NETWORK INTELLIGENCE

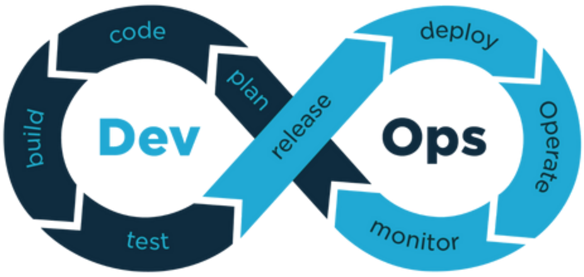
The Digital Security Company

DevSecOps

A Concept Note

What is DevOps?

DevOps is a software development methodology that combines software development (Dev) with information technology operations (Ops). The goal of DevOps is to shorten the systems development life cycle while delivering features, fixes, and updates frequently in close alignment with business objectives.
DevOps aims to maximize the predictability, efficiency, security, and maintainability of operational processes. To implement DevOps successfully in an organization, it's necessary to address the following aspects:



People

•Educate the team
•Adapt cultural change (Collaboration, Sharing, Team work, Organized, Self-Competent are the primarily cultural changes)

Process

•Develop and follow a streamlined delivery process, deployment process and feedback process.
•Follow CI/CD pipeline

Technology

•Using the right tools in order to automate or simplify processes

DevOps Pillars

Implementation of DevOps automation in the IT-organization is heavily dependent on tools, which are required to cover different areas of the systems development lifecycle (SDLC):

1. Infrastructure as code — Ansible, Puppet, Chef
2. CI/CD — Jenkins, Shippable, Bamboo
3. Test automation — Selenium, Cucumber, Apache JMeter
4. Containerization — Docker, Rocket, Unik
5. Orchestration — Kubernetes, Swarm, Mesos
6. Deployment — Elastic Beanstalk, Octopus, Vamp
7. Measurement — NewRelic, Kibana, Datadog
8. ChatOps — Hubot, Lita, Cog

Why DevOps?

> *Teams that practice DevOps deploy 30x more frequently, have 60x fewer failures, and recover 160x faster.*
>
> *-Puppet Labs State of DevOps Report*

Adoption of DevOps is being driven by many factors – including:

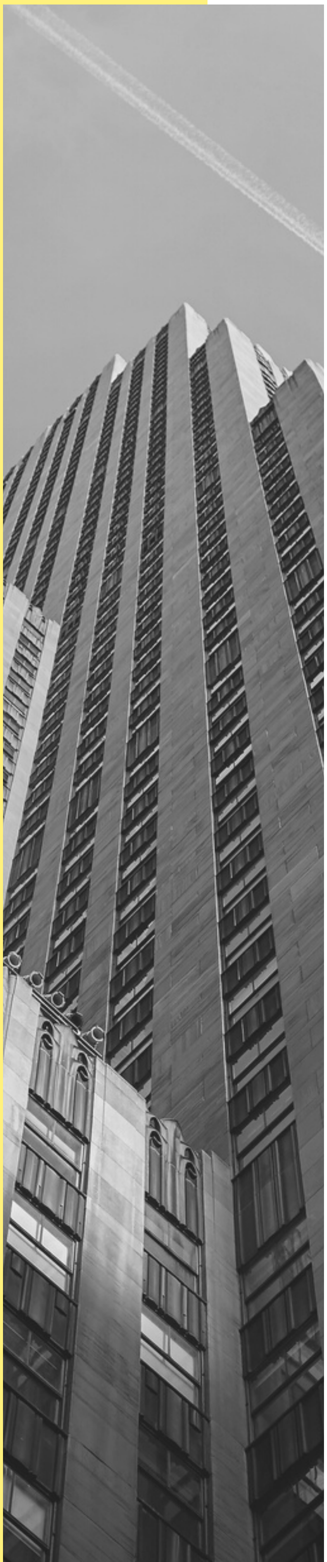
- Use of agile and other development processes and methods;
- Demand for an increased rate of production releases – from application and business unit stakeholders;
- Wide availability of virtualized and cloud infrastructure – from internal and external providers;
- Increased usage of data center automation and configuration management tools;
- Increased focus on test automation and continuous integration methods;
- A critical mass of publicly-available best practices.

Some of the benefits that DevOps seeks to deliver are listed below:

- DevOps aims to reduce conflicts between teams and promote faster delivery of product with increased transparency.
- Traditional application development approaches, while typically rigorous, are often time-consuming and inflexible.
- Usually the development team and the operations team work in silos. By adopting DevOps these communication barriers between the teams are broken so that the software delivery process and the deployment process can happen effectively. These processes are further fastened with the power of automation.
- Some of the roadblocks which usually appear in traditional development methodologies are:

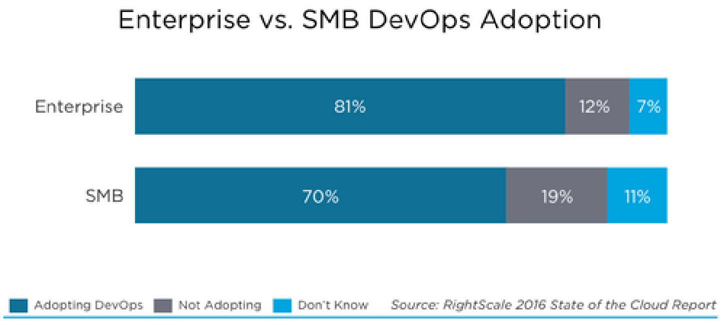
1) Weak collaboration
2) No or less visibility
3) Increased time to market
4) Existing legacy processes & tools
5) Lack of teamwork
6) Lack of transformation and adaption to changes

Characteristics of DevOps:



Since DevOps isn’t an overnight shift, but rather a gradual journey, some of the aspects that signal a mature DevOps environment would be:

- Faster delivery à approx. 50+ deployments per day
- More focus on delivery and less on design à DevOps with the help of Agile methodology puts less focus on design and more on building and delivering an MVP to the customer continuously.
- Code-driven configuration management and infrastructure provisioning.
- Microservices to achieve FaaS (Function as a Service) & BaaS (Business as a Service)
- Rapid self-service system packaging and provisioning with technologies like OpenShift, Docker, Terraform, Vagrant.
- Eliminating process bottlenecks
- Achieve segregation of duties
- Most importantly reduce overall cost and failure rates typically associated with software development



Source: RightScale 2016 State of the Cloud Report

RightScale statistics of DevOps adoption

What is DevSecOps?

Embedding security into the DevOps processes is referred to as DevSecOps. While DevOps addresses the business need of rapidly delivering products and release code in order to satisfy customer demands, it is important that security must work in tandem with Agile and DevOps processes.Just as DevOps addresses the traditional silos between Development and Operations, DevSecOps seeks to address the silos between Dev, Ops and Security teams. Automated application security further facilitates reducing friction and removing bottlenecks in the CI/CD cycle.
Let’s take a high-level view of how security would get embedded into the People, Process, Technology triad of DevOps:

In traditional development methods, security is kept at the very end of the release process. Hence, security has been viewed as a bottleneck to the rapid development methodologies such as Agile along with the software delivery pipeline.
This results in a major contention and distrust between development and security teams unless they work in tandem.

People

•Organization-wide security awareness
•Integration of security team within development and operations teams
•Weightage to security team in the process

Process

•Define processes which integrate security in development cycle.
•Clearly document and communicate it
•DevSecOps aims to align processes to achieve secure development as a whole

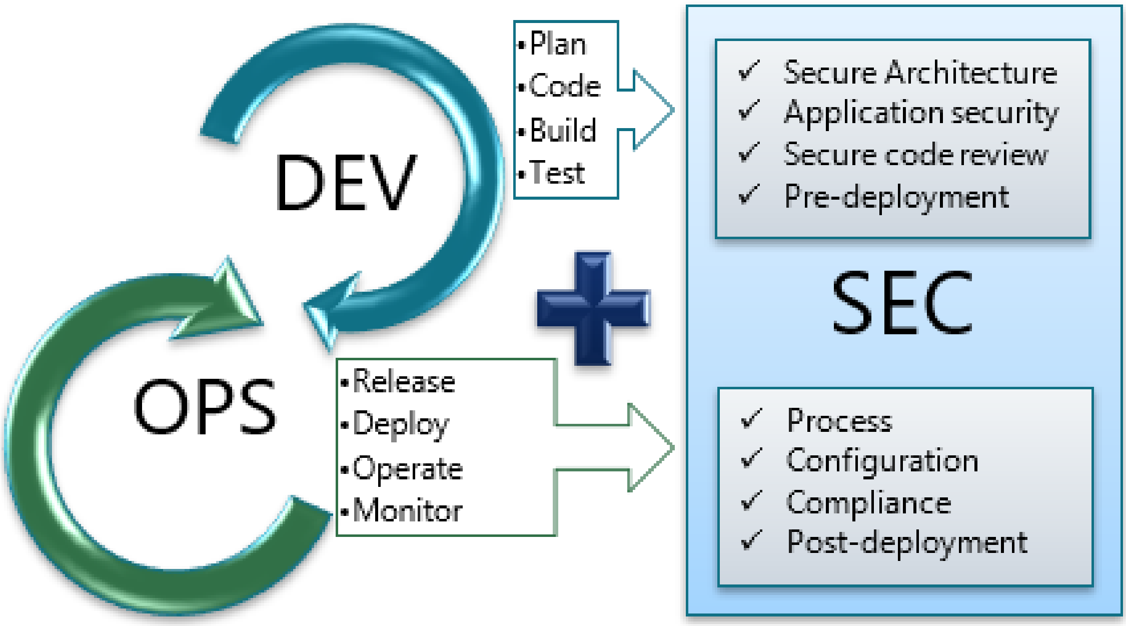
Technology

•Technology helps in automating security, ensuring right defences in development lifecycle

Our DevSecOps Approach:

We work with numerous organizations – both in the technology and traditional industry verticals who are at various stages of DevOps maturity. And help them embed security within the DevOps cycle through the reengineering of processes, implementation of security tools, and integrating security engineers into the DevOps teams.

Our consultants have extensive experience in the field of application security of cutting across various technology platforms such as ASP, ASP.NET, Java, PHP, Ruby on Rails, C++, etc. as well as difference architecture such as MVC



Key Principles:

Automate security

The ability to automate security testing through scripting, static and dynamic analysis, composition analysis, and integration of testing within existing tools and processes goes a long way toward identifying flaws early in the lifecycle and speeding up the delivery of secure code

Detecting Security Flaws Earlier

DevSecOps aims to find code vulnerabilities early and this requires IDE plugins that deliver immediate feedback to the developer if a piece of code that they are writing is insecure

Eradicating false positives

Achieving an effective “break the build” approach requires technology that can deliver valid findings via reports and dashboards, creating operational visibility. False positives must be kept low to ensure development teams trust that security tools won’t create additional work for them. Our teams help in configuring automated tools and analyzing their output in such a way that these cases are reduced, and accuracy of tool output is increased

Focusing on orchestration

As almost everything, including infrastructure becomes code, finding and eliminating vulnerabilities is mission critical. We can help organizations to align multiple security systems, processes and controls to bring in security orchestration within the CI/CD cycles

Architecture Level Consulting:

Threat Modeling

For DevOps – threat modeling service is delivered in different stages. In this phase, our consultants help the organization by building multiple attack scenarios (which are also known as Abuse Cases) at each stage. Further, each stage evaluates security measures in the DevOps lifecycle.
Here are the key stages from a service delivery perspective:

Architecture level threat modeling

This stage identifies all threats from an architectural point of view.
This also involves design level flaws such as integration related issues which may affect data and CI/CD pipeline.
Output: Identification of threats based on the functionality of the application, architecture, deployment and configuration, as well as the technologies that form part of the solution.

Process level threat modeling

This stage identifies threats related to processes which are developed for the CI/CD pipeline.
This stage is also responsible for identifying threats related to operational activities in DevOps lifecycle.
Output: Any process level gaps which might impact security or security automation are identified.

Application level threat modeling

Break down the application into its components by identifying trust boundaries, data flow, entry points, and privileged code.
This stage also requires identifying the key security objectives of the application in terms of authentication, cryptographic requirements, input validation, authorization configuration management, session management, etc.
Output: Identification of threats from application security perspective however not completely deep diving into application security testing.

Architecture Level Consulting:

Document the threats

Document the threats using the template provided that includes at a minimum the threat description, the threat target, the risk, the attack technique, and the suggested countermeasures

Rate the threats

The STRIDE model can be used to rate the threats

Enhanced Application Security:

Application Security

Application security issues should be identified via both automated as well as manual testing. Automated testing is the focus and should be implemented using embedded code review tools (such as Checkmarx, Fortify, etc.), automated scanning upon deployment to staging/UAT environments using tools such as Qualys, Acunetix, etc., and then ensuring vulnerabilities are remediated before the code is pushed to deployment in production. Additionally, certain applications would also benefit from manual testing that aims to defy the business logic and find more serious flaws in the application's security that automated tools might miss out on. Here companies can either choose to use the manual approach for only selected high-risk applications and/or sign up for a bug bounty program.

Enhanced Application Security:

Code Analysis

Here is a brief snapshot of our Code review methodology followed by our consultants:

- Review of software documentation, coding standards, and guidelines.
- Discussion with organization’s development team about the application.
- Analyze the areas in the application code which handle functions regarding authentication, session management and data validation.
- Identification of un-validated data vulnerabilities contained in your code.
- Identification of poor coding techniques allowing attackers to exploit them for launching targeted attacks.
- Evaluation of security issues specific to individual framework technologies.
- Automation of the entire process by implementing secure code review tools in the CI/CD pipeline

Production and Post deployment:

Security Operations, Log Analysis and Monitoring

- Runtime Checks & Monitoring
- Log Parsing & syslog
- Threat hunting
- Security science

Production and Post deployment:

Configuration Review

- Perform network security assessment on production systems
- Perform configuration review against industry best practices and baselines defined by organization
- Define policies in vulnerability scanner to automate configuration review
- Automate periodic scans by integrating the vulnerability management tool within the CI/CD pipeline

Vulnerability remediation

- Provide detailed recommendations towards closure of the vulnerabilities
- Continuous knowledge transfer on the vulnerabilities found during review process

Runtime Defense

- Consulting on cloud security solutions
- Interactive application security testing (IAST)
- Run-time application self-protection

Container security

- Hardening of containers
- Integrating container with container security tools for vulnerability management

Compliance as Code

- Defining policies and process for production environment
- Processes for managing changes in Continuous Delivery
- Chef Compliance
- Compliance for Cloud-based platforms

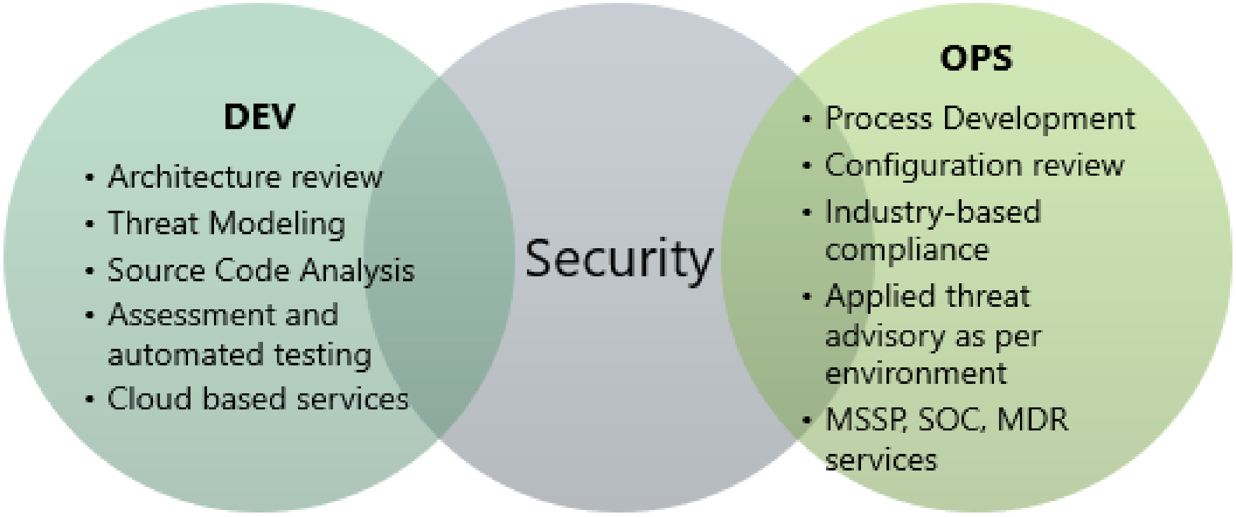
Production and Post deployment:

Trainings

We have a comprehensive array of training programs that address an organization’s applications and systems security requirements:

- Secure .Net Coding
- Secure Java Coding
- Secure PHP Coding
- Certified Web Application Security Programmer
- Operating Systems Security
- Database Security
- Network Security
- Cloud Security

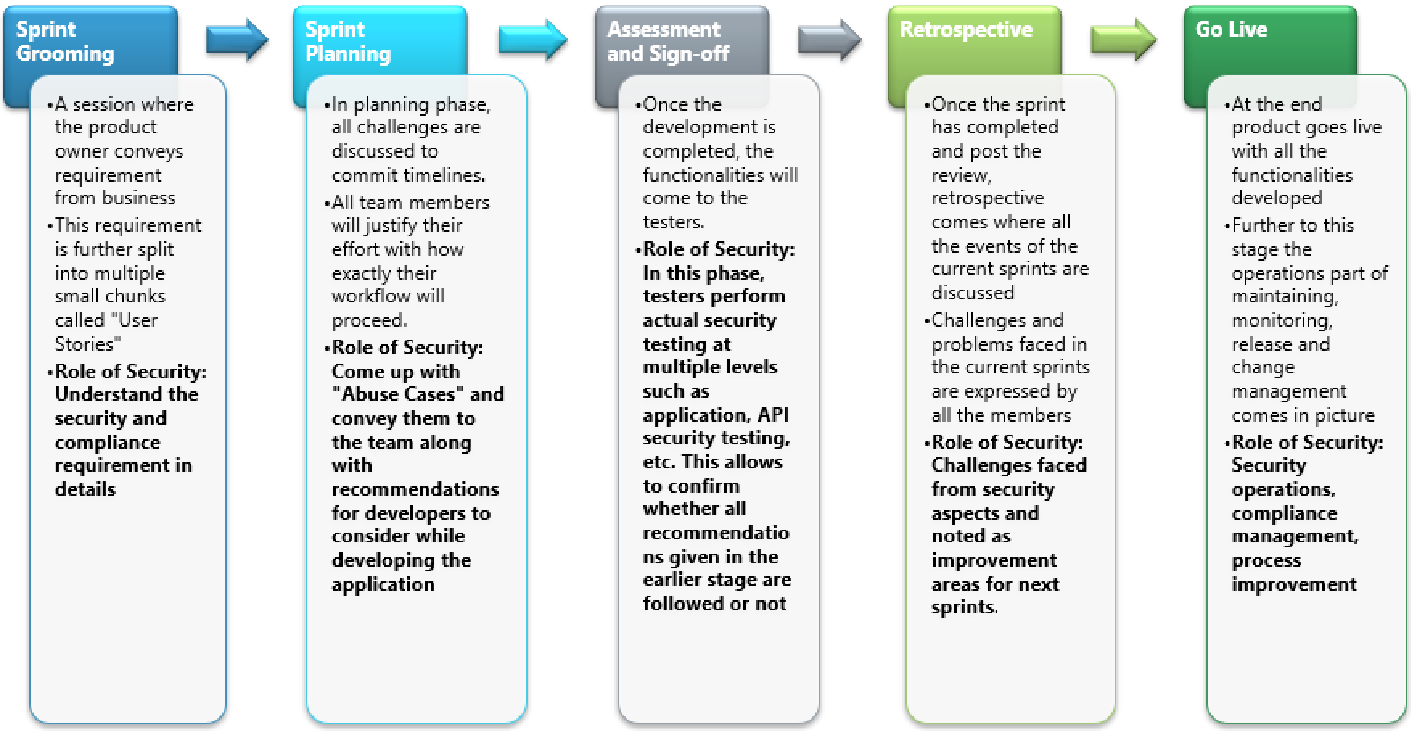
Embedding Security into DevOps:



Case Study:

Any organization may not require implementing DevSecOps at once. There could be few steps initially which would ultimately merge into a full-fledged CI/CD pipeline. The approach below showcases how various security services can be embedded into the existing DevOps culture

AGILE SPRINT:



Sprint Grooming

- A session where the product owner conveys requirement from business
- This requirement is further split into multiple small chunks called "User Stories"
- **Role of Security: Understand the security and compliance requirement in details**

Sprint Planning

- In planning phase, all challenges are discussed to commit timelines.
- All team members will justify their effort with how exactly their workflow will proceed.
- **Role of Security: Come up with "Abuse Cases" and convey them to the team along with recommendations for developers to consider while developing the application**

Assessment and Sign-off

- Once the development is completed, the functionalities will come to the testers.
- **Role of Security: In this phase, testers perform actual security testing at multiple levels such as application, API security testing, etc. This allows to confirm whether all recommendations given in the earlier stage are followed or not**

Retrospective

- Once the sprint has completed and post the review, retrospective comes where all the events of the current sprints are discussed
- Challenges and problems faced in the current sprints are expressed by all the members
- **Role of Security: Challenges faced from security aspects and noted as improvement areas for next sprints.**

Go Live

- At the end product goes live with all the functionalities developed
- Further to this stage the operations part of maintaining, monitoring, release and change management comes in picture
- **Role of Security: Security operations, compliance management, process improvement**

Final Take-aways:

- DevSecOps helps to address the issues raised from the traditional secure SDLC lifecycle to achieve a secure and reliable way for software delivery
- DevSecOps ensures identification and fixing of the vulnerabilities in each stage of the development process which in turn reduces the project cost
- DevSecOps team consists of Developers, Tester, QA, Operations, and Security Team
- The DevSecOps team is a cross-functional team (i.e., a developer can do testing if needed. Some organizations even rotate the responsibilities of the team), thus ensuring 'Security is everyone's job'. DevSecOps makes everyone responsible for Security
- Enhanced monitoring and auditing leads to improved threat hunting, which reduces the likelihood of a breach, avoiding bad publicity and reputational damage (to say nothing of regulatory fines)
- It also encourages companies to move to the cloud instead of using depreciating and increasingly vulnerable hardware
- Security auditing, monitoring, and notification systems are managed and deployed so that they can be continuously enhanced
- Ensures the 'secure by design' principle by using automated security review of code, automated application security testing, educating, and empowering developers to use secure design patterns
- DevSecOps fosters a culture of openness and transparency from the earliest stages of development
- Finally – the goal of shifting security LEFT is achieved

About Us:

Network Intelligence has been a cybersecurity services provider for over 20 years. With 500+ employees spread across the globe, our client list includes marquee names such as Morgan Stanley, Standard Chartered Bank, Western Union, American Express, Capgemini, Infosys and many others.

Our areas of expertise extend beyond traditional technologies into areas such as Cloud, IoT, DevSecOps and OT/ICS. Our teams have a deep understanding of cybersecurity regulations and standards such as ISO 27001, GDPR, PCI DSS, HIPAA and others.

New York | Sydney | Amsterdam | Riyadh | Dubai | Qatar | Mumbai | Bengaluru | Singapore

✉ info@niiconsulting.com

www.networkintelligence.ai