unlocking security
to create the future you trust in

aktios:

rest secured,
we’ve got IT covered

secdevops

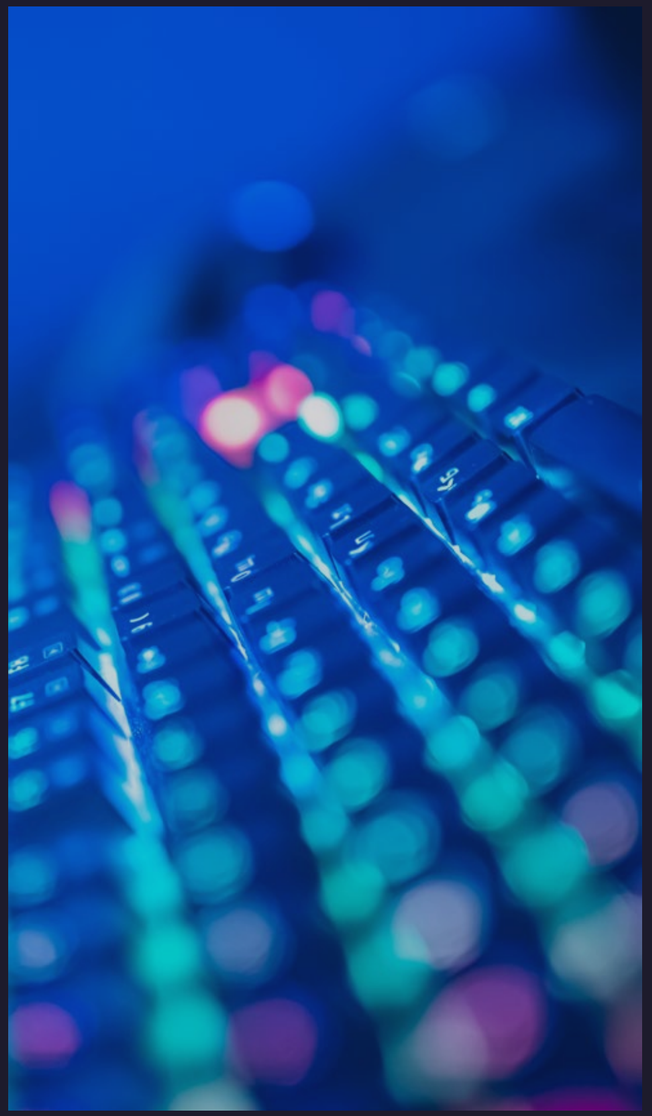
code strong, defend right

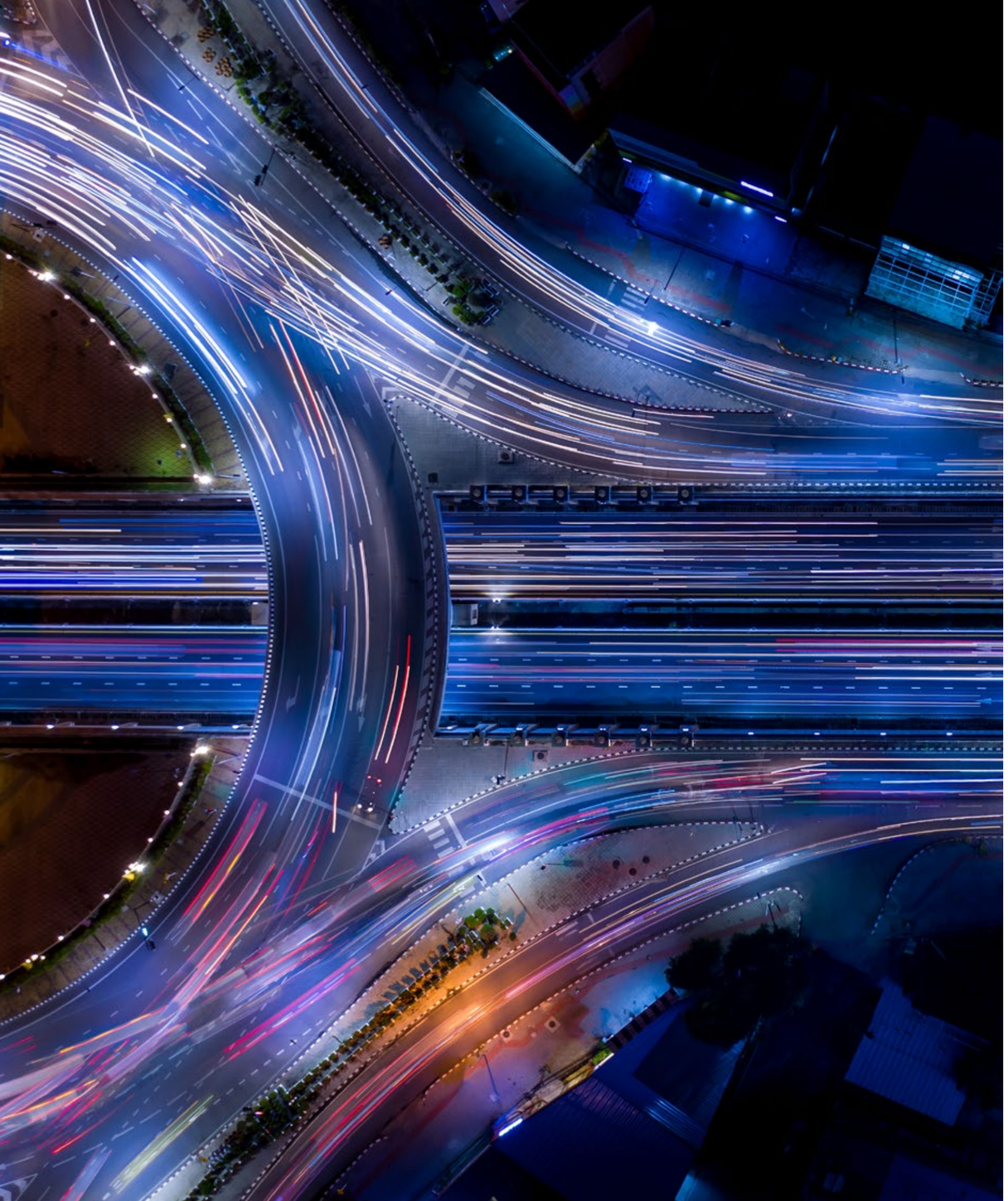
We are an innovation-oriented company that specializes in development and cybersecurity solutions.

Our team consists of technology enthusiasts who battle on all fronts, equipped with creativity and expertise.

Yet, what sets us apart is our unconditional commitment to security and quality.

We invite you to explore our culture of safe development.





foreword

The lesson we have learned in the past years of crisis and pandemics is that we can no longer know with certainty how events will unfold. What we can do, however, is to rely on people, on our frontline teams, to detect the signs and correctly react to unpredictable and rapidly changing situations.

During a crisis or in the face of an incident, our teams are the true guardians of the company's future and resilience. Thus, we must do everything in our power to enhance their already remarkable ability to adjust to various circumstances by providing them with the right framework and tools.

Cybersecurity plays a fundamental role here because, in a vulnerable scenario, it will provide the insight, tools, and trust needed to reinvent your business, limit exposure, and thereby secure the future of your organization.

The goal is to integrate security into our mindset, processes, and day-to-day operations. If we want to achieve operational excellence, we must embrace the challenge and take advantage of this complete change of culture, both in organizational and operational aspects. To accomplish this, we need to start from the source, shifting it all to the left:

Shift left is a practice of addressing cybersecurity from the preliminary stages of any project. By setting a common framework for all teams and using Security by Design and SecDevOps approaches, it helps to address different needs such as agility, efficiency, and security at a practical level. And exactly here, at this fragile balance point where strictness meets flexibility, lies the aforementioned operational excellence.

For quite some time, cyber threats stopped being seen just as a technological risk. The harsh reality is that they pose an extremely critical business threat.

Hence, security architecture cannot be an obstacle to the efficiency or agility of operations; it must be built as an incentive for value creation.

leverage for excellence

Security by Design and SecDevOps are the two approaches that best embody the previously mentioned concept of 'shift left'. The idea is to change the focus from solely security concerns to the earlier stages of projects as well. Addressing the security aspect from the earliest stages and raising awareness of threats and corresponding responsibilities among all people involved allows, on the one hand, making technical and functional decisions that minimize risks (for example, avoiding, as much as possible, certain personal data), and on the other hand, promptly addressing vulnerabilities that would be more complex and costly to handle later on.

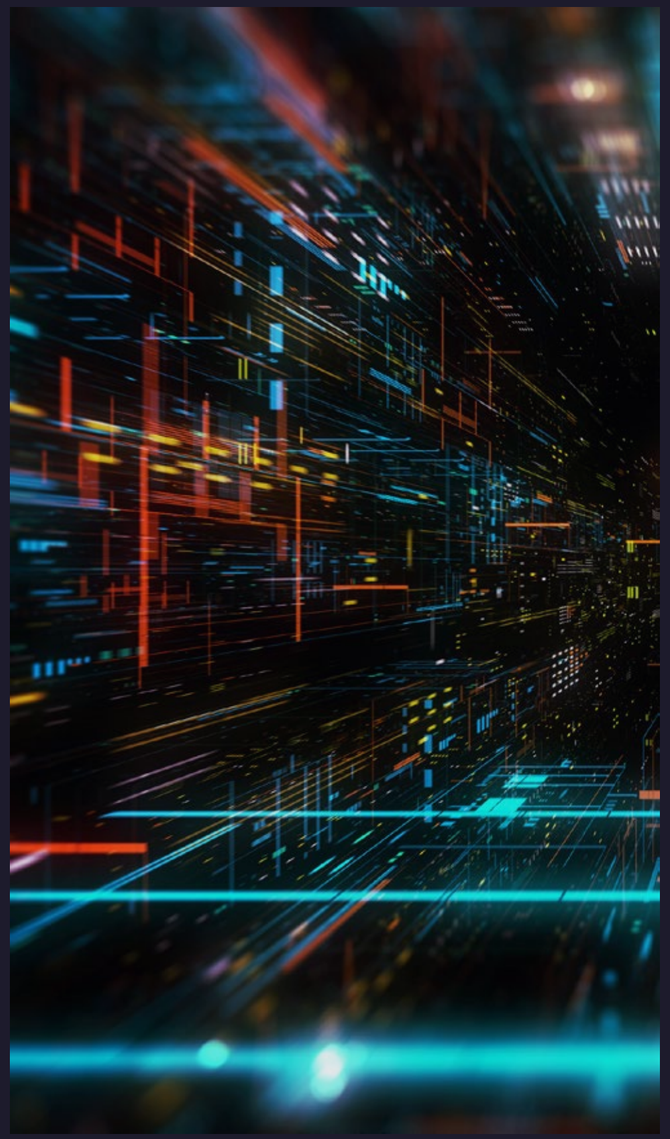
key value drivers

Agile	Faster and more agile delivery and reduced 'time to market': SecDevOps enables more effective application delivery and confident iteration to protect and enhance benefits. Integrating security into DevOps workflows eliminates potential bottlenecks and accelerates the efficiency and agility of organizations.
Risk reduction	Improved security posture and risk reduction: SecDevOps integrates security and its practices throughout all stages of the software development lifecycle and service operations. That, in turn, leads to better collaboration, deeper trust, and greater transparency among development, security, and operations teams resulting in lower-risk software.
Reduce costs	Reduced development and operational costs: SecDevOps practices accelerate the development lifecycle and eliminate the vast majority of issues before they reach the production stage. All potential incidents are resolved seamlessly and very quickly.
Improved experience	Improved customer experience and satisfaction: Thanks to producing higher quality and more secure software, SecDevOps increases the value organizations provide to their customers. Customers themselves also appreciate more frequent enhancements and updates to the solutions. In addition, customer satisfaction also increases when organizations look at systems from the perspective of end users and have insight into the end-to-end customer journey

devops, devsecops...

DevOps emerged more than ten years ago to improve the speed and quality of development and execution of software as well as promote greater collaboration and shared responsibility between the development and operations teams. DevOps is a paradigm that focuses on the functional characteristics and performance of software, and, unfortunately, within this model, security is either a bottleneck or is ignored. Security teams continue to exist in a separate silo with distinct tools, culture, and processes from their DevOps counterparts.

That is why, DevSecOps is the next logical stage in the evolution of the DevOps approach. By integrating security teams and practices into DevOps workflows, you can further accelerate the speed of delivery, improve software quality and increase the reliability of services in production. Breaking down silos between security and DevOps teams is essential to unlock the full potential of the DevOps approach.



...and secdevops

SecDevOps takes it even a step further by highlighting the security's presence at the first stage of the Software Development Cycle (SDLC). In DevSecOps, security is integrated into all phases of the SDLC, whereas in SecDevOps, security is the first step of the SDLC.

This approach encourages taking into account security principles and standards throughout the entire process of creating the application. It is applied even as early as the steps prior to the development lifecycle and deployment of software. Security is integrated at every stage and is supported by adequate tools right from the beginning.

In the current, hyper-competitive world where the threat landscape is rapidly changing, and some risks can even jeopardize business survival, no organization can afford security vulnerabilities in production systems.

SecDevOps is proactive rather than reactive: a culture of 'security first' truly enables the creation of reliable, available, resilient, easy-to-defend, and long-lasting software.

Creating a thriving SecDevOps environment doesn't simply start with IT tools and technology; it's all about fostering a culture that prioritizes security.

laying the groundwork

people and culture

People and culture, two elements that form the genuine foundation of safe development. It encompasses the values and structure of the organization, the communication model, the leadership style, etc... and also entails fostering:

- an open mindset, cherishing transparency and accountability
- right training to empower teams and individuals in making agile critical decisions
- team members capable of promoting and reinforcing the security culture and awareness

laying the groundwork

processes

Processes: an optimized framework to implement this culture, with a particular emphasis on:

having adequate documentation, right from the start of risk analysis and threat modeling, to respond swiftly and in a standardized manner to potential problems or incidents.

establishing objectives and indicators for security as well for continuous improvement and measurement.

ensuring that each of implemented methods facilitates communication and feedback among all individuals and teams.

laying the groundwork

technology and tools

Technology and tools, essential for governance, elimination of inconsistencies and to reduce the complexity of integration by relying on:

fostering automation, observability, and traceability through infrastructure and security 'as Code' scripts, static and dynamic analysis, and integration testing with existing code.

solutions that allow early detection of possible failures, automated validation, and functionality and security testing in infrastructure, not just within the code.

careful choice of tools and fine-tuning them to reduce alert fatigue, minimize false positives, and integrate seamlessly into the ecosystem.

secure CI/CD

a high-level checklist

training

pre-commit checks	Threat Modeling Architecture Risk Analysis Manual Code Review Email Notifications Configuration Review
commit checks	Compile and Build Code Run SAST Tools Automatic Security Testing Gather Metrics
build checks	Comprehensive SAST SCA Risk Based Security Testing Gather Metrics
test checks	Broader SAST DAST/AST Malicious Code Detection Gather Metrics
pre-deploy checks	Configuration Management Provisioning Runtime Environment
deploy checks	Security Scanning Vulnerability Scanning Bug Bounty Threat Intelligence

monitoring

major challenges to overcome

difficulty in
recruiting security talent

SecDevOps addresses this problem by encouraging development and operations teams to share responsibility in protecting systems, equipping them to do so by providing frameworks and tools that implement security.

resistance
to change

While some friction may arise in the initial stages of change, awareness, transparency, collaboration, and synergy among people and teams ultimately lead to a positive outcome. A critical aspect here is the design of the processes. We need to ensure that security is seen not as a hindrance or scrutiny but as another important and valuable element.

a myriad of
production environments

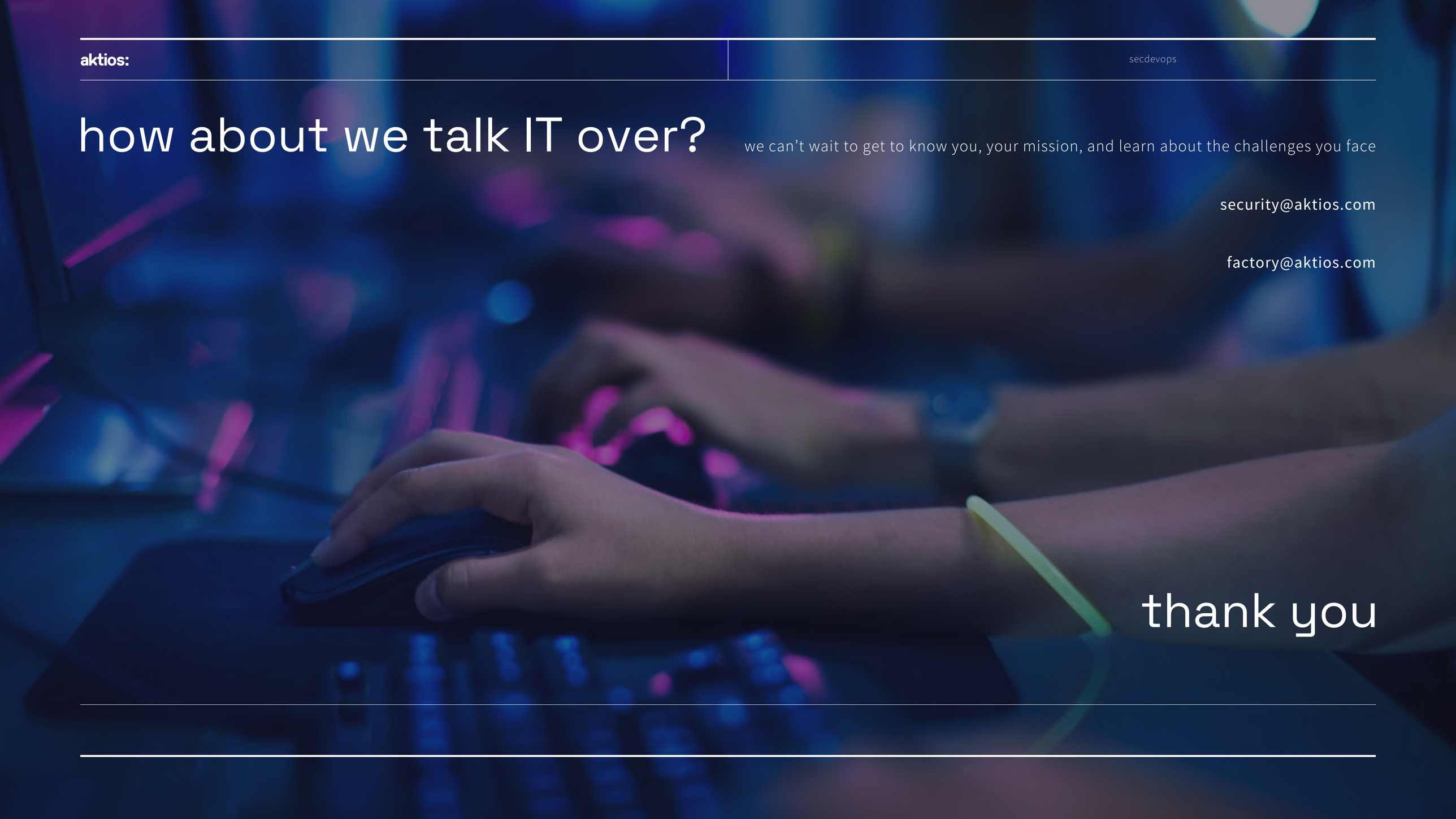
Ensuring consistency across hybrid and diverse environments is the foremost security challenge in the cloud era. The only way to confront it is to put the right technology in the hands of different teams. Distribution of suitable tools and solutions throughout the entire cycle is the key to maintaining control.

how about we talk IT over?

we can’t wait to get to know you, your mission, and learn about the challenges you face

security@aktios.com

factory@aktios.com



thank you

rest secured,
we’ve got IT covered

aktios: