What is DevOps

The unification of how to manage Development (programmers, developers, security, application analysts, application owners, project managers), IT Operations (system admins, network admins, data center, storage, database admin) and Information Security in a tightly-integrated way.

DevOps is the belief that collaborating will produce better results, and break down barriers and finger pointing.

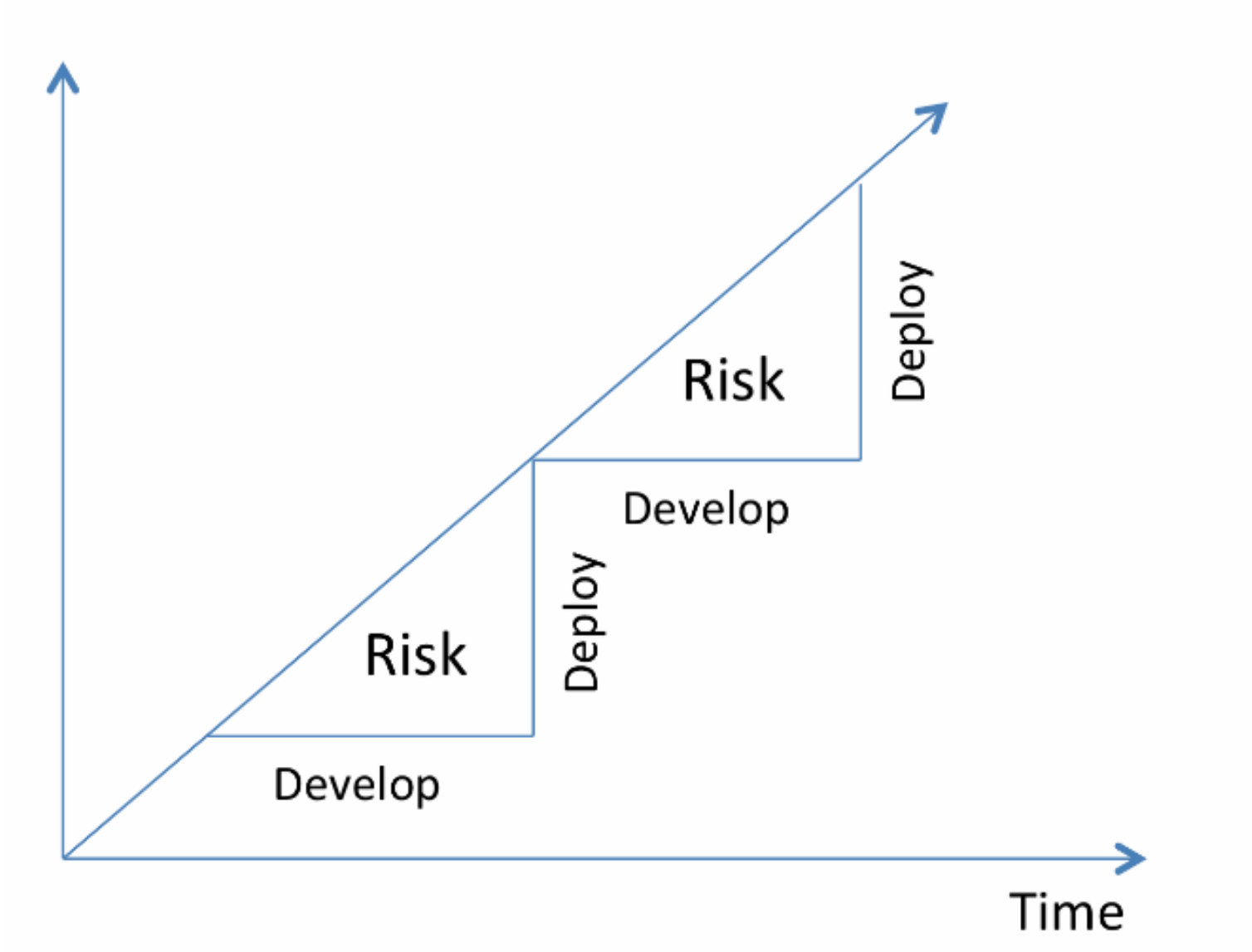
What is DevSecOps

DevSecOps helps improve a system development life cycle by securing the building blocks of the delivery pipeline without slowing down the life cycle process. It fills the gaps by implementing security through all stages of development and helps find solutions that satisfy your company's cybersecurity needs..

Application security during the development lifecycle is critical — and knowing how to integrate security into your DevOps is DevSecOps.

Think of DevOps as CLAMS

Culture	**Hearts & Minds Embrace change**
Lean	**Focus on producing value Keep everything to a minimum [tools, meetings, sprints]**
Automation	**CI/CD** **Infrastructure as Code**
Measurement	**Measure everything** **Set targets and chase anomalies**
Sharing	**Open information sharing** **Collaboration**


Risk
Deploy
Develop
Risk
Deploy
Develop
Time

Common DevOps & DevSecOp Strategies - Cultural

1. Regular code reviews are required, and Ops is involved with code reviews
2. No app launches without automated testing in place at both the infrastructure and app level.
3. Bi-weekly 10- 60 minute standups with Dev, Security and Ops staff
4. Find individuals that have both Dev and Ops skills and make liaisons
5. All Production environments mirrored by identical Development environments
6. Regular infrastructure architecture/config/outage reviews are required, and Dev is involved with infrastructure reviews.
7. Security Posture Review throughout all development phases.
8. Dev and Ops staff all have scheduled "office hours“
9. Both Dev and Ops have 7x24 accountability for the performance and availability of the environment.
10. Automated monitoring or platform monitors infrastructure and software layers 7x24, and pages Dev and Ops 7x24.
11. Shared sign-off by Dev, Security and Ops before any application goes live

Infrastructure Should be Treated Like Code

Packages installed, versions

Server and application configuration (such as timezone settings)
Relationships with other servers and services

We want

- Automated, repeatable operations
- Predictable outcome
- Remove manual, error prone steps
- Manage change during server lifecycle
- Ability to test outcomes
- Build security into every stage of the DevOps

How to Get There..

DevOps is a journey

Dev and Ops need to look introspectively to understand their strengths and challenges, and look for ways to contribute towards breaking down silos

Dev sharpen skills on ops/admin, Ops sharpen skills on engineering

Revisit legacy architecture

Set small goals to be awesome

Don't automate what you don't understand

CLAMS: First, be lean.

James Burke
Security Engineer
410-733-1277
James.burke@secureitservices.biz