve and emphasises the need for commitment to continuous improvement.

# Continuous Integration & Delivery



PLAN

BUILD

TEST

DEPLOY

RELEASE

Continuous Integration

Continuous Delivery

In conclusion, **both trunk-based development and continuous delivery contribute significantly to software delivery performance, but they require careful implementation and monitoring of their effects on the team's performance and overall outcomes.** Teams that persist through challenges and invest in the right practices are more likely to realise their full potential in terms of improved software delivery and operational performance.

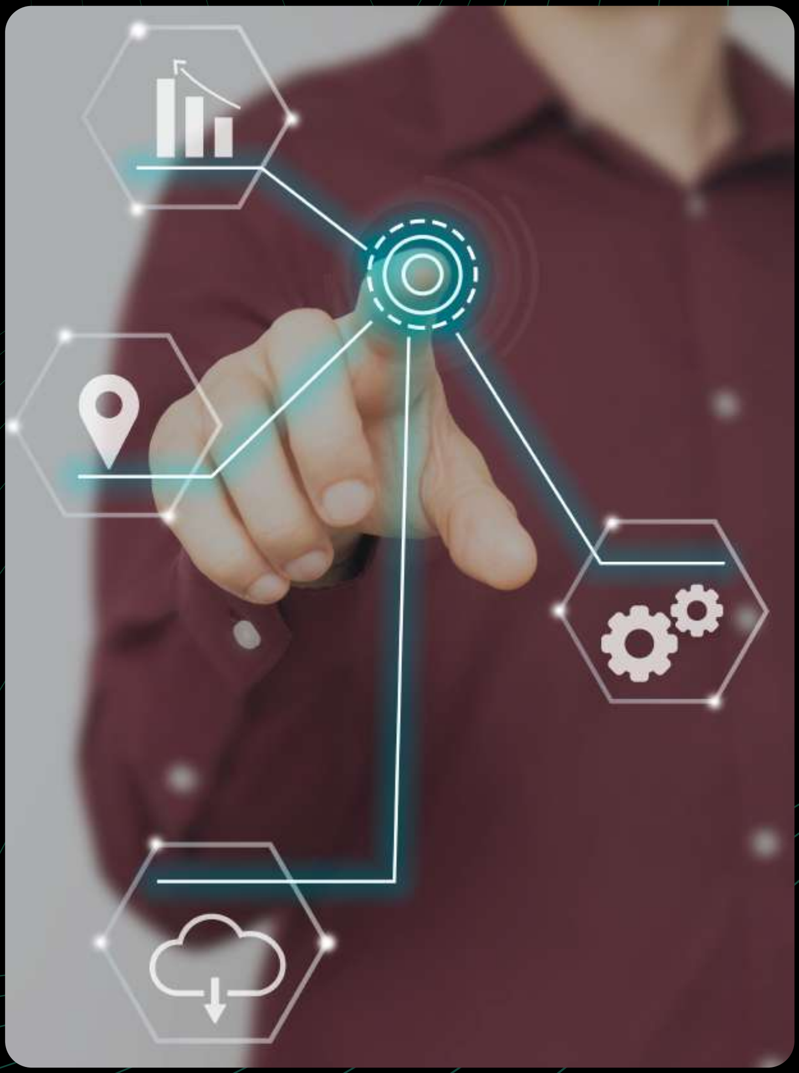
## Synergy of Technical Capabilities

Technical capabilities build upon one another, and the combination of various practices can amplify their ability to promote high levels of software delivery performance. For example, combining continuous delivery, loosely-coupled architecture, version control, and continuous integration can create software delivery performance that exceeds the sum of its individual parts.

Data from the reports emphasises the need for teams to continuously adapt and experiment with software development practices to identify what works best in their specific context. Continuous improvement is crucial for achieving higher organisational performance. Teams that recognise the importance of continuous improvement tend to perform better than those that don't.

However, it's essential to acknowledge that what works for one organisation may not necessarily work for another. The effectiveness of best practices depends on the unique context and characteristics of each team and its environment. Therefore, teams should be prepared for both successes and failures as they experiment and tailor DevOps practices to suit their specific needs.

Overall conclusions stress the significance of context in interpreting the impact of different practices and capabilities on organisational performance, encouraging teams to embrace continuous improvement and experimentation to find the best strategies for their success.



# Software Delivery Performance Metrics

## The 4 Key Metrics

01

### Lead time

Lead time is the time it takes to go from a customer making a request to the request being satisfied. Shorter lead times enable faster feedback.

02

### Change fail percentage

This metric looks at the percentage of changes made to production that fail; the same as percent complete and accurate in Lean product delivery.

03

### Mean time to restore

Reliability is traditionally measured as time between failures, but in a modern software organization failure is inevitable. Thus, reliability is measured by how long it takes to restore service when a failure occurs.

04

### Deployment frequency

Deployment frequency is a proxy metric for batch size; the more frequently you deploy the smaller the size of the batch. Small batch sizes reduce cycle times, reduce risk and overhead, improve efficiency, increase motivation and urgency, and reduce costs and schedule growth.

Taking a look at the way metrics were gathered and used to assess performance. The authors used clustering techniques to categorise teams based on their software delivery and operational performance. They focused on five key metrics to measure performance:

- **Lead Time for Changes:** The time it takes from code commit to successful production deployment.

- **Deployment Frequency:** How often code is deployed to production or released to end-users.

- **Time to Restore Service:** The time taken to restore service after an incident or defect impacting users occurs.

- **Change Failure Rate:** The percentage of changes to production that result in degraded service and require remediation.

- **Reliability:** How well services meet user expectations, such as availability and performance, and the ability to meet or exceed reliability targets.

The authors analysed clustering results to understand the performance of teams based on software delivery and operational metrics. The clustering revealed four main clusters, each representing a distinct combination of performance characteristics:

- **Starting Cluster:** This cluster represents teams that are likely in the early stages of developing their product, feature, or service.
  - They may be less focused on reliability at this point and are more focused on gathering feedback and exploring.
  - Their performance is neither high nor low across any of the measured dimensions.

- **Flowing Cluster:** This cluster exhibits high software delivery and operational performance (SDO).
  - They have loosely-coupled architectures, provide flexibility in employee work arrangements, and excel in version control, continuous integration (CI), and continuous delivery (CD).
  - Relatively less focus on documentation, but their strong SDO performance suggests other factors contribute to their success.

- **Slowing Cluster:** This cluster makes up the highest proportion of respondents and includes teams from larger organisations, often less cloud-native.
  - They exhibit a performance-oriented, generative culture, and while they do not deploy too often, they tend to succeed when they do.
  - This cluster has low throughput and high positive-work culture, an unusual combination that warrants further investigation.

🟩 **Retiring Cluster:** This cluster performs poorly in both stability and throughput, but surprisingly outperforms others in organisational performance.

- However, this high organisational performance comes at the cost of high burnout rates, susceptibility to errors, and a burden of unplanned work.
- Their reliability might be enough to achieve high organisational performance, but without speed and stability, their teams face the consequences of burnout and unplanned work.

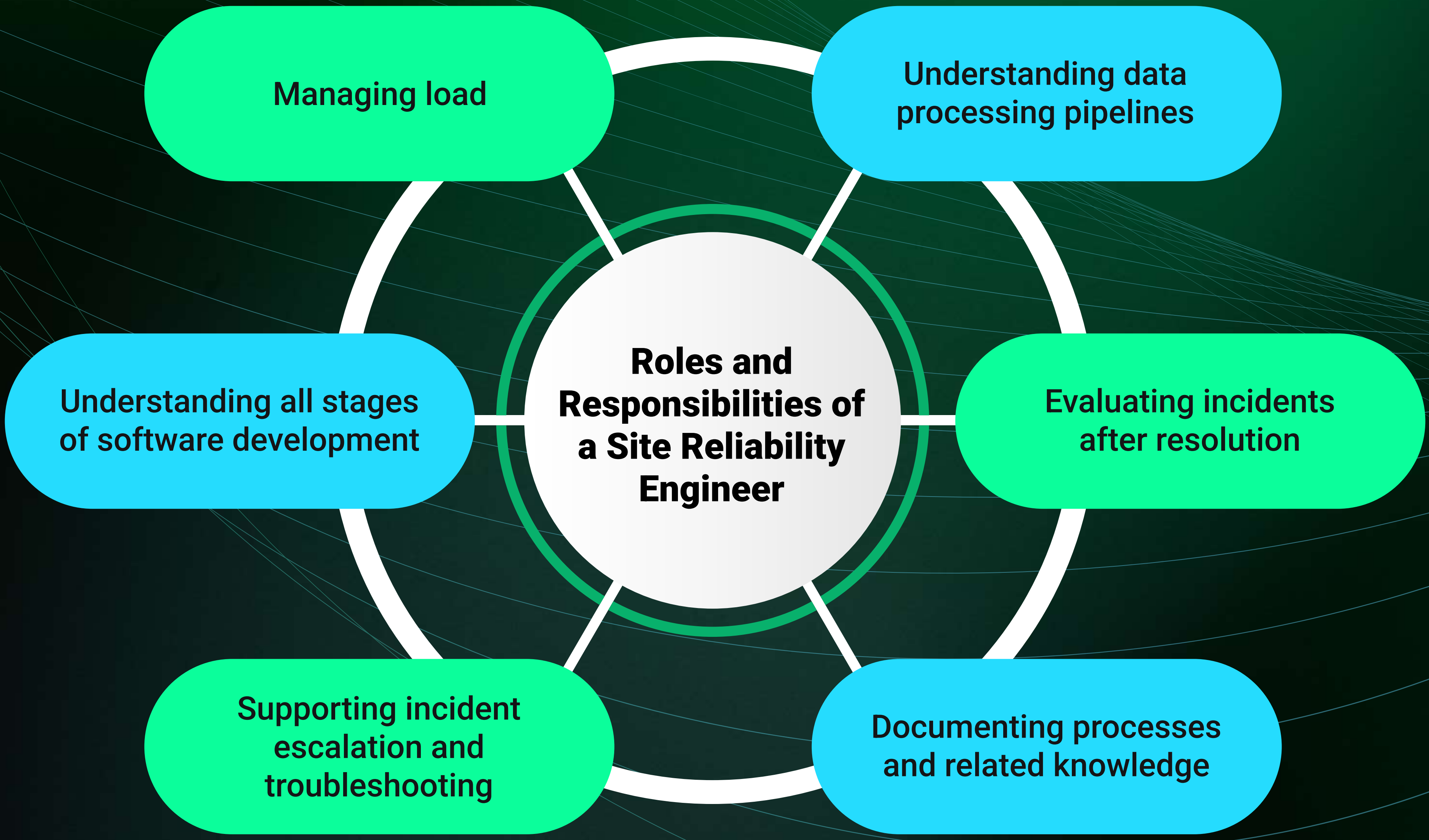
The surveys emphasise the importance of operational performance in conjunction with software delivery performance to achieve optimal results. The Flowing cluster, which exhibits the highest SDO performance, demonstrates the significance of factors like loosely-coupled architectures, flexibility, and strong CI/CD practices.

The prevalence of the Slowing cluster among respondents indicates the presence of larger organisations that may have a more established and generative work culture, despite not deploying as frequently. The Retiring cluster's unexpected performance results demonstrate the potential trade-offs between reliability and other performance metrics, as high organisational performance is accompanied by higher burnout rates and unplanned work.

Deeper analysis of the data recognises the variability within clusters and the potential for teams to transition between clusters based on their development stage and evolving priorities. The authors acknowledge the need for further research to explore underlying factors and better understand the relationship between throughput and culture.

Overall though, the results provide valuable insights into the diverse landscape of DevOps performance and the critical role of operational performance in conjunction with software delivery performance and the clustering approach helps teams understand and compare their software delivery and operational performance to others in the industry. The inclusion of performance metrics acknowledges the importance of reliability in conjunction with delivery performance to achieve optimal organisational performance. **Teams are encouraged to continuously improve and experiment with DevOps practices to find what works best in their specific context.**

# Site Reliability



Roles and Responsibilities of a Site Reliability Engineer

- Managing load
- Understanding data processing pipelines
- Understanding all stages of software development
- Evaluating incidents after resolution
- Supporting incident escalation and troubleshooting
- Documenting processes and related knowledge

Site Reliability Engineering (SRE), originally developed at Google and now adopted by many organisations, continues to gain traction and demonstrate how it plays a vital role in technical operations. SRE emphasises empirical learning, cross-functional collaboration, extensive automation, and the use of measurement techniques like Service Level Objectives (SLOs) to assess and maintain reliability. While some modern operations practices may apply similar methods with different names (e.g. ITIL describes similar methods and concepts), the survey uses neutral and descriptive language to assess the extent of these practices objectively.

Reliability practices related to reliability engineering, such as setting clear reliability goals and using salient reliability metrics, are still strong predictors of high organisational performance. These practices ensure that software and systems are dependable and consistently meet expectations.

What the studies further revealed was that SRE adoption is widespread among the teams surveyed, with a majority of respondents utilising one or more SRE practices. The relationship between reliability, software delivery performance, and outcomes is nuanced. When reliability is poor, pushing code faster into that context won't benefit users.

Site Reliability Engineers have long emphasised that reliability is the most crucial "feature" of any product, and the research supports the notion that keeping promises to users is essential for improved software delivery to benefit the organisation. Furthermore the extent to which people report meeting their reliability expectations also influences organisational performance. Highlighting that organisations which consistently deliver reliable software and services tend to perform better.

Finally, it was noted that implementing SRE in established organisations may encounter the "J Curve of change," as described in the "Enterprise Roadmap to SRE" publication. This curve involves early success, followed by periods of diminished returns or regressions. However, organisations that persist through these challenges often experience sustained elevated achievement.

The research confirms this J Curve pattern among technology teams studied and the impact of SRE practices on a team's ability to reach reliability targets is non-linear. Initially, the adoption of SRE may not positively affect reliability. However, as a team's SRE maturity grows, it reaches an inflection point where the use of SRE strongly predicts reliability, leading to improved organisational performance.

Reliability is a human endeavour, and the SRE approach exemplifies this. Positive team dynamics, a "generative" culture characterised by trust and collaboration, drive reliability. Stable teams with consistent membership also deliver greater reliability for user-facing services. Additionally, reliability engineering benefits from augmenting human efforts with process and tooling, such as cloud computing and continuous integration.

# Platform Engineering

Platform engineering is a strategic discipline focused on designing and constructing self-service capabilities to reduce the cognitive load on developers and enable swift software delivery. Platform teams provide shared infrastructure platforms to internal users responsible for delivering value through software development. These users primarily include software developers and engineers. The platform team consistently develops, constructs, maintains, and supports the underlying infrastructure to create self-service solutions. This empowers development teams to expedite their work and ensures uniformity across the organisation's practices.

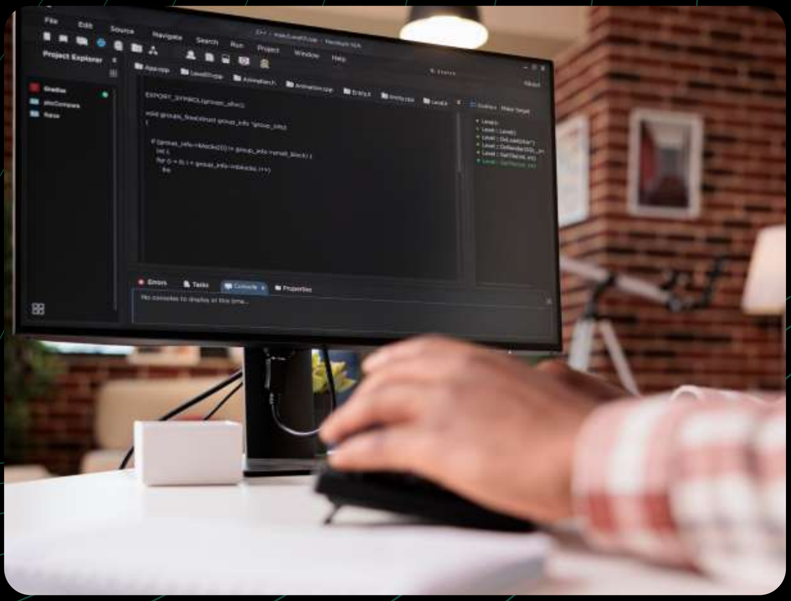
A central aspect of effective platform engineering is adopting a product-oriented mindset. This involves establishing feedback loops with platform users to understand their needs and challenges. Much like product management, platform teams engage in activities such as user research, outlining product roadmaps, incorporating feedback, iterative refinement, launching new features, and continuous maintenance. By embracing these principles, platform teams closely resemble successful product management practices.

**It's important to note that relying solely on automation and infrastructure coded as software doesn't suffice to develop a sophisticated DevOps practice.** The crux of highly developed DevOps organisations lies in refining the organisational structure, establishing distinct team identities, and fostering collaborative interactions among teams.

Notably, **the adoption of platform teams is a hallmark of advanced DevOps practices within enterprises.** While this doesn't mean that a platform team model is the sole path to DevOps success, it does establish itself as a well-established and proven avenue, particularly for large-scale enterprises.

Data from the studies underscores the significance of platform teams in the context of DevOps. Showing that organisations which are further along in their DevOps journey are more likely to employ platform teams, with a notable 65% of such organisations using self-service platforms. In contrast, organisations at the early stages of their DevOps evolution exhibit a lower adoption rate, around 40%.

Why do platform teams wield such transformative power for organisations of substantial scale and complexity? This question lies at the heart of the industry's understanding of platform engineering and the pivotal role of platform teams. Exploring the critical attributes that define a highly functional platform team was a central aspect of parts of the research. Below we look at some important points that came out.



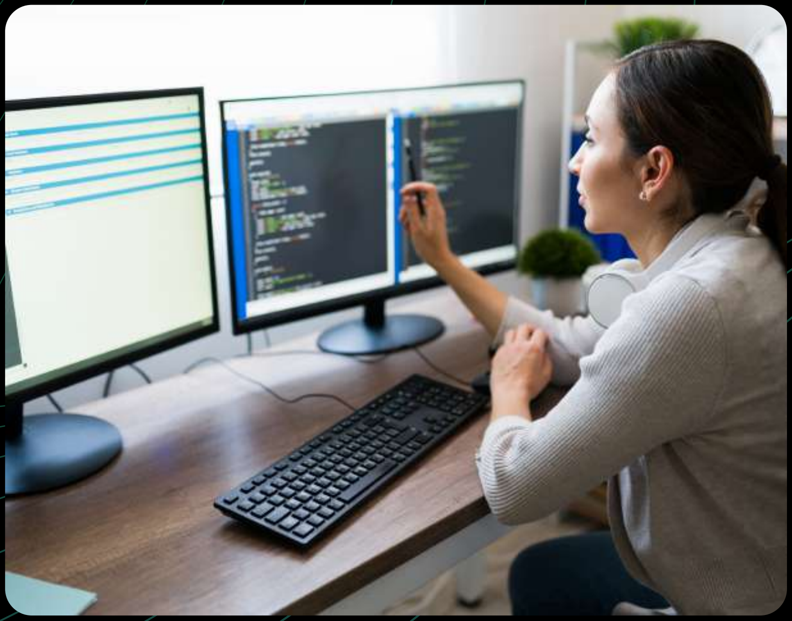
# Platform Engineering and the Resilience of Platform Teams

The concept of Platform Engineering, often overshadowed by the limelight of modern DevOps practices, possesses a lineage that stretches further back in time. It took root long before the emergence of the DevOps movement in the mid-2000s, tracing its origins to the early days of the digital realm. In fact, the foundational idea of constructing digital platforms to facilitate the seamless delivery of software on a grand scale has been an established practice for decades.

Historically, major players in the tech landscape, whose primary focus rested on software development, discerned the value of this approach well before the present era. These trailblasing entities recognised that by forging a path of infrastructure standardisation, erecting self-sufficient interfaces tailored for developers, elevating the level of abstraction, and appointing dedicated teams to oversee the maintenance of these pivotal platforms, a new horizon of efficiency and excellence could be reached. The outcome? Developer teams armed with the prowess to expedite the creation, deployment, and operation of applications, all while upholding an elevated standard of quality.

Nevertheless, the inception of these platforms did not come without its trials. In yesteryears, the foundational tools that now underscore the DevOps doctrine, particularly those pertaining to infrastructure as code, were mere echoes of the future. The technology tapestry of that time lacked the weaving of these intricate threads, resulting in a necessity for these pioneering establishments to construct their platforms from the very loom of invention. Unlike the current landscape, these early adopters enjoyed a simpler terrain, unencumbered by the masses of legacy IT that plagues the modern businesses.

Intriguingly, the approach taken by these nascent platform pioneers was not merely a creation, but a veneration of the fundamentals of efficiency and structure. The saga of Platform Engineering underscores the perennial wisdom of building upon a solid foundation, creating an environment where innovation could flourish, and software could take flight. As we navigate the ever-shifting currents of technological evolution, platform engineering has become a critical practice for future organisations to stay ahead of the curve.



## Relevance in the Present Landscape

In the contemporary terrain, the modern approach to platform engineering is characterised by several intrinsic qualities. Among these, the most overarching principle is the cultivation of a product-centric perspective. This entails treating your platform as a dynamic assortment of self-service products that continually evolve to harmonise with the evolving needs of developers. **The platform team, in its essence, aspires to alleviate the cognitive load on developers, paving the way for the swift delivery of software and greater innovation from the people delivering features of value to the end user.** This expeditious software flow, in turn, empowers the teams responsible for shaping value streams to bestow their offerings upon consumers without necessitating direct engagement with other teams.

For IT platforms, this paradigmatic approach commences by offering foundational infrastructure services in the form of self-service products, which are then harnessed by developer teams or, in some contexts, referred to as "value stream" teams. The blueprint and advancement of the platform should be an outcome of collaborative organisational learning practices, and the adoption of the platform internally should be spurred by internal advocacy, rather than being enforced through top-down mandates. All these intricacies dictate that your platform team must possess an amalgamation of skills, spanning development, operations, cybersecurity, product management, and product marketing, regardless of the specific designations each member holds.

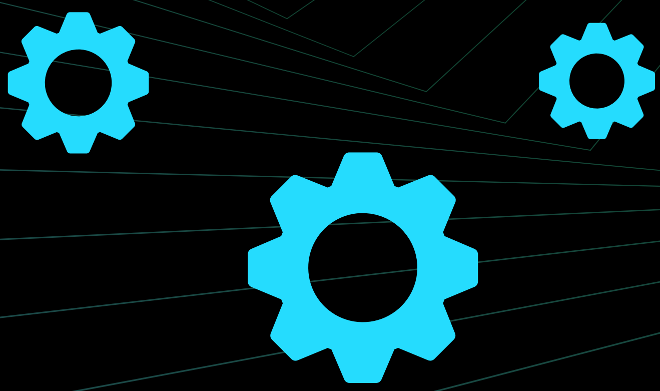
A significant transformation in mindset for many enterprises lies in the understanding that while the platform team should be well-versed in IT operations, their role does not extend to operating the applications residing on the platform itself. Instead, their responsibility is centred around delivering a reliable and robust platform that empowers value stream teams to independently craft, launch, and oversee their own applications. This distinction underscores the shift towards enabling and equipping, as opposed to assuming direct operational control.

## Insights from Research Unveiled

The findings gleaned from research cast a revealing light on the subject at hand. Amidst the annals of technological evolution, the emergence of platform teams stands as a relatively novel development within the grand tapestry of DevOps history.

Within the research results, a notable 27%, attest to the establishment of platform teams within the past two to three years. Moreover, an even more pronounced 16% share their experience of platform team implementation transpiring within the last one to two years and serves as a testament to the swift momentum that this practice has gained, signifying that the seeds of change sown within recent times have already borne fruit.

The revelations encapsulated within this research mirror the dynamism and the ever-evolving nature of the technological domain. It underscores the notion that while the foundations of DevOps may have been laid over a span of years, the domain of platform teams has evolved with remarkable agility, pivoting to a new paradigm that promises to shape the future course of software delivery.



## The Choice of Platform Engineering

Having traversed the multifaceted advantages that platform engineering brings to the fore, it becomes apparent that its benefits permeate the entire spectrum of an organisation, from developers to operations, from security teams to senior IT business leaders.

For the majority of respondents (54%), problem solving is the platform's primary goal, which likely reflects how platform teams aim to prevent other teams from reinventing the wheel by solving common problems time and again. A resounding 22% acknowledge amplifying the velocity of delivery as the primary aspiration. This is closely followed by the pursuit of scalability, resonating at 18%, emblematic of businesses navigating the path towards enhanced efficiency and expansion. For 10% of respondents, the catalyst was borne out of engineers grappling with excessive workloads and prompting the exploration of innovative mechanisms.

Other key stats showed:

- External guidance emerges as a beacon for 10% of respondents
- Regulating infrastructure costs served as the propellant for 9%
- Another 9% described scenarios where disparate value stream teams had inadvertently engaged in redundant work
- 8% of those surveyed said the drive emerged from the expansion of the product catalogue

The mosaic painted by this data underscores a profound narrative – that platform engineering is not a mere choice, but an imperative, ushering a realm of accelerated delivery, streamlined scalability, optimal resource allocation, and harmonious collaboration. The reasons that underpin this choice reverberate through the corridors of efficiency, innovation, and the quest for sustained growth. As the technological canvas evolves, platform engineering remains an indispensable brushstroke in shaping the contemporary landscape.

## Automation is key

Automation is at the heart of successful DevOps journeys. By streamlining and accelerating the software development and delivery lifecycle it plays a pivotal role in achieving DevOps objectives. By eliminating manual, error-prone tasks and ensuring consistency across the development pipeline. Automated processes enhance efficiency, reduce deployment errors, and enable teams to respond quickly to changing requirements. Moreover, automation enables the seamless integration of testing, deployment, and monitoring, allowing for rapid feedback loops and the identification of issues early in the development cycle. By automating routine and repetitive tasks, DevOps teams can focus on innovation, scalability, and improving the overall quality of software, leading to faster delivery cycles and increased agility in response to market demands.

Last years reports showed the following trends when it came to how automation was integrated:

- High-performing teams are more likely to use automated testing and automated deployment.
- They also continued to show increased efficacy, reduce errors, and more consistent quality.
- They also demonstrated higher code quality in end products because they received faster feedback.

## Security is a growing concern

Over the last few years the complex geopolitical landscape and high-profile security vulnerability headlines has made cybersecurity the top priority for most organisations. However, many organisations don’t have dedicated security teams. As a result, the burden generally falls on the usual suspects: DevOps engineers and/or full-stack developers. Somehow these people have become experts in at least half-a-dozen different and complex disciplines. Obviously this simply isn’t possible and as a result, output barely touches the surface; but more than this, those people who are supposed to be helping to reduce burden, are now being burdened and over-exerted themselves.

Last year's studies found that organisations are more aware than ever of the potential risks associated with software vulnerabilities, data breaches, and compliance violations.

Respondents also reported that teams adopting techniques like DevSecOps, were more able to shift security earlier in the development lifecycle; and by doing so were more easily able to identify and address security issues and reduce the likelihood of security incidents.

See below for more on Cybersecurity.

## Summary

Overall, the reports highlight the importance of cloud infrastructure, automation, leadership, diversity and platform engineering in achieving success in DevOps. They also emphasise the growing importance of security and the increasing adoption of continuous delivery practices.

In conclusion, nurturing a flexible and inclusive work environment is vital for promoting employee well-being, team performance, and overall organisational success. Organisations should proactively identify areas of improvement and prioritise creating a positive and supportive culture to foster a thriving workforce.

They should also invest in a generative culture, modern development processes like CI/CD, and proper infrastructure for security to achieve better security practices and positive outcomes for both their software development and team well-being. Security need not come at the expense of other development priorities but can be integrated into the existing workflow to improve overall performance and reduce risks.

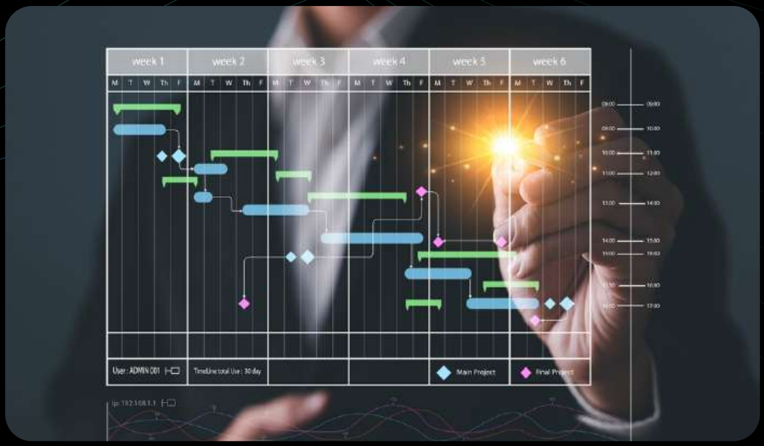
# CYBERSECURITY

As already mentioned, IT security has become one of the most talked about topics and certainly the highest priority on many people's plates. In the realm of cloud security, the allure of sophisticated attacks often steals the spotlight in these conversations, captivating attention with their intricacies and advanced methodologies. However, a closer examination of the data captured in Threat Horizons Reports reveals a contrasting reality: a substantial proportion of cloud compromises stem from mundane yet potent attack vectors, such as stolen credentials and security misconfigurations. While these might lack the allure of high-profile exploits, they remain prevalent and represent a critical area where defenders can significantly mitigate risks.

The importance of continuous vigilance and good cloud hygiene cannot be overstated. The evolution of cloud environments naturally tends to drift away from their baseline security settings, making it imperative to instate measures that consistently monitor and enforce robust security practices.

The examination of data regarding compromises of organisations with services deployed on cloud infrastructure reveals a diversification in the initial access vectors employed by threat actors compared to previous reports. Weak passwords persist as the most prevalent factor, accounting for 41% of observed compromises. However, API key compromise has emerged as a significant factor, playing a role in nearly 20% of the cases studied later on. Furthermore, later studies also showed there was notable diversification, with SSH being targeted in 26% of cases, closely followed by Jenkins CI servers and PostgreSQL at around 22% and 17%, respectively.

The heightened diversification efforts by threat actors underscore the ever-changing threat landscape confronted by organisations everywhere and the increased use of APIs to compromise apps suggests a rise in automation employed by threat actors meaning that attacks could well be on the rise.



In one of last year’s reports, observations from Q2 2023 affirm that weak credentials persist as a primary entry point for cloud compromises. Incidents involving brute-forcing default accounts, exploiting vulnerabilities in Secure Shell (SSH) and Remote Desktop Protocol (RDP), and compromising default VPC networks underscore the gravity of this security gap. It's evident that the strategic use of cloud-native security suites and rigorous auditing remains vital in detecting and preventing such breaches.

Moreover, vulnerabilities in software, notably PostgreSQL, have witnessed an observable increase in compromises, hinting at a broader risk landscape across multi-cloud environments. Organisations utilising multi-cloud setups might face analogous threats in their AWS and Azure environments. The emphasis on security best practices and managed database services emerges as pivotal strategies to mitigate these risks effectively.

Data collected from Google’s Chronicle Security Operations further emphasise the pressing need to address service account-related risks, as compromised service accounts pose a severe threat, enabling attackers to gain persistence and escalate privileges within cloud environments.

**These warnings highlight the criticality of evaluating alternative authentication methods and proactive monitoring to thwart potential breaches.**

The surveys also delve deeper into the realm of Software-as-a-Service (SaaS), unveiling how the increasing reliance on cloud-hosted SaaS systems expands the attack surface. With a growing number of applications connected to major platforms like Microsoft 365 and Google Workspace, the risk of security incidents, including data breaches, malicious applications, ransomware, and corporate espionage, intensifies significantly.

Threat actors are not only exploiting vulnerabilities within single SaaS systems but also orchestrating multi-SaaS cloud intrusions, underscoring the need for comprehensive security measures across diverse cloud environments. From unauthorised access and supply chain compromises to exploiting OAuth application vulnerabilities, threat actors demonstrate agility in leveraging diverse tactics to infiltrate and exfiltrate data from cloud-hosted SaaS systems.

In the face of these evolving threats, defenders are urged to remain steadfast in fortifying cloud security by prioritising good cloud hygiene, proactively monitoring for vulnerabilities, leveraging cloud-native security suites, and implementing robust authentication protocols. As cloud ecosystems evolve, the continuity of vigilance and adaptability in security practices remains paramount in mitigating risks and safeguarding sensitive data from sophisticated attacks.

Below are some key findings from last year's studies

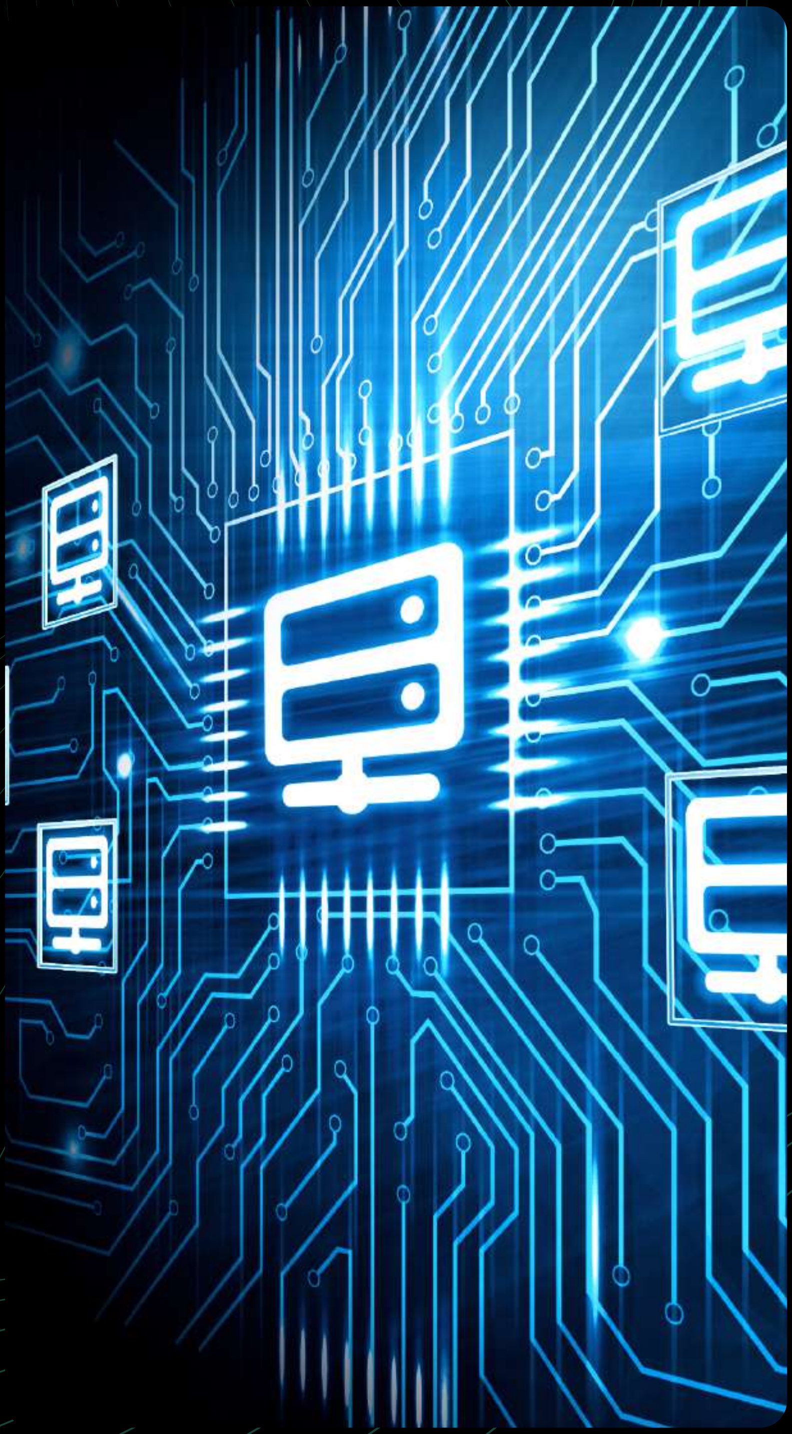
# Ransoming file transfer services

Mandiant, a subsidiary of FireEye, is known for its expertise in cybersecurity threat intelligence. They often release reports detailing various threat actor activities and tactics. In the first half of 2023 they observed financially-motivated threat group FIN11 exploiting zero-day vulnerabilities in Progress Software's MOVEit Transfer application and conducting data theft extortion operations affecting numerous organisations.

The exploit activity began days before Progress disclosed the vulnerability (CVE-2023-34362) as an SQL injection error, allowing unauthenticated access to MOVEit Transfer's database and exposed organisations in Canada, India, and the US. The attackers deployed a Web shell called LEMURLOOT to steal data, sometimes within minutes of the exploit. Mandiant also suggested the impact could extend beyond the identified victims. The company urges organisations to patch urgently.

Censys identifies 3,803 potentially vulnerable MOVEit hosts, with concerns about diverse industries relying on the software, including finance, education, and the US federal and state government. The assault on MOVEit mirrors comparable zero-day exploit activity that aimed at Forta's GoAnywhere Managed File Transfer product in January. During that instance, the attackers utilised a zero-day remote code execution flaw (CVE-2023-0669) in GoAnywhere to establish unauthorised user accounts on certain customer systems. Subsequently, they exploited those accounts to pilfer data and install additional malware.

Security experts warn that compromising file transfer solutions provides threat actors access to sensitive information from numerous businesses. The ongoing exploitation of MOVEit Transfer emphases the growing appeal of such technologies to ransomware actors seeking data theft over encryption and highlights the need for organisations to promptly apply patches and reinforce security measures to mitigate the risk of data theft.



# Threat Actors Leveraging Legitimate Cloud Services

Threat actors are increasingly using legitimate cloud services to host malicious infrastructure, exploiting the trust placed in these services by enterprises and consumers. Google's Threat Analysis Group (TAG) has encountered instances where threat actors abuse cloud-based storage and productivity services, evading detection by blending into legitimate traffic volumes.

In an examination of new attack vectors against cloud environments, a search was conducted on VirusTotal (VT) for 2022 malware samples that communicated with three geographic regions of major cloud service providers (CSPs). The analysis revealed that over 6,000 malware samples dynamically interacted with CSPs, utilising various pre-specified or randomly selected IP addresses and TCP/IP ports. Some instances involved attempts to conceal malicious activities by communicating through well-known ports and explicitly utilising TLS. To counteract such threats, Mesoform advises SRE functions to monitor and restrict both inbound and internal cloud network communications, employ hardened VM images, and scrutinise cloud instance audit events for unexpected administrative or user activities - ideally using SIEM systems.

Among the identified malware samples communicating with CSPs, the utilisation of well-known ports such as 80 (HTTP) and 443 (HTTPS) was more prevalent compared to ephemeral ports (e.g., above 1023). This pattern may be attributed to the common practice of CSPs and their customers opening these ports to expose normal services. The use of these ports could also be attributed to disguising malware activities as well as encrypting their transmissions to further hide what's going on and maintain long-running compromises.

However, malware might target registered or ephemeral ports during the scanning process for open TCP/IP ports, or to exploit less-common cloud services. This approach, albeit more easily monitorable, is probably used for quick get-in, get-out attacks. This diverse range of techniques reflects an evolving landscape of malware tactics within cloud environments.

# Cybersquatting

Another noteworthy threat which was highlighted in recent years was the practice of cybersquatting, registering domain names that violate trademark rights with the intent to sell the names for a profit to those businesses. It has seen a significant surge in the past decade and we're now also seeing a surge in threat actors utilising typosquatting, a variation of cybersquatting, to target cloud storage platforms like Google Cloud Storage, Amazon S3, and Azure Blob. Typosquatting capitalises on user typos when entering web addresses, directing them to alternate sites owned by cybersquatters, opening avenues for various cybercrimes. Tackling cybersquatting demands proactive monitoring, legal actions, and robust management strategies to safeguard against evolving threats in the digital landscape. Furthermore, typosquatted URLs closely resemble legitimate ones, making detection difficult, potentially allowing threats to slip past security systems.

The main issues seen from cybersquatting are:

- **Phishing and Malware Distribution:** Users visiting typosquatting domains might encounter phishing pages or unknowingly download malware.
- **Identity Theft and Reputation Damage:** Cybersquatters may register literal company names, leading to identity theft or reputation harm.
- **Cloud Storage URL Manipulation:** Threat actors forge URLs on cloud storage platforms, closely resembling legitimate names, enabling malicious activity to go unnoticed.

# Mitigations

Ensuring security in depth is paramount in safeguarding not only sensitive information but the very core of an organisation's integrity. As Mesoform regularly navigates the intricate landscape of cybersecurity, we are acutely aware that relying on a single layer of defense is akin to leaving your front door key under the mat. By embracing a comprehensive approach to security, encompassing layers of defense mechanisms, we fortify against an array of potential threats. Each layer acts as a sentinel, poised to detect and repel different types of incursions. This multi pronged strategy not only bolsters resilience but also minimises the likelihood of a catastrophic breach. In an era where cyber threats constantly evolve and adapt, the philosophy of security in depth becomes our digital shield, instilling confidence that our digital presence is well-guarded against the relentless tide of cyber adversaries.

Mesoform employs, what we call, a PRO approach (Proactive, Retrospective and Observative). Each with their own layers. For example, Proactive includes using IAM, RBAC, mutating constraints and validating constraint controls. Below is a set of concepts and processes organisations should consider adding (if they don't have them already) to their defence tool kit for the issues described above.

- Domain Monitoring Services: Utilise domain monitoring services to track typosquatted domains and their permutations.

- Playbook Development: Develop a response playbook specifically for addressing typosquatted domains and cloud storage cybersquatting.

- Provider Reporting: Report instances of cloud storage cybersquatting to the associated cloud providers (Google, Amazon, Microsoft).

- Proactive Domain Registration: Proactively register domain permutations to minimise the risk of typosquatting.

- Attack Surface Management: Include checks for domain and cloud storage typosquatting in security management efforts.

- Legal Actions: Victims can file complaints under the Uniform Domain-Name Dispute-Resolution Policy (UDRP) or the U.S. Anticybersquatting Consumer Protection Act (ACPA) for trademark protection.

- Native Security Controls: Leverage native security controls within SaaS applications, aligning configurations with industry best practices.

- SaaS Security Posture Management (SSPM): Automate protection and identify misconfigurations.

- Identity and Access Management (IAM): Manage high-privilege accounts and implement least privilege principles rigorously.

- Intrusion Detection Systems (IDS) and Network Monitoring Tools: Use IDS and network monitoring tools to detect C2 traffic or exfiltration.

- Centralised Logging and Anomaly Monitoring: Implement robust centralised logging and monitor environments for anomalous behaviour.

As cloud security threats evolve, proactive measures, a multi-layered defence approach, and continuous adaptation are fundamental in thwarting sophisticated attacks targeting cloud-hosted environments.

In a recent **Tech Musings blog series,** Mesoform took a proactive look at a number of other security concerns, why they matter and things to consider for your organisation. Pop over to our website to **have a look.**

## Risks

01 **Hacking**

02 **Theft**

03 **Whistleblowing and social media**

04 **Malware infections**

05 **Social engineering**

06 **Electronic eavesdropping**

# The OWASP Top Ten Project

It's worth a special mention to the Open Worldwide Application Security Project (OWASP), which is a nonprofit foundation that works to improve the security of software projects. It utilises a comprehensive methodology to identify and rank the top web security risks. The process involves data collection from various sources, including security companies, organisations, and independent researchers. The collected data is then analysed and evaluated based on factors such as prevalence, exploitability, and impact on web application security. The final list of vulnerabilities represents the most significant risks faced by web applications today.

The OWASP Top 10 is a standard awareness document for developers and web application security teams. It represents a broad consensus about the most critical security risks to web applications. It was last updated in 2021 and should have its next iteration for 2025. The latest top 10 is:

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server Side Request Forgery (SSRF)

Last year, OWASP did release the latest findings from their API Security Project which aims to provide value to software developers and security assessors by highlighting potential risks associated with insecure APIs and demonstrating methods to mitigate these risks. Mesoform has already published an analysis of the results in an article on our website. If your business has any API, it's worth heading over to have a read. Below is the OWASP 2023 API security top ten:

1. Broken Object Level Authorization
2. Broken Authentication
3. Broken Object Property Level Authorization
4. Unrestricted Resource Consumption
5. Broken Function Level Authorization
6. Unrestricted Access to Sensitive Business Flows
7. Server Side Request Forgery
8. Security Misconfiguration
9. Improper Inventory Management
10. Unsafe Consumption of APIs

## Summary

In summary, the landscape of IT security, particularly in the context of cloud environments, has become a paramount concern. While discussions often focus on sophisticated attacks, Threat Horizons Reports reveal that a substantial number of cloud compromises stem from seemingly mundane yet potent attack vectors, such as stolen credentials and security misconfigurations. Despite lacking the glamour of high-profile exploits, these vectors are prevalent and demand vigilant defence.

Continuous vigilance and adherence to good cloud hygiene are crucial. Cloud environments naturally evolve away from baseline security settings, necessitating consistent monitoring and robust security practices. The analysis of compromise data highlights a diversification in threat actors' initial access vectors, with weak passwords remaining prevalent but API key compromise emerging significantly. The heightened diversification suggests an evolving threat landscape and an increased use of APIs, potentially driven by automation.

Addressing weak credentials as a primary entry point for cloud compromises is imperative. Cloud-native security suites and rigorous auditing play a vital role in detecting and preventing breaches. Additionally, vulnerabilities in software, like PostgreSQL, indicate a broader risk landscape in multi-cloud environments, emphasising the need for security best practices and a comprehensive, multi-layered defence approach.

Finally, the reports call for a holistic and adaptive approach to cloud security, urging defenders to prioritise good cloud hygiene, leverage cloud-native security suites, implement robust authentication protocols, and remain vigilant in the face of evolving threats. The provided mitigations and proactive measures offer a few useful tools in your defence toolkit against the dynamic landscape of cyber threats in cloud environments but there’s much more to be aware of, so make sure you have a team that is well skilled in DevOps, SRE, Cybersecurity and Platform Engineering.

# CONCLUSION

In conclusion, the synthesis of these reports underscores the critical role of cloud infrastructure, automation, leadership, diversity, and platform engineering in successful DevOps practices. Moreover, it emphasises the increasing significance of security measures and the adoption of continuous delivery practices. Nurturing a flexible and inclusive work environment emerges as essential for promoting employee well-being, team performance, and organisational success.

To achieve this, organisations must invest in a generative culture, modern development processes such as CI/CD, and robust security infrastructure without compromising other development priorities. The landscape of IT security, especially in cloud environments, demands continuous vigilance against diverse threat vectors like stolen credentials and security misconfigurations. Implementing cloud-native security suites, robust authentication protocols, and proactive measures is imperative to defend against evolving threats.

Ultimately, a holistic and adaptive approach to cloud security is essential, highlighting the importance of skilled professionals in DevOps, SRE, Cybersecurity, and Platform Engineering to safeguard against the dynamic cyber threat landscape.

## For the short future

In the dynamic realm of the IT industry, let us unite in a proactive stance, advocating not only for robust security measures but also for the holistic well-being of our employees.

As leaders and contributors within this ever-evolving landscape, we bear the collective responsibility of nurturing environments that prioritise both professional excellence and personal wellness.

Central to our mission is the cultivation of a workplace culture that champions a harmonious work-life equilibrium, recognizing that sustained productivity flourishes alongside individual fulfilment.

We endeavour to provide the necessary resources and support systems that empower our teams to thrive, both personally and professionally.

By embracing a culture of continuous improvement and shared responsibility, we not only safeguard the interests of our organisations but also nurture the talents and aspirations of our dedicated IT professionals.

Let us illuminate the path forward, crafting a brighter, more secure future for IT workplaces around the world and the individuals who shape them.

mesoform