Scrut Automation

Creating a DevSecOps Culture for Your Company

Contents

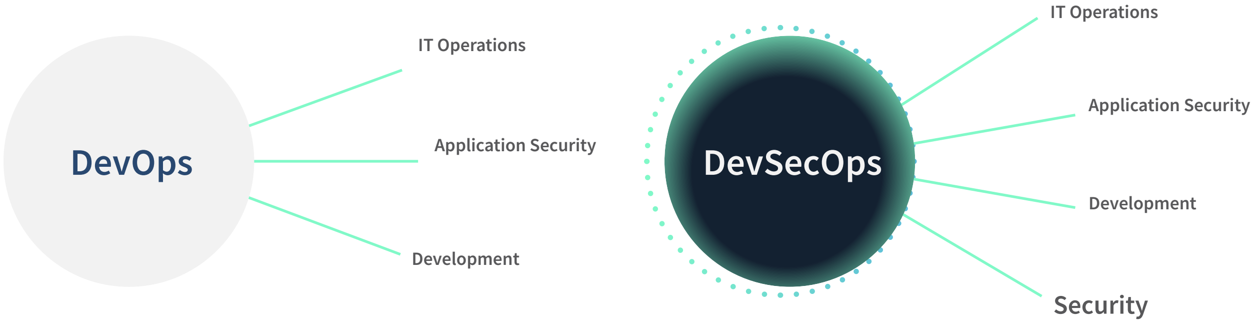
Introduction

DevSecOps, an extension of the DevOps process, is helping cloud-native organizations improve their development and operations by adding security to the mix. Getting to success with DevSecOps is about more than just procedures and toolsets, however.

Securing complex cloud infrastructure is more critical and more complicated than ever. Even though cybersecurity and compliance have never been easy to achieve, working natively in the cloud can make these workloads all the more challenging. Cloud-native businesses that lack a rigorous, comprehensive security program face not only risk exposure from increasingly sophisticated threat actors, but also compliance risks related to privacy laws and the like. It is thus imperative for security and compliance practices to be deeply integrated into the cloud-native software development lifecycle (SDLC).

Today, that means implementing DevSecOps, which adds security to DevOps processes. DevSecOps involves adding new tools and processes to the SDLC. Culture is also important for success. Making DevSecOps do its job and enable greater cyber defenses involves a cultural shift for Development, Security and Operations teams—as well as for stakeholders in compliance, legal and other parts of the organization. They must come together as one to forge a new way of thinking about security as it relates to the full SDLC in the cloud.

From DevOps to DevSecOps



Understanding DevSecOps requires first getting a good grasp of DevOps, the concept on which it is based. The term DevOps refers to the unifying of software development (Dev) and IT operations (Ops) processes and teams. The author and software developer Patrick Debois first coined the term in 2009. He, among others, was reacting to software quality problems that were becoming more serious and frequent as fast-paced agile software development methodologies took over from the traditional "waterfall" process.

With the waterfall approach, a dev team writes code and then, as the saying went, "threw it over the wall" to IT ops, who would put it into production. The two processes and teams were separate.

This was less of an issue when software releases occurred once or twice a year. With agile development and the continuous integration/ continuous deployment (CI/CD) pipeline, new code might be coming out every day. To resolve the inevitable difficulties that arose with this new tempo of software releasing, DevOps makes a software product's lifecycle into a shared responsibility among operations and engineering.

However, dealing with application security vulnerabilities still remained a separate process, outside of the DevOps workflow. This is a problematic gap, because, if anything, the new age of rapid code releases had the potential to increase cyber and compliance risks dramatically in software applications.

DevSecOps offers a solution by adding security (Sec) to the DevOps workflow and putting a priority on application and infrastructure security from outset. Dev, Sec, and Ops teams identify and remediate security issues starting at the earliest stages of the SDLC. Making DevSecOps work requires new processes and the integration of security tooling into the DevOps workflow and CI/CD pipeline.

Hence, DevSecOps is about more than just processes and tooling. It's a culture, one that must be nurtured carefully if an organization wants teams that can build functional and secure products for end-users.

Security Beyond Checking the Box

Too often, as the headlines reveal, an organization may believe it has performed all the necessary tasks required to be secure—only to weather a massive data breach or ransomware attack. While the cause of security breakdowns vary from business to business, one of the most common drivers of risk is a "check the boxes" approach to cyber defense. Security teams and their partners in compliance and IT operations buy and install the "right" solutions, like next-generation firewalls and intrusion detection systems, but they may not be thinking about security in the most effective way.

With cloud native software, which is exposed to more attack surfaces than software hosted in a standard on-premises environment, security works best when people come together in a culture of collaboration. This means DevSecOps, executed in a way that fosters human-centric principles and practices.

A healthy DevSecOps culture will have a positive impact on compliance as well as security. This is because, in general, the better an organization's security controls, the more robust its compliance efforts will be. For example, many security controls, such as those for identity and access management (IAM) serve compliance requirements as well.

A Closer Look at Compliance

Compliance, much alike security, cannot be treated as a “check the box” workload in a cloud-native company. To understand why this is the case, consider how frequently a cloud-native application changes. Its code base is updated frequently and its hosting environment along with other infrastructure parameters may also evolve more rapidly than is the norm with on-premises infrastructure.

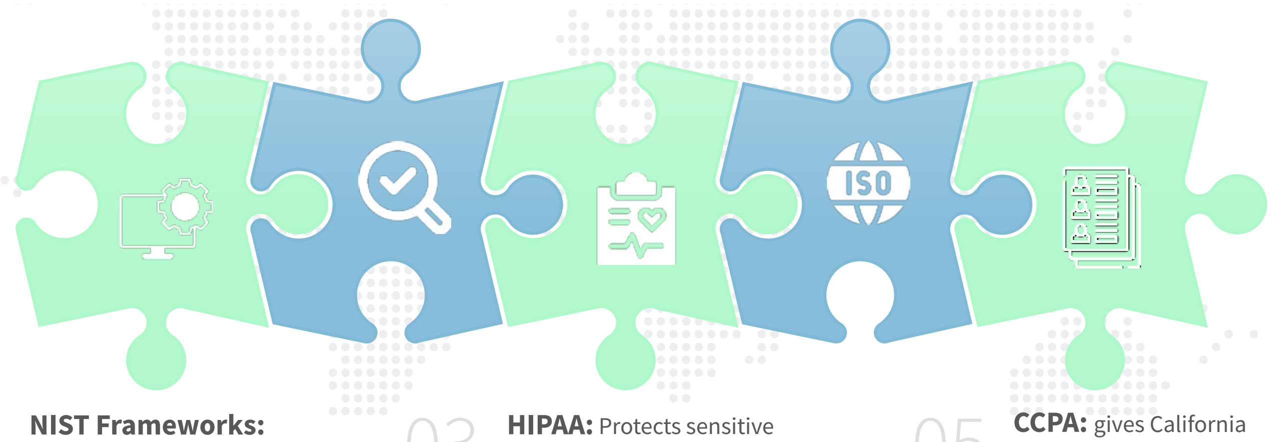
Each change has the potential to render a compliance control deficient. For example, if a new release introduces malware into the code base, that might expose an application to a data breach, which could cause a violation of privacy laws.

Cloud-native companies also tend to be at the forefront of digital transformation. This means forming new connections between systems, data sources, and devices—any one of which can potentially throw the organization out of compliance with the law or an industry framework. DevSecOps, as realized by a strong DevSecOps culture, is arguably the only way to mitigate this risk.

A DevSecOps culture is also essential for maintaining compliance with the various frameworks that affect software development and IT practices at cloud-native companies. Whether it’s a NIST framework, HIPAA or SOC 2, a strong DevSecOps culture will facilitate the achievement of desirable compliance outcomes.

02 **SOC 2:** Provides guidance to auditors in evaluating the operating effectiveness of an organization’s security protocols

04 **ISO 27001:** international standard for the management of information security



01 **NIST Frameworks:** overs the complete IT estate, including software development

03 **HIPAA:** Protects sensitive patient health information from disclosure without the patient’s consent or knowledge

05 **CCPA:** gives California consumers more control over the personal information that businesses collect about them

NIST Frameworks

The National Institute of Standards and Technology (NIST) promulgates multiple cybersecurity frameworks. Of these, the NIST Cybersecurity framework (NIST CSF) is one of the most popular and influential. It covers the complete IT estate, including software development. NIST CSF's five recommended areas of control span the identification (ID) of cyber risks and digital assets that require defense, protection (PR), threat detection (DE), response (RS) and recovery (RC).

ID
Identification Of Cyber Risks

PR
Protection

DE
Threat Detection

RS
Response

RC
Recovery

Each of these areas of control, if addressed in a sound security plan, will yield positive results in terms of compliance. And, in each area, a DevSecOps culture can enable compliance with the framework.

For example, control PR.AC-1 mandates the issuance, management, and verification of identities and credentials for accessing data or other digital assets. This may not seem like a control that relates to software development, but in a DevOps and CI/CD cloud-native environment, it most surely does. Each group of stakeholders in DevSecOps must think about how identity management figures into the DevSecOps workflow and apply DevSecOps principles to implement the control for all affected software in the pipeline.

SOC 2

Systems and Organization Controls 2, or SOC 2, is a framework developed by the American Institute of Certified Public Accountants (AICPA) to provide guidance to auditors in evaluating the operating effectiveness of an organization's security protocols. To be SOC 2 certified, a business must pass a rigorous SOC 2 audit.

SOC 2 covers security, system availability, processing integrity, confidentiality, and privacy. In each area, a DevSecOps culture can make a difference in how easily and efficiently a company can pass its SOC 2 audit. For instance, under confidentiality, SOC 2 recommends encryption, which is implemented during the development and software releasing process, or at least it should be.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the US federal law that protects sensitive patient health information from disclosure without the patient's consent or knowledge. In practical terms, HIPAA has led to the development and implementation of strict controls on patient data privacy. These include encryption, restrictions on data hosting, and more. To maintain HIPAA compliance, DevSecOps processes and culture should factor these controls into the SDLC.

ISO 27001

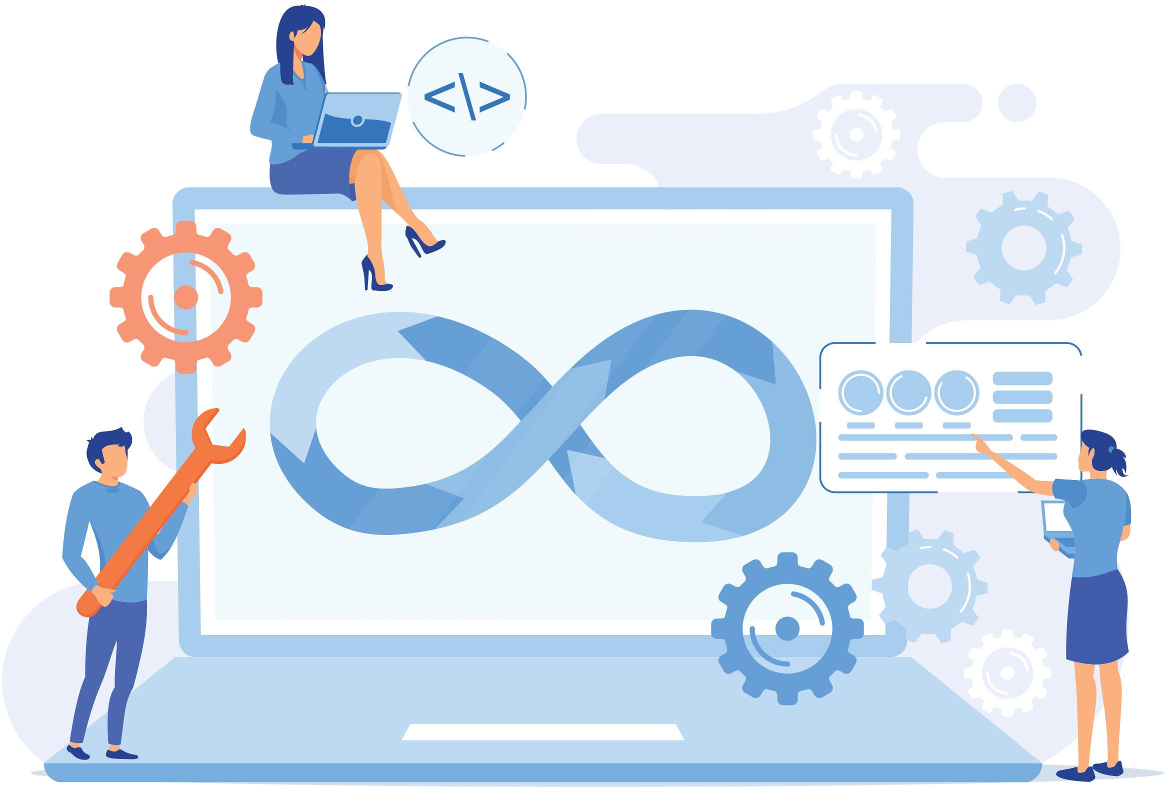
International Standards Organization 27001 (ISO/IEC 27001) is an international standard for the management of information security. To be certified as compliant with ISO/IEC 27001, an organization must systematically examine its security risks. This means taking account of threats, vulnerabilities, and impacts. From there, the company must design and implement a coherent and comprehensive set of controls and other risk mitigation countermeasures.

For a cloud-native business to comply with ISO/IEC 27001, it must factor the relevant controls and countermeasures into its SDLC. This is an achievable goal for an organization with a DevSecOps culture. Without one, compliance will be a significant challenge.

CCPA

The California Consumer Privacy Act of 2018 (CCPA) is an American state law that gives California consumers more control over the personal information that businesses collect about them. Like HIPAA, CCPA has led to the development of many controls over data privacy and security. And, also like HIPAA, CCPA comes with serious penalties for companies that violate the law, such as through a data breach.

A cloud-native company that needs to comply with CCPA, which is necessary if it does business in California, must embed all relevant data protection controls into its SDLC. This is easier to do when there is a DevSecOps culture at work than it is in a “check the boxes” IT culture.



Cloud Security-by-Design

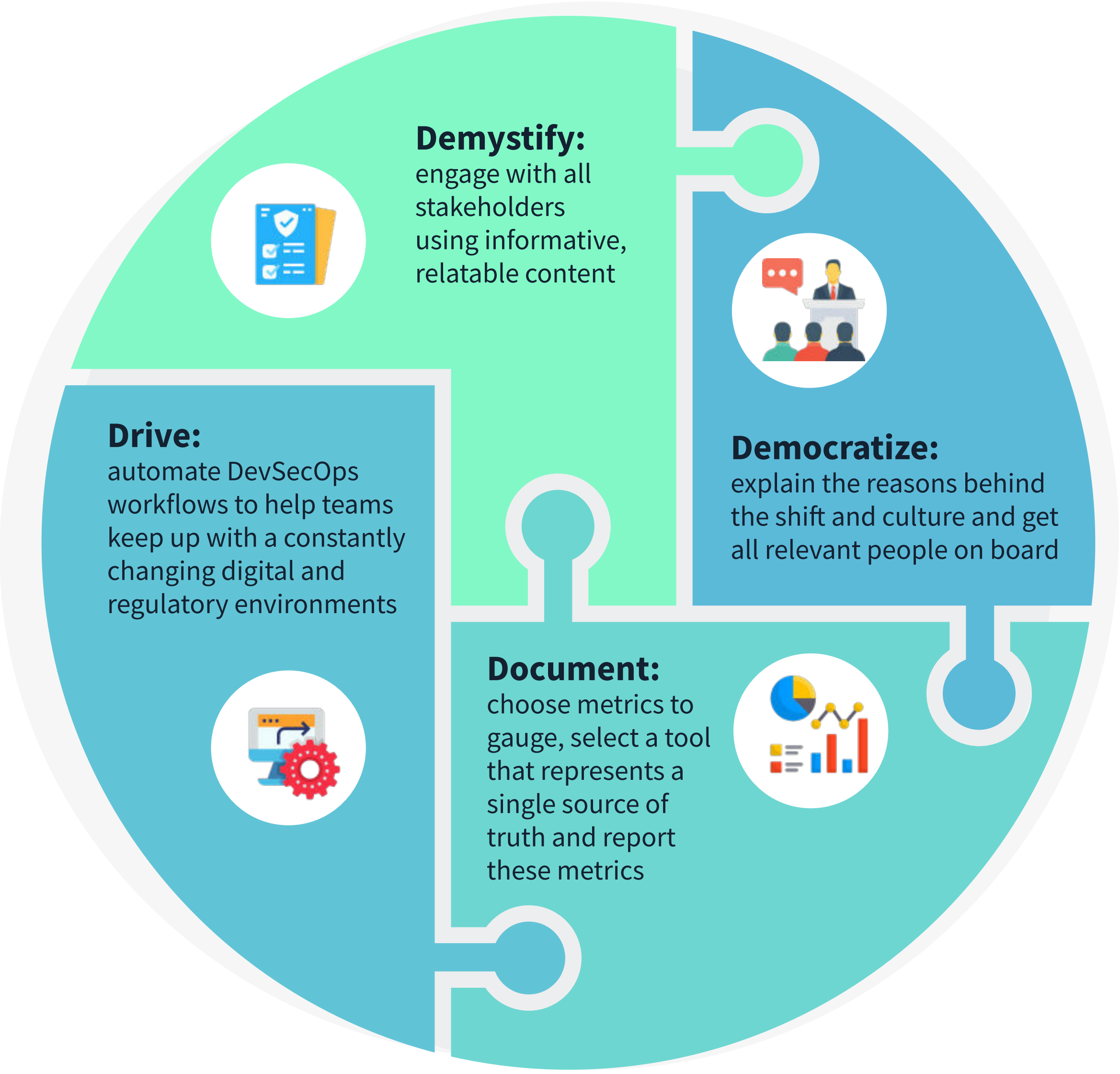
Creating a DevSecOps culture involves building security into a cloud-native product's design itself. The DevSecOps cloud security-by-design ethos calls for thinking thoroughly about every feature, every integration, and every hosting and infrastructure decision. As developers write code or use existing open-source code libraries, they must keep security and compliance in mind. This means communication and collaboration between stakeholders.

After all, developers may not know about the security and compliance ramifications of a particular coding choice.

Security-by-design must also be balanced with user experience. Everyone involved in DevSecOps has to channel end users and think about how they will interact with the product. As these two potentially conflicting forces come together in a DevSecOps culture, it is possible to build cloud-native products that are both; secure and easy to use.

Creating a DevSecOps Culture for Your Company

Given that proactive security operations are non-negotiable in today's dynamic threat landscape, what does it take to establish a DevSecOps culture that will build security into the foundation of the development process? At a minimum, everyone connected to Dev, Sec, and Ops must participate if the culture is flourish and become sustainable. Success then depends on a four step process suggested by best practices:



Demystify: engage with all stakeholders using informative, relatable content

Democratize: explain the reasons behind the shift and culture and get all relevant people on board

Drive: automate DevSecOps workflows to help teams keep up with a constantly changing digital and regulatory environments

Document: choose metrics to gauge, select a tool that represents a single source of truth and report these metrics

Demystify

Creating a DevSecOps culture may feel daunting for leaders and engineers alike. Many people in the organization may not be familiar with the basic idea of DevOps or agile development. They may not even understand how requirements for security and compliance affect software development. The best approach is to engage with all stakeholders using informative, relatable content. As people learn about DevSecOps and why it matters, they will likely embrace the idea and want to be involved in making DevSecOps culture a reality. Hence, **demystifying** the process gets everyone on board with tangible, actionable steps.

Democratize

Culture, by definition, needs to include everyone. If people feel that an idea is being pushed on them, it may not take hold in the right way. It's essential to **democratize the DevSecOps culture**. This occurs when leaders take the time to explain the reasons behind the shift and culture and get all relevant people on board. From there, people and teams need to be trusted to give input and take on the added responsibilities of DevSecOps.

Document

Some consider documentation to be the most critical step in creating a DevSecOps culture. Track and note the goals and methods for a DevSecOps culture, from the specific policies and processes to the higher-level principles involved. From there, the best practice is to choose metrics to gauge whether teams are moving in the right direction. This will ideally mean selecting a tool that represents a single source of truth, one that measures time to resolve security issues, number of vulnerabilities detected and so forth. It is necessary to report these metrics in a way stakeholders can easily understand. **This capability is also critical for maintaining compliance.**

Drive

Once the participants are committed to the idea of a DevSecOps culture, it's time to scale up and keep the process moving. Nothing stands still in IT, and with DevSecOps there are many moving parts. For this reason, automation is critical. Tools that automate DevSecOps workflows help teams keep up with a constantly changing digital and regulatory environments. Going further, using augmented intelligence whenever possible helps people be more productive, such as with AI-driven software testing.

Conclusion

Cloud-native businesses must defend their digital assets in a complex, increasingly hostile cyber threat environment. At the same time, compliance risks are growing ever more serious. The best approach for a cloud-native business that wants to achieve and maintain a robust security posture is to adopt DevSecOps. With DevSecOps, security becomes embedded in the SDLC. The frequently updated cloud-native software that is foundational the success of the business becomes more secure.

DevSecOps is a culture as much as it is a set of processes and technologies. When it's implemented in accordance with best practices, a DevSecOps culture helps teams innovate while keeping the company ahead of threats. Getting there means adopting a proactive mindset and the right tools.

This is where Scrut can help. Scrut makes it easier for companies to simplify and streamline information security for cloud-native companies. The solution enables the establishment of an enduring DevSecOps culture by offering complete visibility into cyber assets and helps manage infosec risks in a single platform.

Discover how **Scrut can streamline** the transition to a **DevSecOps culture at your company** by booking a free demo today.