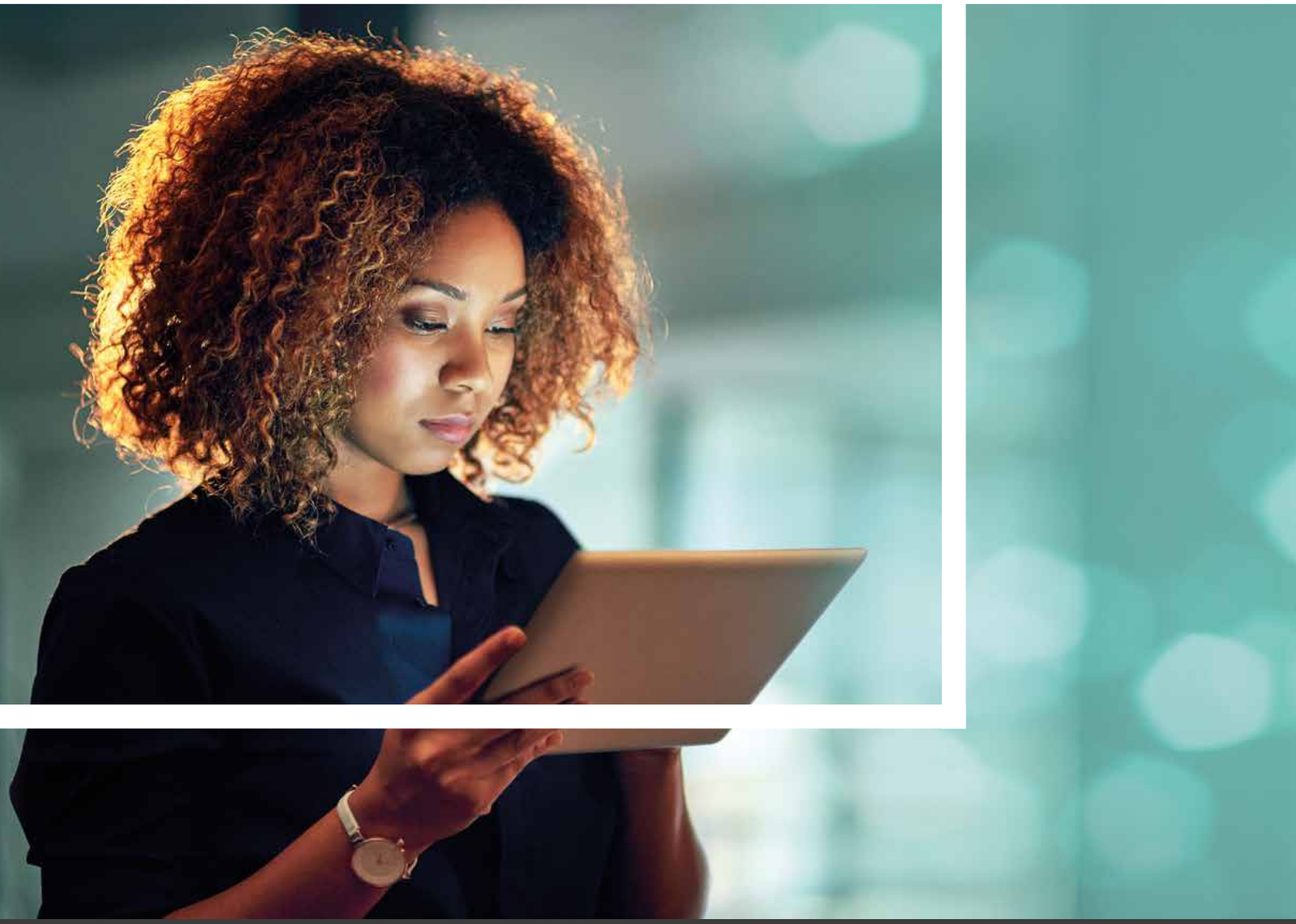
www.pwc.de/cybersecurity

DevSecOps

Reduce business risks by integrating security into IT development and operational processes



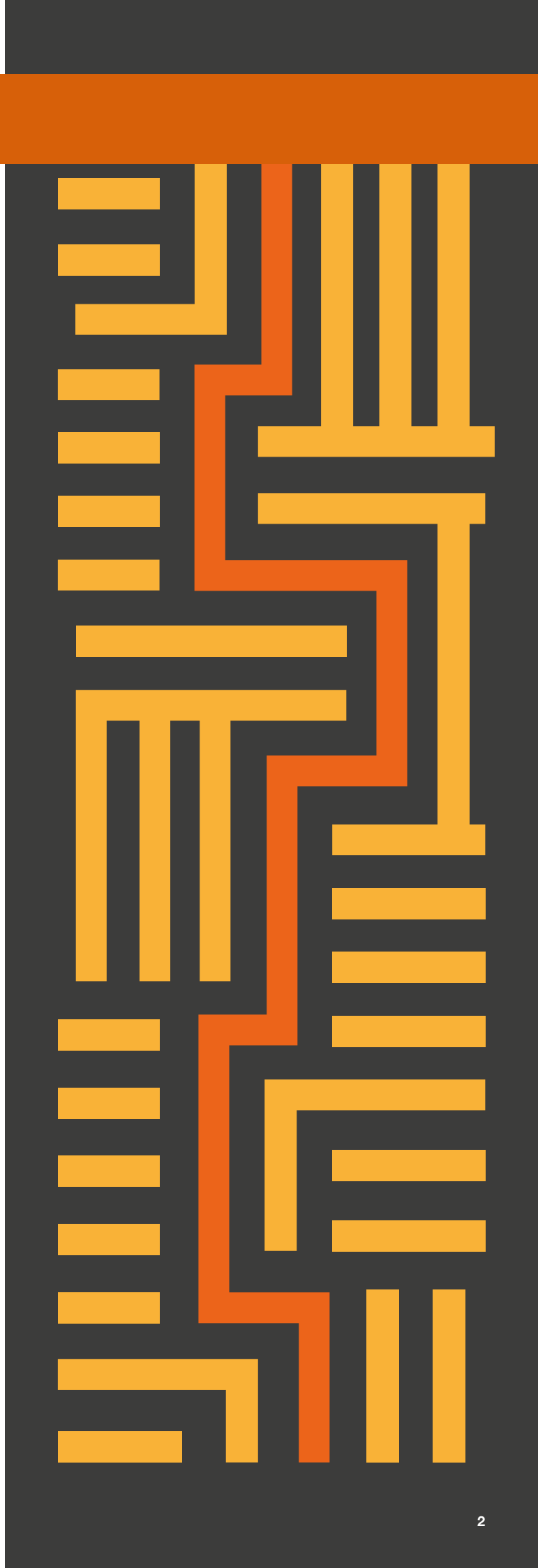
pwc

Background

Cybersecurity and minimising cyber risks are major challenges for companies worldwide. The number of security incidents affecting companies in various industries is steadily increasing, and cybercrime is becoming a lucrative business for criminals. The increasing complexity of IT systems also makes it difficult for companies to "think security" in every part of product life cycles and within their supply chains and business processes. As companies shift more and more of their business to the cloud systems, their attack surfaces grow.

Continuous security in IT systems and products using traditional development and operating processes cannot keep up with today's rate of attacks and modern attack strategies. Security has played a rather minor role in the development of IT systems and products in the last ten years: it's usually only thought about, analysed and tested at the very end of the development process. In many cases, this late focus on security prevents efficient handling of errors and problems that arise, and consequently leads to insecure IT systems and products being launched. If security incidents occur during operations, remedying the underlying security issues is very expensive. Loss of the company's reputation increases these costs even further – especially if issues come to light after a product has been launched on the market. Attacks themselves can also cause severe damage, as the ever-increasing use of digital technology means that cyberattacks can nowadays have an effect on the real world: hackers might succeed in disrupting vital systems in hospitals, compromising self-driving vehicles or interrupting supply chains.

In summary, IT and OT security needs to be integrated by design in a very early stage within the software product lifecycle without delaying product launches and slowing down business agility.

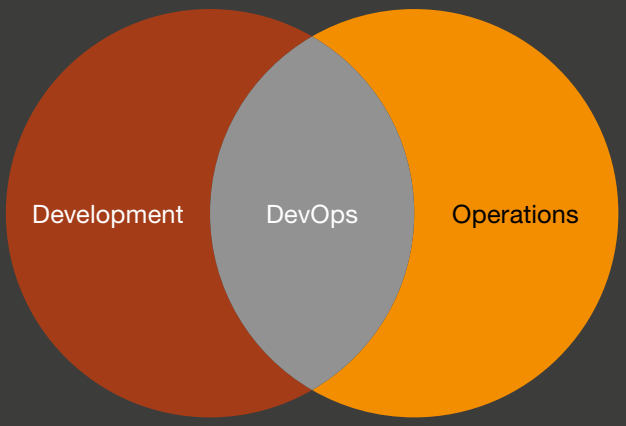


DevOps

Many companies are adopting the DevOps approach to IT product development and lifecycle management. DevOps is made up of development and operations and allows the processes from these two units to merge and work together smoothly and continuously. This approach presents several advantages for businesses:

- Faster go-to-market
- Efficient importing of changes/new releases
- More agile work methods/simplification of complex work processes
- Increased automation in the development process
- Continuous product testing
- Higher-quality work processes (using automation tools)
- Enhanced business performance

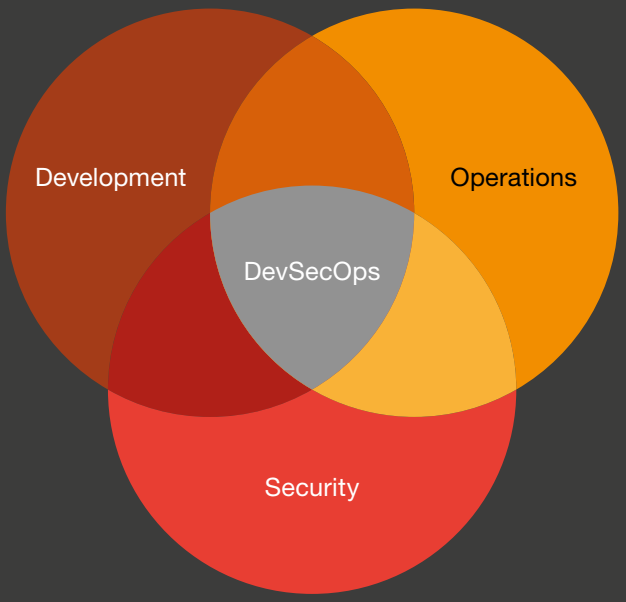
… but misses the overaching topic of security.

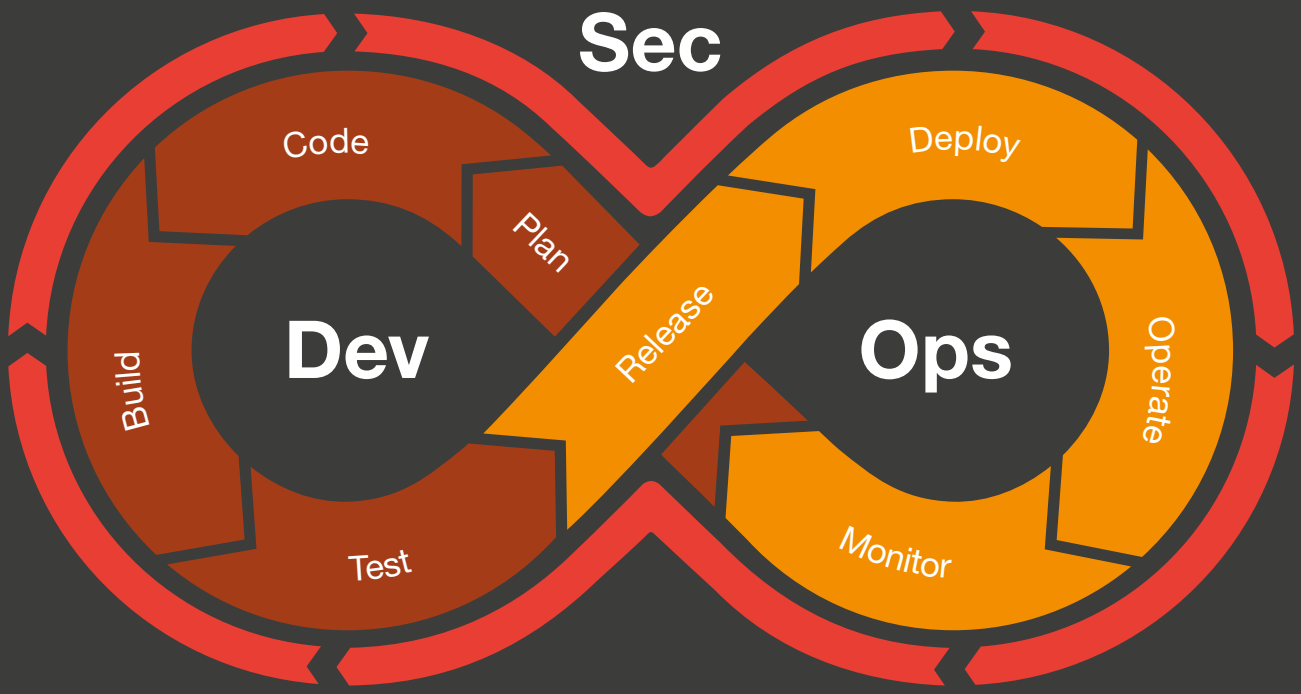


DevSecOps

The DevSecOps approach was introduced to include security in the development and operating life cycle management process from an early stage. Here, the topic of security is considered and integrated at every stage of development and operating processes, adding an extra layer around the DevOps concept. This allows companies to efficiently deal with the issue of security:

- Integrating and testing security in all phases of development and operating processes
- Using secure IT systems and products to provide inherent safeguarding of business processes
- Minimising the risk of cyberattacks
- Automation of manual security tests
- Agile and flexible implementation of changes at short notice, keeping security in mind





Many software products, various deployment stages (e.g. development, testing, production) and complex infrastructure are involved in the software development process, meaning that a large number of access requests for specific resources (e.g. file shares, databases, code snippets) arise at various stages of the IT product lifecycle. These requests must be authenticated with credentials. However, credentials are often not properly secured, and thus offer attackers a gateway into company networks. One option available to attackers is to escalate privileges gained from attacking, or "sniffing" credentials – moving around a company network by collecting more and more privileges. Credentials play a role in the vast majority of all cyber attacks, as they are essential targets for spying on and manipulating an IT system or product. To defend against this, DevSecOps requires adherence to the principle of least privilege: this offers major benefits, since each set of credentials only authorises access to specific resources.

It is for precisely these reasons that security was added to DevOps to create DevSecOps, as well as to secure general processes and address vulnerabilities during the Software life cycle. Besides thinking about traditional development and operational lifecycle processes, more and more companies are adopting a cloud-first strategy, but doing this safely requires every step towards cloud systems to be thought about and planned with security in mind – whether it's a company-wide changeover or a specific business case. DevSecOps, therefore, must always play a role in the transition to cloud systems.

Integrating security into the individual phases of development and operating processes minimises sources of error and the attack surface exposed to cybercriminals during the provisioning of IT systems and products. Traditionally, lack of integration of security enabled vulnerabilities in IT systems or products to be exploited during these phases of development or operation. By contrast, the DevSecOps approach continuously subjects various units in the company to security checks, allowing vulnerabilities to be dealt with proactively. Security gaps found and fixed after a product is launched on the market are significantly more expensive than security gaps identified and fixed during the development process.

Business processes also benefit from the agile approach of DevSecOps: agile working makes it possible to react quickly and effectively to new requirements or changes in the business or on the market while still keeping an eye on security. Automating security benefits the entire company by reducing costs resulting from errors and making remediation of errors more efficient.

Challenges

What challenges do companies face when introducing and implementing DevSecOps?

DevSecOps requires security to be considered in all areas within a company, and responsibility for security must be distributed across various actors within the development and operating processes. When introducing this new approach, the first step to take is to restructure familiar working methods – and in doing so, bring about a cultural change in the company. As well as ensuring practical implementation of agile working at lower corporate levels, it's also vital that upper management levels think about agile and "live agile". A uniform understanding of agile is essential for acceptance and successful implementation. Without an open corporate culture and without exchange between teams and departments, the concept will fail.

Different industries face various challenges when adopting to new IT product lifecycle processes. There are many sets of regulations that companies have to fulfil (e.g. MaRisk, BAIT, ISO/IEC 27001). DevSecOps is a great enabler for aligning company processes with the regulations, helping companies to stay compliant throughout the product life cycle.

IT and OT security by design means also thinking about an eficient and secure software development process through the whole software lifecycle.

Solution approaches

DevSecOps uses an approach known as the zero-trust-model to ensure secure communication in the digital world. This model is a cornerstone for reducing the costs of business continuity planning and disaster recovery planning, and works on the basis of interpreting every communication between different assets as insecure. This approach enforces authentication and authorisation every time a connection is established, and assets are only trusted if they have been explicitly approved. This is where secrets management solutions come into play.

Implementing these solutions means that companies can enable digital transformations, optimise user experience and ensure security in services such as remote working. This whole approach – DevSecOps, using the zero-trust model and managing critical assets with a secrets management solution – is cloud scalable and hybrid cloud scalable, and drives frictionless interaction to improve DevSecOps retention.

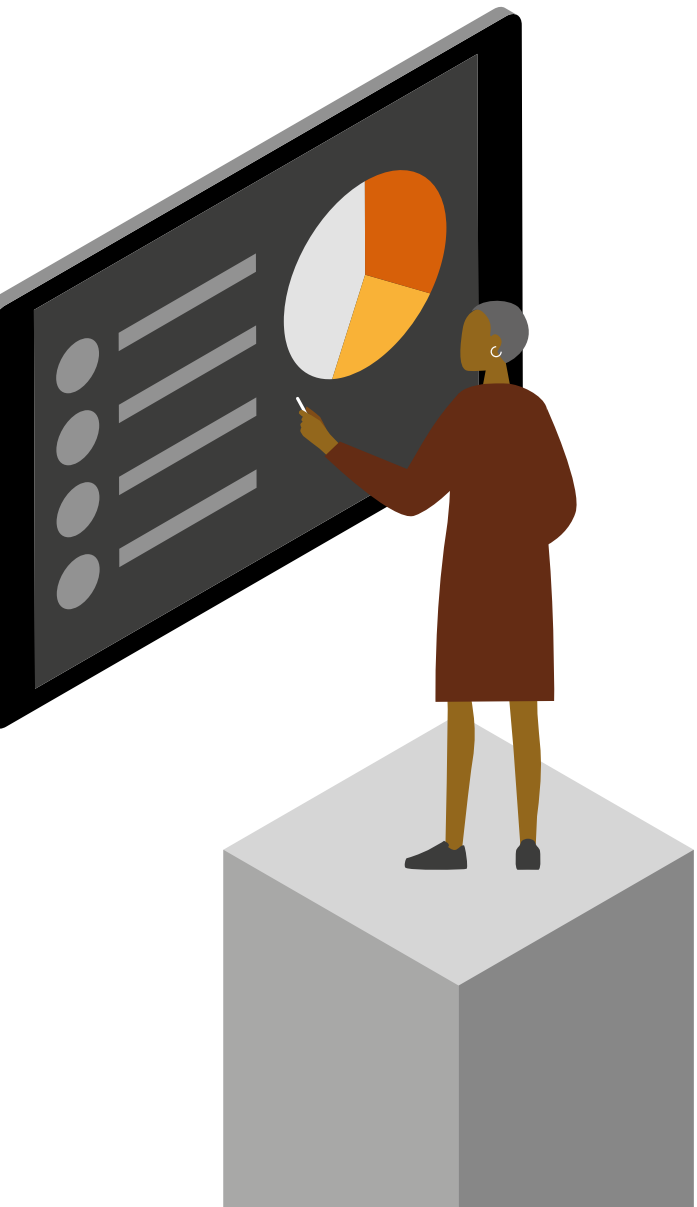
Mitigating cyber risks is already a key target for companies, and it will only become more important in the future. Using the zero-trust model and implementing this approach throughout the whole development and operational life cycle of a Software or business process will reduce these cyber risks to a minimum. To ensure success, it's important to walk through the company's business processes, taking a risk-based approach to identify business-critical assets and processes. Next, pinpoint the processes that are responsible for development and operations, and move these to DevOps one step at a time. Once migrated to the agile approach of DevOps, identify critical information within the processes and create controls to secure this information (e.g. introducing new security software or a new approval processes).

Conclusion

Automation and digitalisation of the economy will continue to be key topics over the coming years, as will agility to enable companies to compete within the market and within different industries. Approaches such as DevSecOps will be essential for companies to effectively compete in the economy of the future and to avoid getting hung up on internal digital evolution.

Digitalisation is an inexorable process, and it is far easier for companies to proactively address IT security at an early stage than to be forced into doing so by the market later on. With more and more business-critical assets and processes being shifted to cloud systems, companies simply cannot afford to ignore IT security any longer. Industries need to adopt new perspectives and factor in IT security – after all, cybercrime is one of the biggest risks for companies working in the digital world.

PwC and CyberArk can offer guidance and targeted expertise to help with establishing IT and OT security by design and higly integrated and efficient DevSecOps processes.



Contacts

Sven Schreyer
Director
Cyber Security & Privacy
Tel: +49 1512 8493188
sven.schreyer@pwc.com

Linda Noack
Senior Manager
Cyber Security & Privacy
Tel: +49 151 658 759 91
linda.noack@pwc.com

About us

Our clients face diverse challenges, strive to put new ideas into practice and seek expert advice. They turn to us for comprehensive support and practical solutions that deliver maximum value. Whether for a global player, a family business or a public institution, we leverage all of our assets: experience, industry knowledge, high standards of quality, commitment to innovation and the resources of our expert network in 155 countries. Building a trusting and cooperative relationship with our clients is particularly important to us – the better we know and understand our clients' needs, the more effectively we can support them.

PwC Germany. More than 12,000 dedicated people at 21 locations. €2.3 billion in turnover. The leading auditing and consulting firm in Germany.