American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
http://asrjetsjournal.org/

DevSecOps Services: A Study of the Most Common and Rarest DevSecOps Services Available in 2022

Kiran Sharma Panchangam Nivarthi[a*], Sudha Balajinaidu[b]

[a]*31108 Algonquin Trail, Chisago City, MN, 55013, USA*
[b]*15251 Pleasant Valley Rd, Center City, MN 55012*
[a]*Email: Kiransnandu@gmail.com,* [b]*Email: sudha1481@gmail.com*

Abstract

DevSecOps is an evolving set of practices within the prevalent DevOps paradigm that aims to include security at every stage of the development cycle. In order to understand how it has matured since its inception, we looked at a sample of 25 companies offering DevSecOps services to identify which services were most common and rarest. Multiple trends were identified, including a heavy lean towards DevSecOps services towards consultation and organizational adaptation. We also identified compliance to be a focus of many DevSecOps services. DevSecOps consultation and DevSecOps as a Service (DaaS) were identified as two of the most commonly available services in 2022, and isolation, SRE, SIEM, and orchestration were the rarest. Future studies on this subject might reveal different trends in the evolution of DevSecOps services, assuming DevSecOps hasn't been replaced by a more advanced paradigm.

Keywords: DevSecOps Services.

1. Introduction

DevSecOps is an evolving discipline/approach to software/application development. It's the amalgamation of security and DevOps with the primary goal of integrating modernized security practices in DevOps [1]. DevSecOps breaks down the silos between software development and security. It can be defined using the same four pillars used to define DevOps: Culture, Automation, Measurement, and Sharing (DAMS) [2]. However, its challenges are different, including the lack of tools and security education of developers. The lack of developer education is outside the scope of this problem, but another relevant deficiency, i.e., the lack of developer-oriented security testing tools that can facilitate easier DevSecOps adoption, can be asserted or refuted based on the available DevSecOps services and solutions in the market [3].

---

* Corresponding author.

It's difficult to track the pacing of an evolving discipline, especially one that's on the cutting edge of software development. But one way to ascertain how much an approach/discipline has matured since its inception is to look into its demand and supply in the market. This paper aims to identify patterns in DevSecOps services supply by looking into 25 companies offering DevSecOps services and solutions, i.e., gauging its maturity by evaluating the supply.

From the available research papers on DevSecOps, we have been able to identify certain trends that can be endorsed or refuted by the commonplace or rare availability of relevant services. The first trend is that DevSecOps is in its infancy [4]. It's a trend we may be able to observe by looking into the ratio of DevOps companies that offer DevSecOps as an extension of their services. Another trend was the speculation, at least until 2020 [5], regarding the mainstream adoption of DevSecOps as a culture in the development community. We can shed more light on how easy it is to find DevSecOps services online (compared to similar services or conventional security services). Even though DevOps has been widely adopted, the adoption of DevSecOps, even among organizations embracing the DevOps culture, might be lagging behind.

There is also a visible lack of literature and resources on this topic, especially on adoption frameworks/practices [6]. This indicates a need for DevSecOps consultation services, which we can identify as either a prevalent or rare service. There is a growing awareness regarding the use of DevSecOps practices and approaches to automated testing in CI/CD pipelines, especially for development teams with little to no security expertise [7]. A visible prevalence of DevSecOps services or solutions directly addressing CI/CD pipelines can endorse this trend. Another trend is the intersection of compliance with DevSecOps [8]. This might be visible from companies offering compliant DevSecOps services and tools.

The above stated are just some of the trends that can be identified or endorsed by systematically evaluating a sample of companies offering DevSecOps services, though we aim to generate more insights from this online research.

2. Methodology

In order to identify visible trends and most commonly offered DevSecOps services, we looked into 25 companies that offered either DevSecOps services/DevSecOps as services or DevSecOps solutions. The overall pool leans heavily towards Northern America and European markets, with a handful of companies from other regions offering DevSecOps services.

We also looked at some of the corporate investors of the largest DevSecOps communities and groups. The largest one projects OWASP DevSlop with nine corporate supporters that operate in the cyber security sphere, offering tools, products, or solutions that can be employed in DevSecOps. However, only three of the nine companies have included DevSecOps in their service portfolio or as an integral part of their platforms.

This reflects a pattern and a minor challenge we observed – Even if the other six companies had services and tools that could integrate with the existing DevSecOps culture of an organization or help a business

development team adopt the DevSecOps culture, they would be difficult to identify because they are not marketed as such. This would be challenging, even for developers, since the process of finding relevant DevSecOps services would be the same for people outside this domain (managers, business owners, c-suite executives, etc.) – an online search.

We have excluded services and tools offered by or closely associated with market giants like Microsoft Azure and Amazon AWS, which currently have six popular DevSecOps products.

3. The 25 Companies Observed

The 25 companies we looked into for the DevSecOps services they offer are:

Table 1: 25 DevSecOps Services companies, Location.

Company	Location	DevSecOps Services	Comments
Ebryx	New Hampshire, US	● DevSecOps as a Service (DaaS)	Four-step process: Assessment, strategy, implementation, monitoring. Security is integrated at every development step.
Veritis	Texas, US	● DevSecOps Consulting	End-to-end consulting services
Cloud4C	Singapore	● Code analysis and management. ● Threat/vulnerability assessment. ● Compliance monitoring. ● Training.	DevSecOps services lean heavily towards compliance.
Qentelli	Texas, US	● Advisory Service. ● DevSecOps As a Service (DaaS). ● Managed Site Reliability Engineering (SRE). ● Isolation (For automation).	Empowered by Static and Dynamic Application Security Testing (SAST and DAST), automation, and isolation.
Mastek	Mumbai, India	● DevSecOps Consulting	DevSecOps is rolled into their app engineering services.
Soft Kraft	Bielsko-Biała, Poland	● DevSecOps Consulting	It's also labeled as DevSecOps as a Service, giving a slightly misleading sense of scope.
Xenonstack	Texas and California, US	● DevSecOps Consulting ● DevSecOps Managed Services	Its DevSecOps services also include SIEM as a Service and Kubernetes security services.

		● Security Automation	
Relevant	Lviv, Ukraine	● DevSecOps Consulting ● Secure development ● DevSecOps as a Service (DaaS) ● Operational DevSecOps Services	The company also offers 14 other DevSecOps services, separate or rolled into the four primary services.
Royal Cyber	Illinois, US	Nine services, including: ● SAST/DAST/IAST ● Infrastructure security network ● Appsec Pipeline ● Compliance	The company has a relatively extensive DevSecOps service portfolio but not an end-to-end DevSecOps approach.
Radixweb	Gujarat, India.	● DevSecOps Consulting ● DevSecOps as a Service (DaaS)	Eight distinct DevSecOps solutions are rolled into the two services.
Synopsys	California, US	● Real-time code security assessment. ● Application security testing.	It offers specially designed DevSecOps tools.
Apiiro	New York, US	● DevSecOps Orchestration	Allows for easy management of Secure Software Development Lifecycle (SSDLC).
Datadoghq	New York, US	● Unified DevSecOps tool	Facilitates unified security monitoring.
Zeronorth	Massachusetts, US	● DevSecOps platform	The company's core product/service is DevSecOps.
Bridgecrew	California, US.	● DevSecOps platform	Cloud-native security automation.
10pearls	Virginia, United States	DevSecOps consulting is the core service the company offers. ● SAST/DAST/IAST ● Software Composition Analysis (SCA)	Five specific technologies are specified under DevSecOps tools and technologies.
Transformhub	Singapore	● DevSecOps assessment ● DevSecOps as a Service (DaaS)	Automation, Continuous Integration (CI), management, and disaster recovery are also

		● DevSecOps platform	part of the service portfolio.
Dare Planet Technology	Madrid, Spain	● Vulnerability Detection ● Configuration Errors fix ● Multi-Cloud Security Integration ● Error Resolution Automation	12 cloud and cloud-related technologies are specified under DevSecOps capabilities.
Outposts	Ukraine	● Security Automation ● Risk Reviews and Prioritization ● Compliance Control ● Threat Research	DevOps is the company's primary service. Fifteen technologies specified under DevSecOps capabilities/services.
Coforge	New Jersey, United States/India	● DevSecOps end-to-end consultation. ● DevSecOps Maturity Assessment	DevSecOps is one of the six main cloud services the company offers.
Daffodilsw	Haryana, India	● DevSecOps Maturity Assessment ● DevSecOps Implementation ● Assessment of Industry Regulatory Compliance ● Securing DevOps Workflows ● Security Automation	
Netguru	Poznań, Poland	● DevSecOps Consulting ● Risk assessment/Threat modeling ● CI/CD Pipeline and Cloud hardening	The company follows an SSDLC framework.
Ivedha	Canada	DevSecOps as a Service (DaaS)	
TLconsulting	Australia	● DevSecOps consulting ● Compliance consulting	
BARiKAT	Turkey	● Security Tests ● Early Detection ● Secure Software Development	

A few notable observations from the DevSecOps companies and services we looked into are:

- AquaSec is one of the most commonly identified technologies that companies offering DevSecOps services specialize in. It's also the largest pure-play cloud-native security company (self-proclaimed).
- Most DevSecOps companies have DevOps expertise and services in their portfolio unless they are purely cybersecurity/digital security/cloud security companies that have extended their portfolio to include DevSecOps. However, few major DevOps companies in the world offer specific DevSecOps services. This shows that DevSecOps (2022) is still not considered a standard part of the DevOps culture.
- Outside North American and European markets, India and Singapore are two regions with a sizable representation of DevSecOps services/companies offering DevSecOps services.

3. Limitations

There are several limitations that mitigate the scope, depth, and accuracy of the insights we can glean from DevSecOps services currently available in the market, and it's important to recognize them.

- There is no standard language when it comes to DevSecOps services. This is a common problem in almost all tech domains. One company's DevSecOps as a Service (DaaS) might have a completely different scope compared to another's.
- We only looked at companies that have DevSecOps services as a separate offering within their portfolio. There are many IT consulting and other tech companies that may offer similar services but rolled into their DevOps or Security service offerings.
- The limitation is inherent in the sample size. The companies are chosen based on the online ranking/popularity of their website, and the sizes, ages, and geographic reach of the companies are mixed. However, it's entirely possible that we might have missed a strong DevSecOps company with a weak online presence.
- Regional limitations, specifically China. Even though the Chinese have a different development culture and attitude towards the cloud, it has virtually no representation in the sample despite being the second-largest global economy and a heavy tech lean. A possible reason is that the Chinese B2B DevSecOps websites are in the Chinese language and do not rank heavily on Google, unlike most manufacturing-oriented Chinese websites that have English counterparts, as they most offer services to the Western markets.

Despite these limitations, we can at least identify the most common and rarest DevSecOps services in 2022.

4. Most Common DevSecOps Services

The most common services are DevSecOps consultation and DevSecOps as a Service (DaaS).

4.1 DevSecOps Consultation

DevSecOps consultation is one of the most common services offered because, at its core, DevSecOps is a culture that developers and development teams need to adopt [9]. Therefore, understanding the intricacies of the culture and how a particular organization can adapt by leveraging the consultation services of a cybersecurity

professional [10] is the natural first step for most organizations aiming to embrace DevSecOps. It's still a popular service because DevSecOps adoption is still in its infancy, despite DevOps becoming more widely adopted due to the accelerated pace of cloud-native development. The scope of DevSecOps consultation service is determined primarily by two factors – the expertise of the company offering DevSecOps consultation services and the requirements and adoption stage of the business seeking these services.

The company offering this service has to be familiar with the generic challenges associated with DevSecOps implementation and should have a framework in place to identify the specific challenges an organization might face while adopting DevSecOps and have adequate solutions in place. These challenges increase with the scope of the development project and the number of teams working on the project [11]. The scope of the consultation service will also be different if it's for a specific project as opposed to services hired for the cultural adoption of DevSecOps, which may reach outward to include things like its adoption as a decision-making framework [12]. In a project-oriented DevSecOps consultation, the service will have a more problem-solving, technical, and strategic approach. And not all DevSecOps consultation service providers might offer this service for all development stages, while others go beyond to include continuous monitoring of the final product and feature addition.

4.2 DevSecOps as a Service (DaaS)

The primary reason why DevSecOps as a Service (DaaS) appears a common practice is because it's an umbrella term that may include a wide variety of DevSecOps services. It's actually redundant to call DevSecOps as a Service a DevSecOps service, but since that's how it's marketed online, it's important to understand the implications of using this term. The challenge, again, is the lack of standardization. A company that offers a DevSecOps as a Service solution may not offer the same *set* of DevSecOps services as another company. This may require a potential client to look into the individual services, tools, expertise, or development areas covered anyway. However, the "as a service" term has become quite commonplace and triggered a sense of familiarity. We can argue that many organizations that are already heavily using other technological services marketed with a phrasal suffix "as a Service" might be more inclined to accept a DevSecOps service package called "DevSecOps as a Service." Despite the lack of clarity associated with this "service package," it may have the appeal to potentially attract a larger target audience pool.

4.3 Other Common Services

There are several DevSecOps services that are marketed separately or bundled in DevSecOps as a Service solution. Six of the most commonly occurring ones are:

- Compliance-related services. There is a significant overlap of compliance and security in most industries, especially healthcare and finance, so a high frequency of compliance services under the DevSecOps umbrella is natural [13].
- Automation is a crucial part of DevSecOps as it allows for security to be integrated at every step of the DevOps loop [14].

- Risk/Threat Assessment is an integral part of DevSecOps as a security-oriented development approach.
- SAST or Static Application Security Testing is performed on the source code of an application (at rest).
- DAST or Dynamic Application Security Testing is performed when an application is running and doesn't look into the source code for vulnerabilities.
- IAST, or Interactive Application Security Testing, combines both DAST and SAST. It tests an application while it's running and simultaneously helps in identifying the vulnerable segments of the source code.

5. Rarest DevSecOps Services

The rarest DevSecOps services we found on the 25 websites we observed were:

5.1 Isolation

Isolation was the rarest service. Only one company offered it as part of the DevSecOps services, even though it's a noted DevSecOps practice. It allows a development team to create isolated automation processes for testing and reporting.

5.2 SIEM

SIEM, or Security Information and Event Management, is defined by IBM as security solutions that can help an organization identify potential threats and vulnerabilities *before* they disrupt operations. Two out of twenty-five observed companies offered this solution as part of their DevSecOps services, and one company offered cloud SIEM, a separate service.

5.3 DevSecOps Orchestration

DevSecOps orchestration is offered by three out of twenty-five companies observed. Two of them offer a proprietary tool for DevSecOps orchestration.

5.4 SRE

Site Reliability Engineering or SRE is a common IT service, but only three out of twenty-five companies market it as part of their DevSecOps services.

For the rarest DevSecOps services, the following trends were identified:

- One company (Qentelli) offers two of the four rarest services identified. But we cannot associate it with a specific nomenclature use as its other DevSecOps services are in line with the more commonplace terms (SAST/DAST and automation).
- Orchestration, which should have been a very common DevSecOps service or, at least, a commonly used marketed term, is quite rare. We believe that its requirement of proprietary technology/solutions, which not all DevSecOps companies may have access to, is the reason.

- SRE and SIEM are both common cloud services, but relatively few companies have chosen to roll them into their DevSecOps services.

6. Results

As identified earlier in this paper, not all DevOps companies or tech companies with DevOps capabilities offer DevSecOps services. However, a significant number of companies offering DevSecOps originally operated in the IT/digital security domain. So the collective pool of available DevSecOps services indicates that it's growing out of its infancy, even though it has yet to become a standard DevOps offering.

As DevSecOps consultation (with cultural integration as an offering) is still one of the primary services offered in this domain, it strengthens the argument that there are still hindrances in the mainstream adoption of DevSecOps culture in the development community.

It’s easy to find almost all DevSecOps services online, but an existing lack of common terminology might make it difficult to compare certain services. This difficulty is more obvious in rare services compared to the common ones.

Automated testing is one of the most common DevSecOps services, especially in the context of CI/CD pipelines.

There is a significant overlap between compliance and DevSecOps.

7. Discussion

The growth of DevSecOps services is tied to growth and innovation in several other disciplines, predominantly DevOps and cybersecurity [15] and, to a lesser extent, digital compliance and automation [16]. Since DevSecOps is as much about the practices and approach to software/application development as it is about the tools facilitating continuous integration in the development cycle, other overlapping practices like cloud-native. Moreover, all of these individual disciplines/domains associated with development are rapidly evolving under the influence of Artificial Intelligence (AI) [17] and Machine Learning (ML) [18].

This makes predicting the future prevalence of DevSecOps challenging, which makes decision-making in this regard, both from DevSecOps service providers and businesses adopting DevSecOps in their own development practices, leveraging the consulting services and tools made available by the providers. An example would be the future of DevSecOps, while the popularity of DevOps as a popular development paradigm slowly declines in favor of a new, smarter paradigm. Infrastructure automation frameworks like GitOps are already competing in the market as better alternatives, and we may see further evolution along this line. Some Al and ML-based digital security and compliance tools and a correlated set of practices may also evolve parallel to DevSecOps, making parts of it obsolete.

With this in mind, how should businesses, both DevSecOps service providers and ones with in-house

development teams, approach DevSecOps adoption? Should they invest a significant amount of time and resources into completely shifting their practices and opt for the best available services and tools in the market, absorbing their cost only to see them being replaced by others in the next few years? Or should they indulge in partial adoption, not fully realizing the benefits of DevSecOps?

Another avenue of DevSecOps services and the prevalence of certain services compared to others is their overlap with the needs of the market. Based on their development requirements, the level of automation they are comfortable with, compliance guidelines, and digital maturity, some businesses may need specific DevSecOps services that are not prevalent. This leaves them with fewer options compared to businesses with more flexible DevSecOps needs. Is this a market segment more DevSecOps service providers can tap into or a relatively unprofitable inflation of their DevSecOps service portfolio?

Further studies are needed to ascertain the cost (financial, time, skill, and resources) of different DevSecOps services and their potential benefits. This can help DevSecOps, and DevOps companies make smarter decisions about which services to include in their portfolio and invest their time and resources.

8. Conclusion

Many DevOps, security, and other IT companies have expanded their DevSecOps service portfolio over the last five to seven years, and this growth will continue. The service portfolios might grow to include proprietary tools, specialized services, compliance-related expertise, new automation tools, etc. From a survey of the current most common and rarest DevSecOps services, it's clear that much of the target market is still in the adoption phase of DevSecOps since the most common services are geared towards that avenue. Similar studies replicated in the future might indicate different trends, i.e., tools, frameworks, and services focused on empowering organizations to build their own DevSecOps capabilities.

References

[1] H. Myrbakken and R. Colomo-Palacios, "DevSecOps: A Multivocal Literature Review," in International Conference on Software Process Improvement and Capability Determination. Springer, Cham , Palma de Mallorca, Spain, 2017.

[2] N. Tomas, J. Li and H. Huang, "An Empirical Study on Culture, Automation, Measurement, and Sharing of DevSecOps," in 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, Oxford, UK, 2019.

[3] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, "Challenges and solutions when adopting DevSecOps: A systematic review," Information and Software Technology, vol. 141, 2022.

[4] R. Mao, H. Zhang, Q. Dai, H. Huang, G. Rong, H. Shen, L. Chen and K. Lu, "Preliminary Findings about DevSecOps from Grey Literature," in IEEE 20th International Conference on Software Quality, Reliability and Security (QRS), Macau, China, 2020.

[5] M. Sánchez-Gordón and R. Colomo-Palacios, "Security as Culture," in 2020 IEEE/ACM 42nd International

Conference on Software Engineering Workshops (ICSEW), Seoul, Republic of Korea, 2020.

[6] A. Gupta, "An Integrated Framework for DevSecOps Adoption," International Journal of Computer Trends and Technology, vol. 70, no. 6, pp. 19-23, 2022.

[7] B. Jammeh, "DevSecOps: Security Expertise a Key to Automated Testing in CI/CD Pipeline," Research Gate, Poole, England, 2020.

[8] X. Ramaj, M. Sánchez-Gordón, V. Gkioulos, S. Chockalingam, and R. Colomo-Palacios, "Holding on to Compliance While Adopting DevSecOps: An SLR," MDPI Electronics, 2022.

[9] S. V. Deshmukh, D. S. Ahire, N. N. Chavan, N. D. Bharambe and P. Akshay.R.Jain, "IMPLEMENTING DEVSECOPS PIPELINE FOR AN ENTERPRISE ORGANIZATION," International Research Journal of Modernization in Engineering Technology and Science, vol. 3, no. 12, 2021.

[10] K. Carter, "Francois Raynaud on DevSecOps," IEEE Software, vol. 34, no. 5, pp. 93-96, 2017.

[11] Z. Ahmed and S. C. Francis, "Integrating Security with DevSecOps: Techniques and Challenges," in IEEE - 2019 International Conference on Digitization (ICD), Sharjah, United Arab Emirates, 2019.

[12] M. A. Akbara, K. Smolander, S. Mahmood and A. Alsanad, "Toward successful DevSecOps in software development organizations: A decision-making framework," Information and Software Technology, vol. 147, 2022.

[13] A. A. Zeeshan, "Compliance and Security," in DevSecOps for .NET Core: Securing Modern Software Applications, Apress, Berkeley, CA, Compliance and Security, pp. 265-278.

[14] R. Kumar and R. Goyal, "Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC)," Computers & Security, vol. 97, 2020.

[15] J. Díaz, J. E. Pérez, M. A. Lopez-Peña, G. A. Mena and A. Yagüe, "Self-Service Cybersecurity Monitoring as Enabler for DevSecOps," IEEE Access, vol. 7, pp. 100283-100295, 2019.

[16] T. H.-C. Hsu, Practical Security Automation and Testing, Birmingham, UK: Packt Publishing, 2019.

[17] B. Yadav, G. Choudhary, S. K. Shandilya and N. Dragoni, "AI Empowered DevSecOps Security for Next Generation Development," in Springer - ICFSE 2021: Frontiers in Software Engineering pp 32–46, Innopolis, Russia, 2022.

[18] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary and H. Fahmy, "Monitoring Real Time Security Attacks for IoT Systems Using DevSecOps: A Systematic Literature Review," Information, vol. 4, 2021.