DevOps模式下安全挑战和转机

王志刚

DevOps Connect

RUGGED DEVOPS

RSAConference

目录

01 行业现状


DevOps Connect
RUGGED DEVOPS
RSAConference
ASSEMBLE
HEROES
SEC DEV OPS


@DUIVESTEIN | VISION • INSPIRATION • NAVI
~ Marc Marc Andreessen 2011
SOFTWARE IS EATING THE WORLD

SDN/SDE/ABC/IOT 全是DevOps的功劳

In Our Bodies

In Our Homes

In Our Cars

In Our Infrastructure

安全看热闹？

雅虎30亿用户账号信息泄露,该如何避免类似事件

2017-10-13 17:51:00 作者：

BloombergBusiness News Markets Insights Video

Ex-Sony Employees Sue Studio Over 'Nightmare' Data Breach

December 16, 2014 – 10:24 AM MST Updated on December 16, 2014 – 7:35 PM MST

The Sony Pictures Entertainment Inc. headquarters in Los Angeles, California. Photographer: Frederic J. Brown/AFP/Getty Images

(Bloomberg) -- The massive hack of Sony Pictures Entertainment Inc.'s computers has spurred two lawsuits by former employees accusing the movie company of failing to protect the personal information of thousands of workers.

Two ex-employees who sued yesterday called the breach "an epic nightmare, much better suited to a cinematic thriller than to real life." Two others who sued today said Sony knew retribution for "The Interview," a comedy depicting a mission to assassinate

THE HILL

NEWS POLICY REGULATION BLOGS BUSINESS CAMPAIGN OPINION CONTRI

BALLOT BOX | FINANCE | HEALTHCARE

HOME | POLICY | CYBERSECURITY

Largest federal workers union sues OPM over breach

COMMENTS 3

By Cory Bennett - 06/30/15 08:21 AM EDT

The country's largest federal workers union has filed a class action lawsuit against the

BGR TOPICS DEALS REVIEWS PODCAST APPLE IPHONE 6S FREE APPS TIP US SEARCH

Expert who first revealed massive Target hack tells us how it happened

By Chris Smith on Jan 16, 2014 at 11:00 AM

SECURITY

SHARE THIS STORY Tweet Like Share Submit Shop

GOOGLE ADWORDS

google.com/AdWords

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

> SC US

SC UK

Malwarebytes apologizes for jumping the the gun on WinRAR vulnerability

Akhter twins sentenced to prison for hacking State Dept.

NEWS PRODUCTS BLOGS RESOURCES VIDEOS WHITEPA

SC Magazine > News > JPMorgan reassigns CISO a year after major data breach

Robert Abel, Content Coordinator

Follow @RobertJAAbel

July 01, 2015

JPMorgan reassigns CISO a year after major data breach

Share this article:

JPMorgan Chase has reassigned the executive who was in charge of network security a year after controversy arose surrounding his handling of a major data breach at the bank.

Chief Information Security Officer (CISO) Greg Rattray, a former Air Force commander in information warfare and cyber-expert at the National Security Council will now head of global cyber partnerships and government strategy, where he'll manage considerably fewer people, according to Bloomberg.

Rattray and his boss, bank security chief Jim Cummings, were criticized for limiting access to breached data in an effort to prevent leaks and controlling the ensuing investigation to the point that the Secret

FCC s…25 million fine over customer data breach

This one happened at the hands of employees in AT&T's own customer service c… in Mexico, Colombia and the Philippines.

By Rachel King for Between the Lines | April 8, 2015 -- 17:21 GMT (10:21 PDT) | Topic: Networking

黑客宣言：

我们不是漏洞的生产者，我们只是漏洞的搬运工，研发是最好的盟友、也是最强大的敌人。

02 存在问题

应用安全积弊已久，是全产业链的问题

日趋严重

Agile + DevOps

- 业务生存压力
- 速度至上

安全技术及理念落后

-安全圈的自恋
-缺少直接需求

四面楚歌

- 黑客
- 研发
- 开源DevOps、云
- 安全厂商

速度是一切，安全却在拖后腿

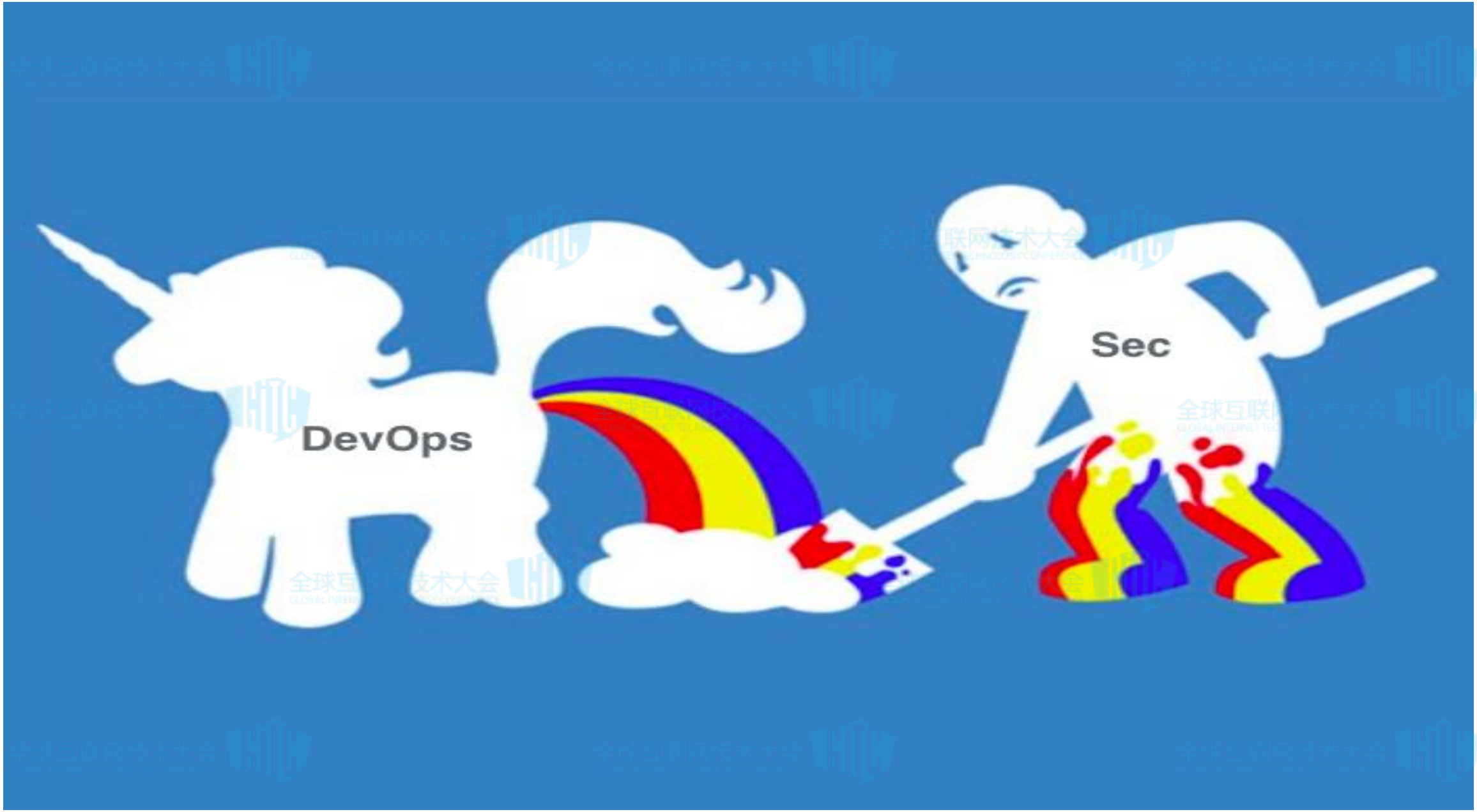
安全防护系统的软件定义、可编程能力低，无法集成到DevOps

应用是攒出来的、而非写出来的

安全技术落后

安全VS开发 不成比例资源匮乏

安全介入晚，因为谁都想绕着走


DevOps
Sec

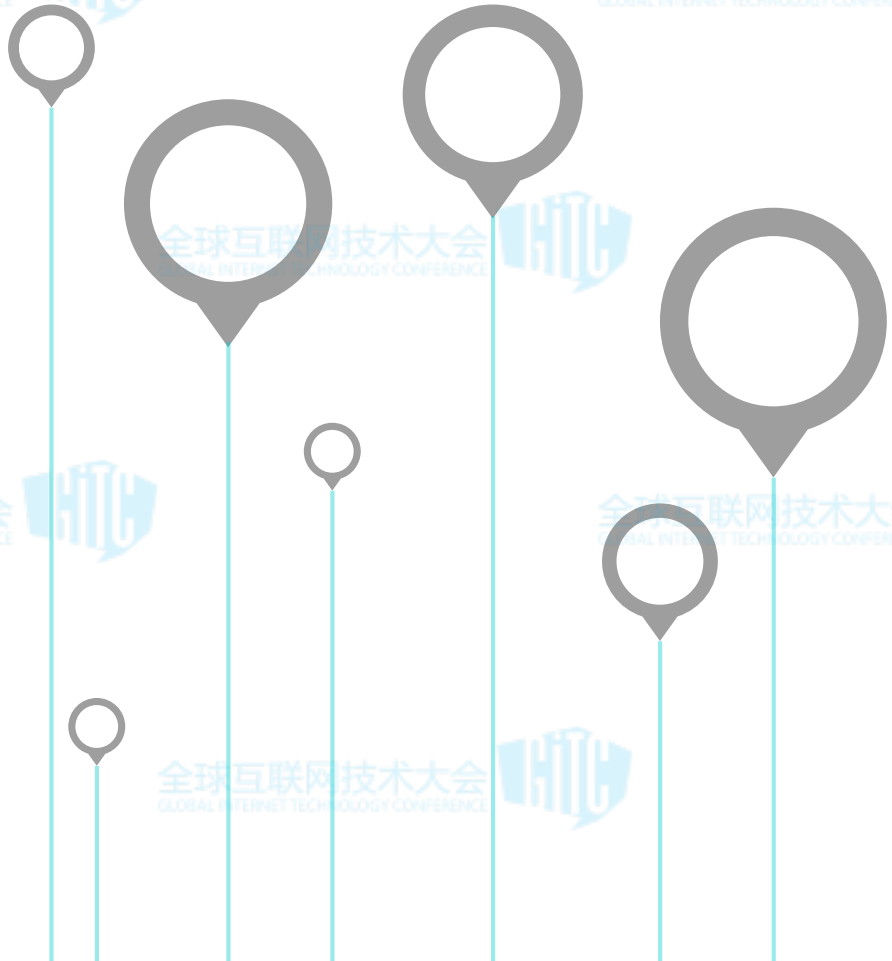
失效

卡点？


The Oregon Trail
Introduction
Options
Quit
Travel the Trail

03 解决方案

解决方案



04 DevOps模式下安全的7条法则


Dev and Ops


Dev and Sec

拥抱DevOps复制DevOps

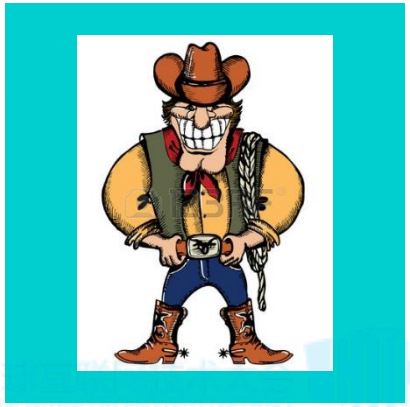
1. Infrastructure as Code

2. Continuous Delivery

3. Culture of Collaboration

第一法则: 沟通与协作

敌对模式



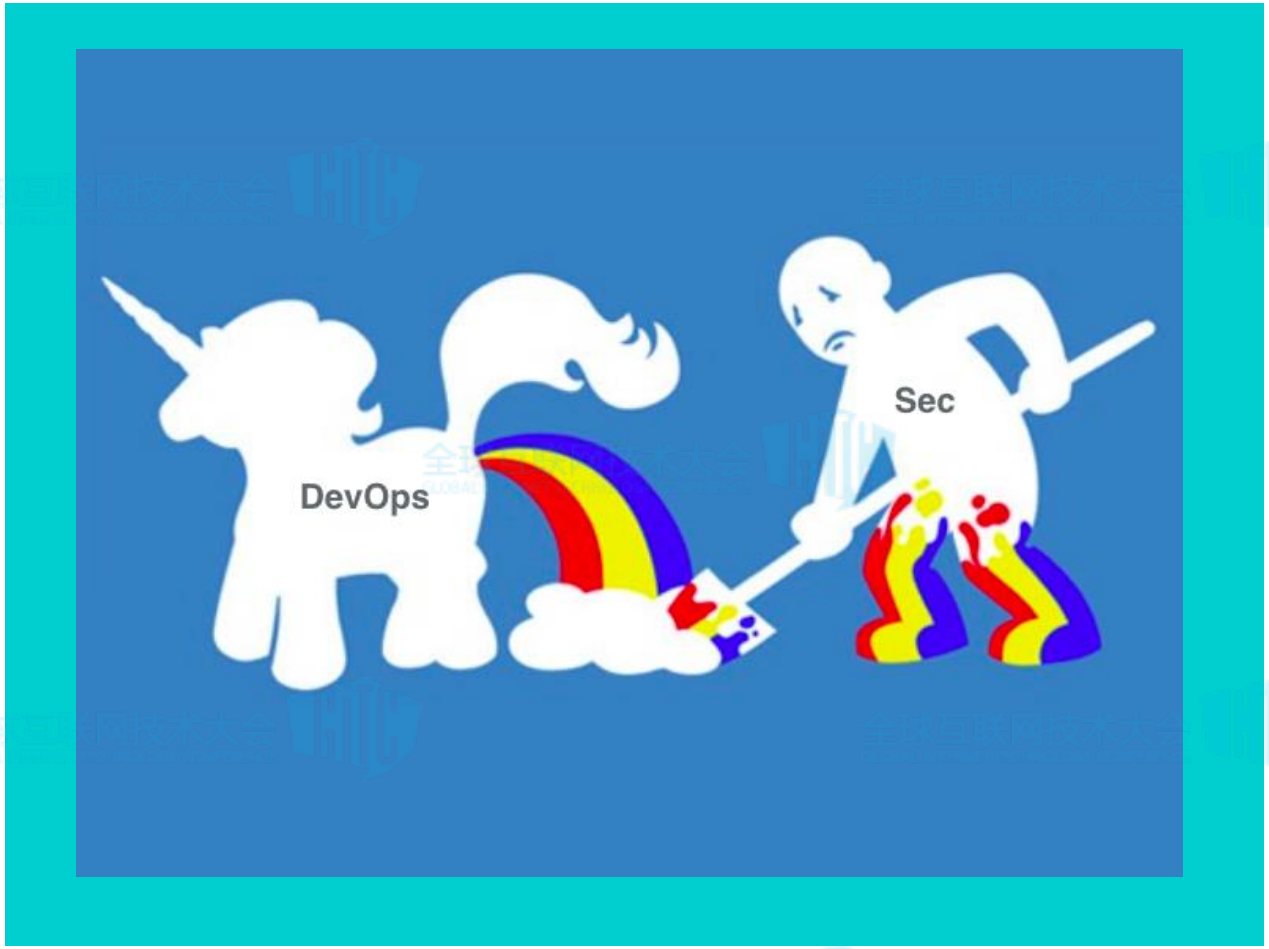
Application Development Department of Anything Goes

Infrastructure & Operations

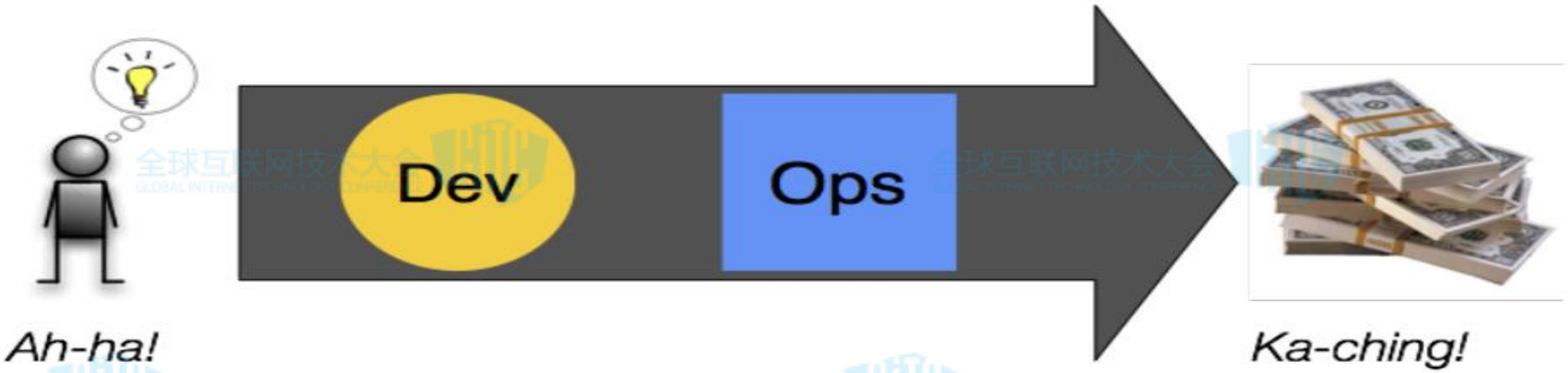
Department of NO

Security and Risk Department of Persistent Nagging

悲催模式



需求驱动进步



生态利益链中安全总是被 “忽 略”

我们总是那个找茬、令人憎恶的人

发动全民安全运动，迫在眉睫但 Who cares?

内驱力

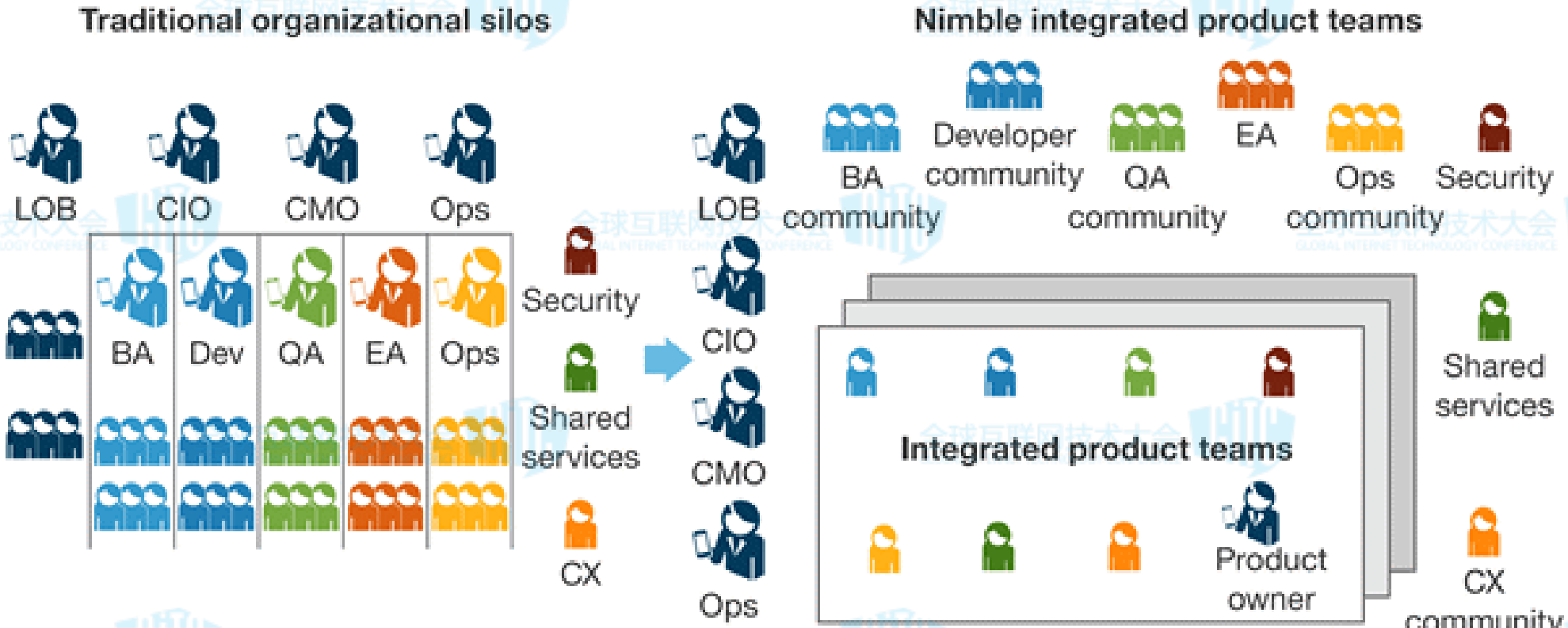
我什么要做

- 不做，你能把我怎么着？
- 我的活已经很多了，别加了
- 做了，我有啥好处？

如何衡量

- 看结果：代码、产品安全 漏洞数
- 看过程：做了哪些安全工作
- 看实力：知识，能力竞赛 CTF? 红黑榜？

DevOps uses integrated product teams



建立顺畅的沟通管道

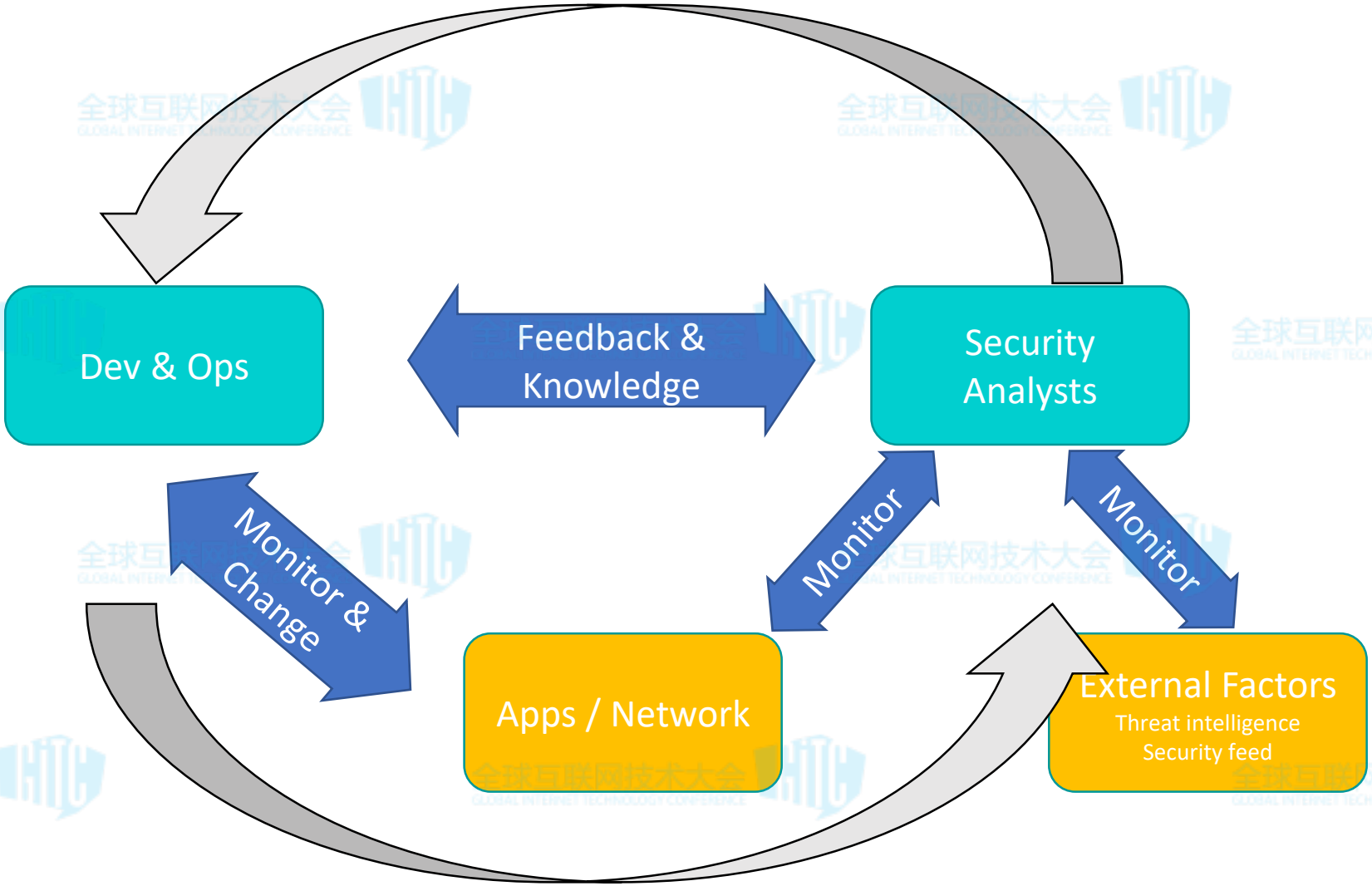
- SEC向DEV学习
- SEC帮助DEV
- DEV向SEC学习
- DEV帮助SEC
- 共同协作
- 建立反馈机制

第二法则: Visibility

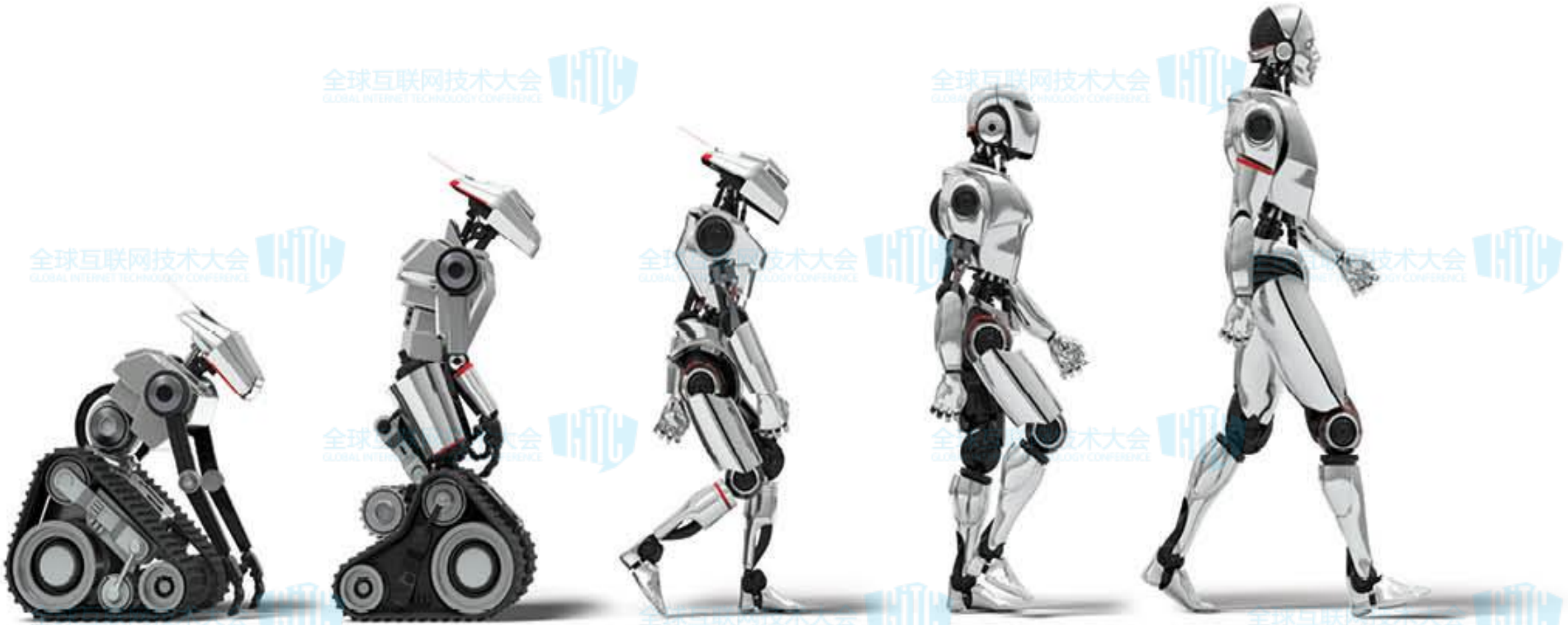
别给我文档，show me your code？

- 没有度量就没有进步
- 让数据说话
- 要结果 更要过程
- 可视化也是相互的
- 全记录的重要性

可视化管道


Dev & Ops
Feedback &
Knowledge
Security
Analysts
Monitor &
Change
Monitor
Monitor
Apps / Network
External Factors
Threat intelligence
Security feed

第三法则:迭代、碎片化

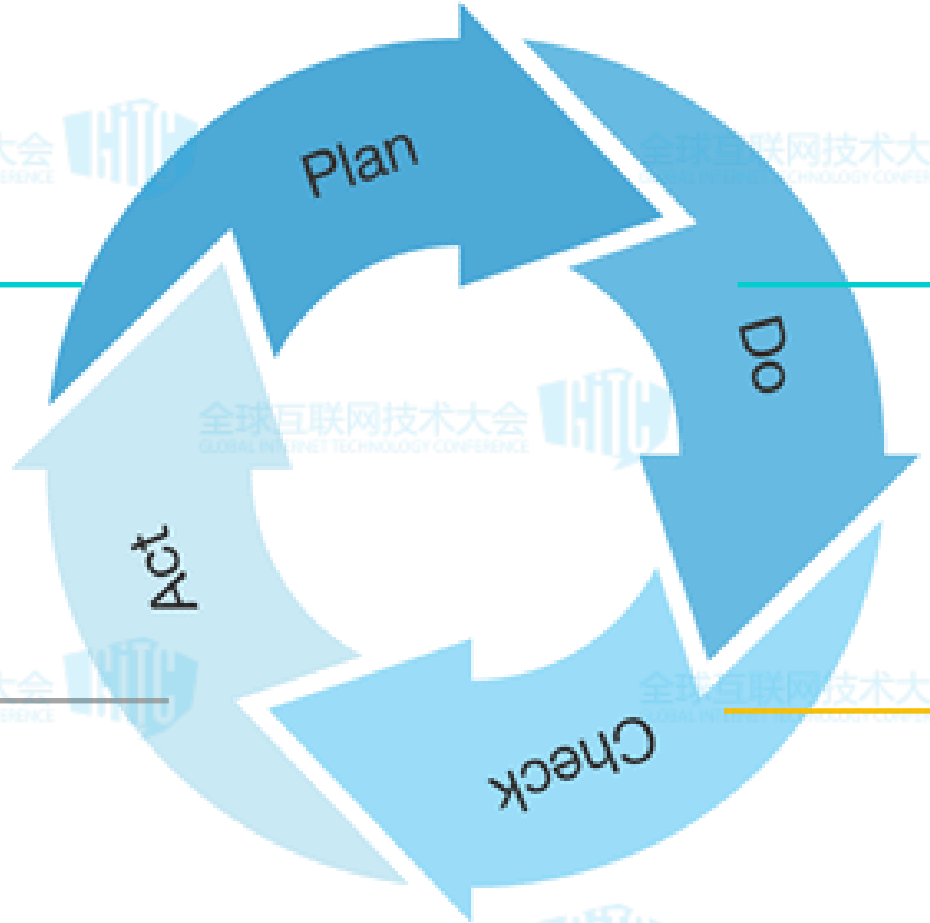


迭代、碎片化

学会逐步改进CD积累

原则、策略、要求

SDK API 服务

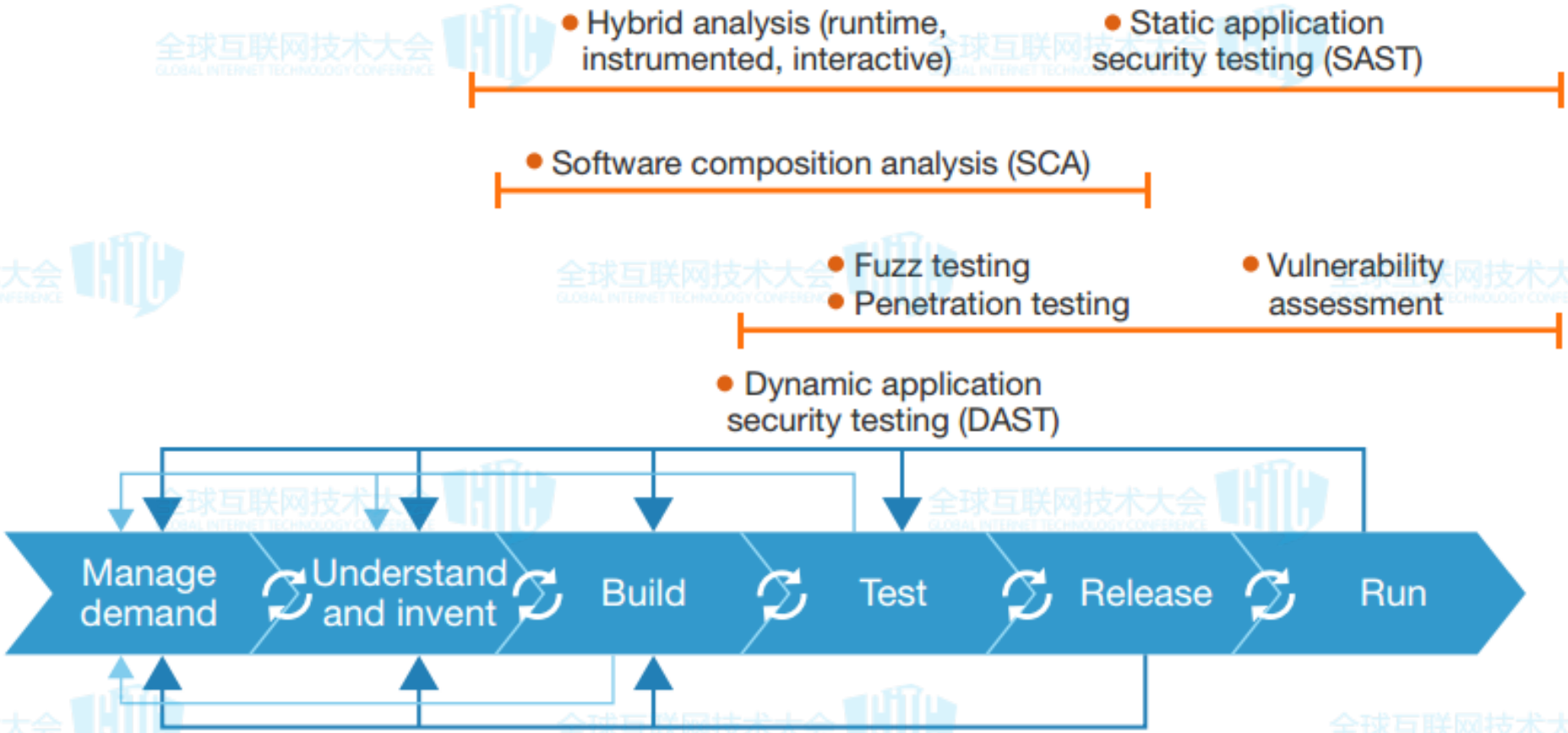


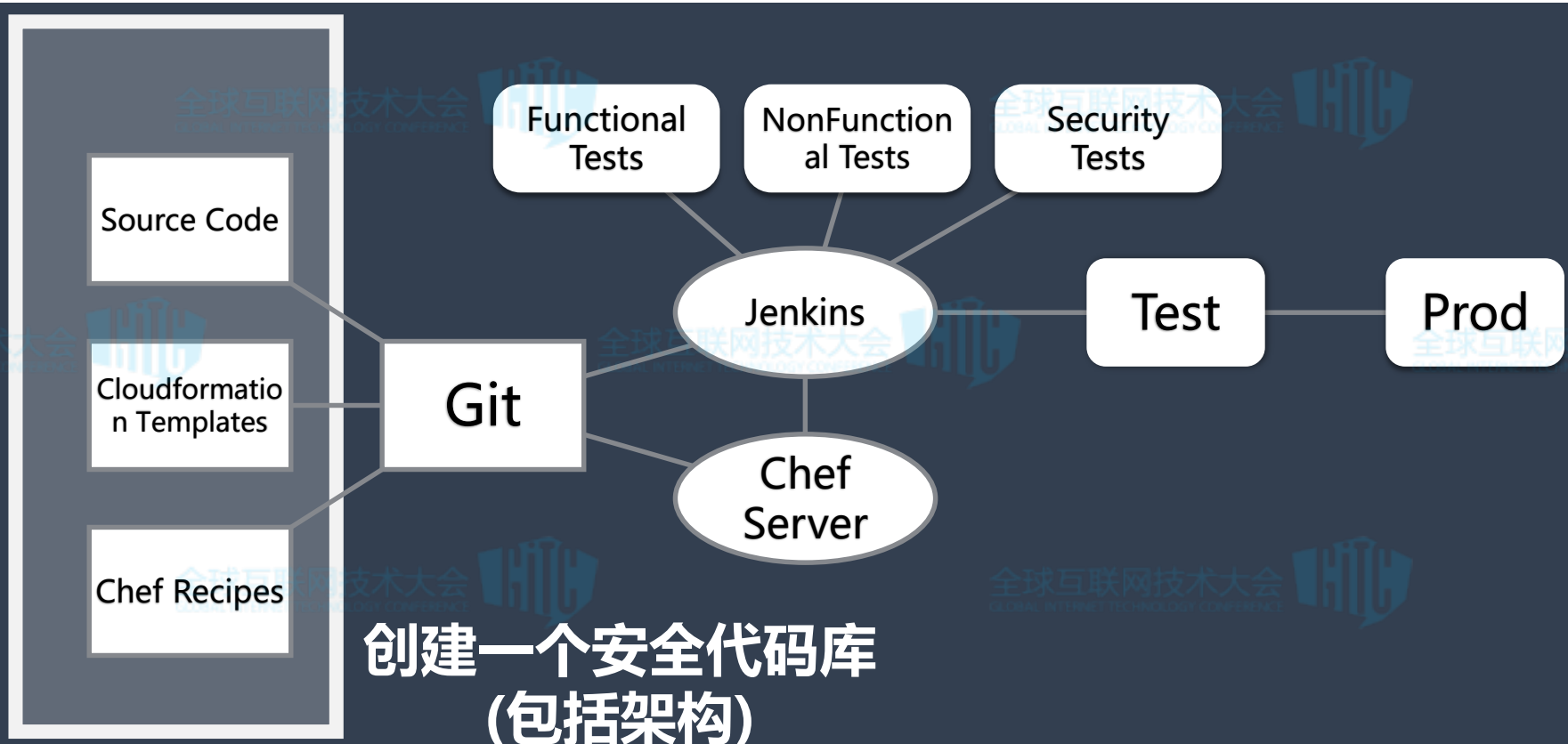
编码规范、指南

代码、库、工具

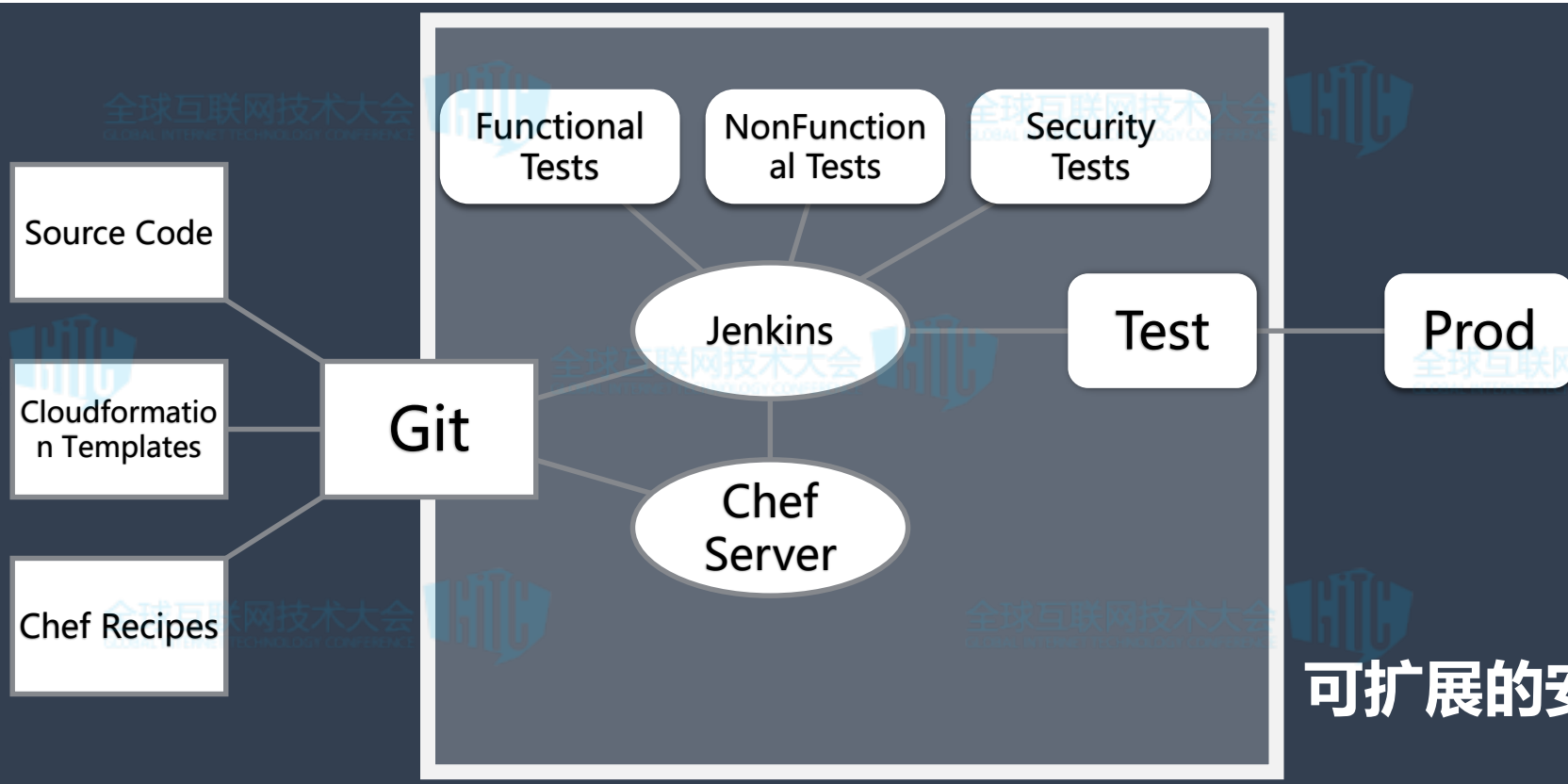
第四法则:嵌入式安全

Modern service delivery life cycle:

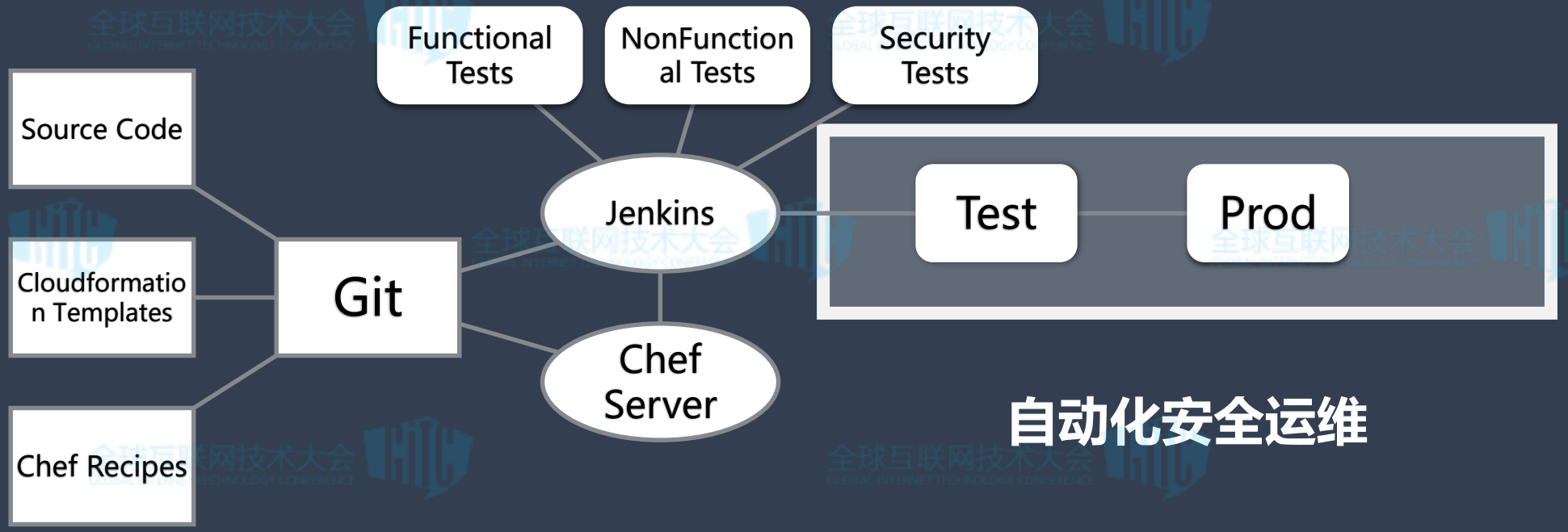




创建一个安全代码库 (包括架构)


Source Code
Cloudformation Templates
Chef Recipes
Git
Functional Tests
NonFunctional Tests
Security Tests
Jenkins
Chef Server
Test
Prod

可扩展的安全测试


Functional Tests
NonFunctional Tests
Security Tests
Source Code
Cloudformation Templates
Chef Recipes
Git
Jenkins
Chef Server
Test
Prod

自动化安全运维

第五法则: 管好软件供应链

90% 现在的代码来自开源

16个下载就有一个有漏洞

31%公司已经或怀疑发生开源的攻击

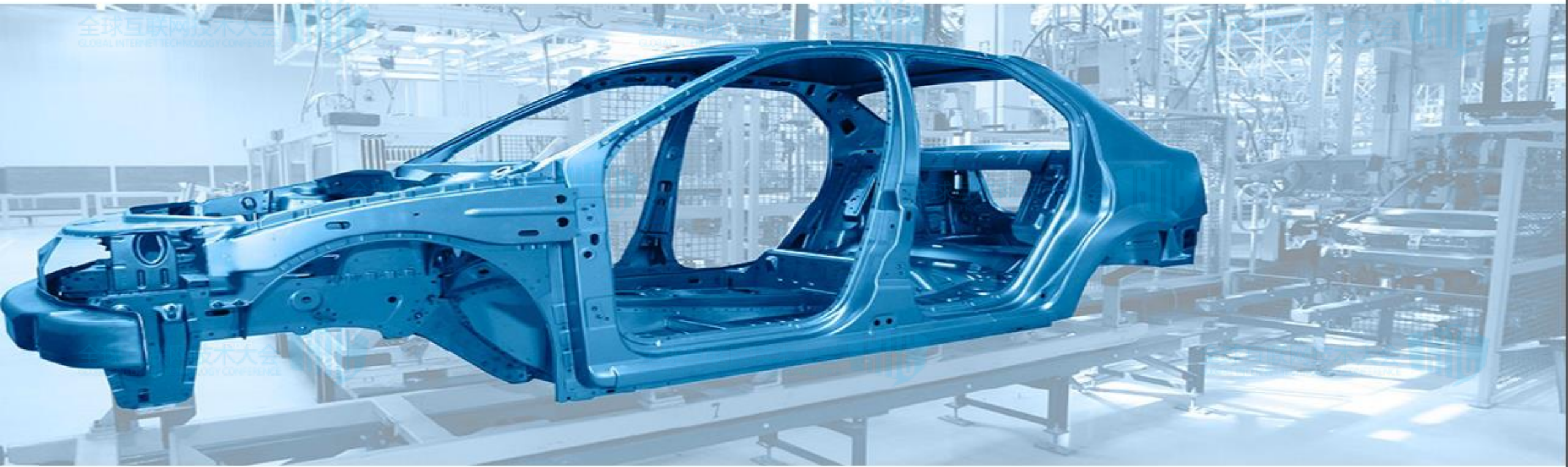
2014年97%成功的攻击可以追溯到10个通用的漏洞，其中8个补丁超过10年

Software Supply Chain Hygiene

Use better & fewer suppliers

Use higher quality parts

Track what you use and where

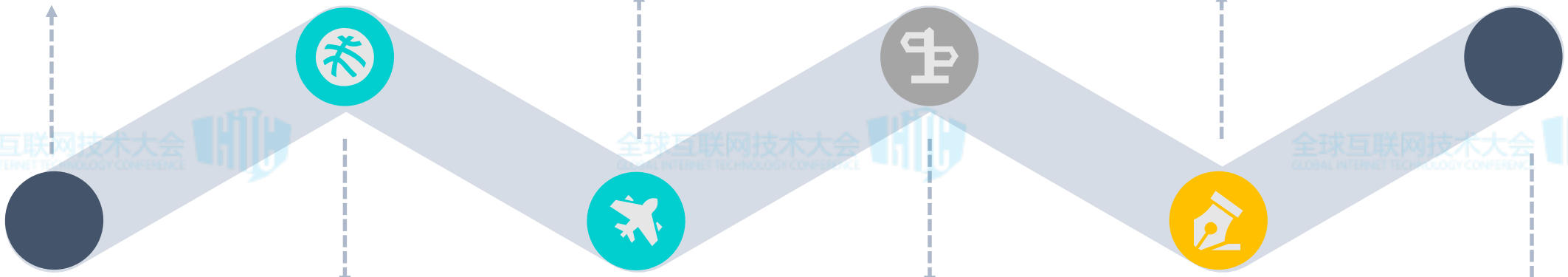


三方软件的实战

坚持用最新的
No CVE

减少维护版本
最好只有一个版本

识别、控制入口
实现自动化扫描
建立软件仓库和软件地图



建立和维护关键
白名单、黑名单、灰名单

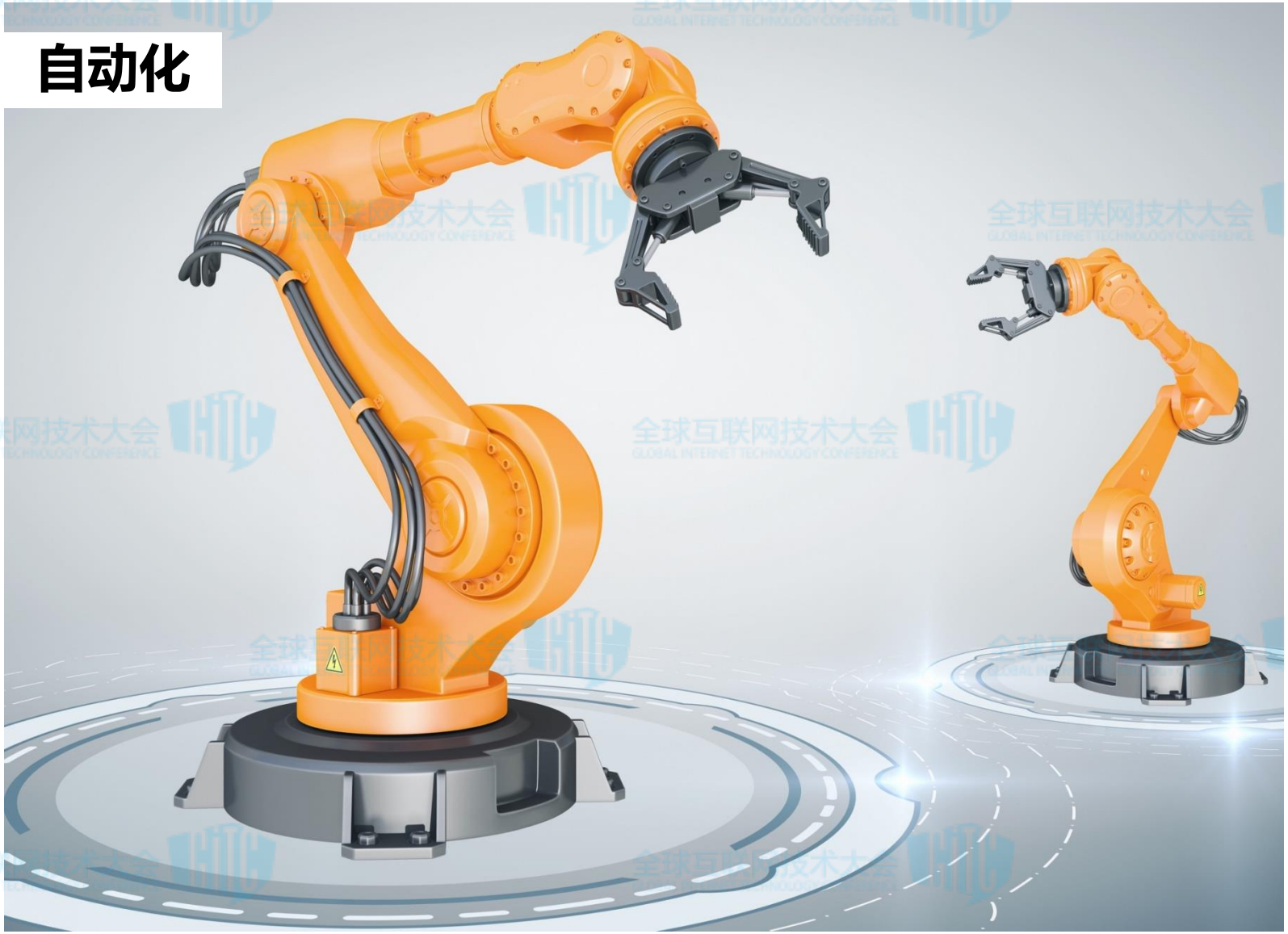
不要露掉网络、数据库
操作系统

使用 CD Pipeline
管理3rd 软件

当发现漏洞，通过CD Pipeline工具快速更新所有软件

第六法则:自动化、自服务

自动化



动态可配置

网络

应用

系统

可自动调用

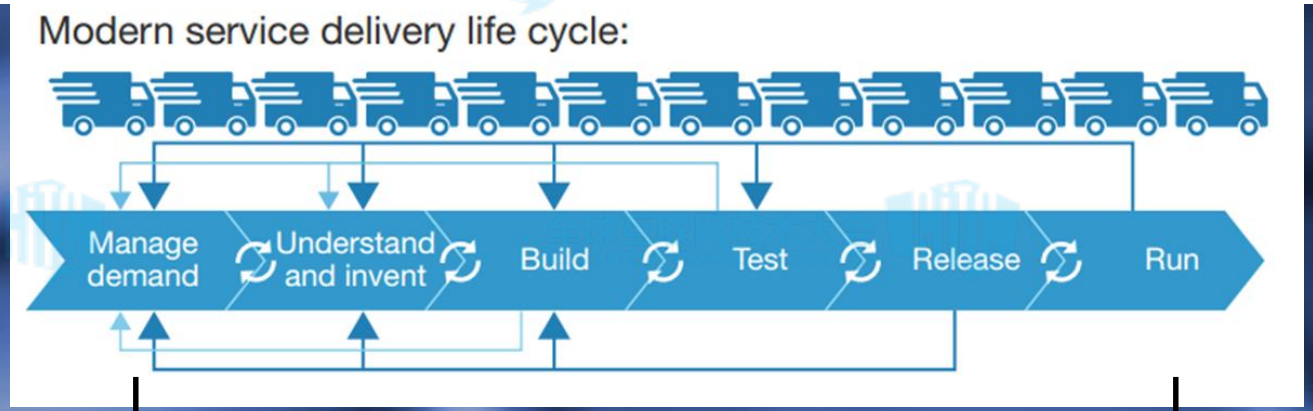
自动化生成数据监控

Protect IP and flag potential insider threat automatically without ruining the collaboration

Each tool in the continuous delivery pipeline includes tracking and logging

Ability to know exactly who (attackers, developers, I&O pros, S&R pros, users) performed what change and when

Protect IP and flag potential insider threat automatically without ruining the collaboration



2. Flag high risk changes

1. Create automatic security alerts

3. Enable proper authentication and authorization on all systems

4. Track drift across development, testing, and production environments

5. Define security based quality gates

- Source: “DevOps Makes Modern Service Delivery Modern” and “The Seven Habits Of Rugged DevOps “ Forrester reports

Security as Code

规则明确、结果准确

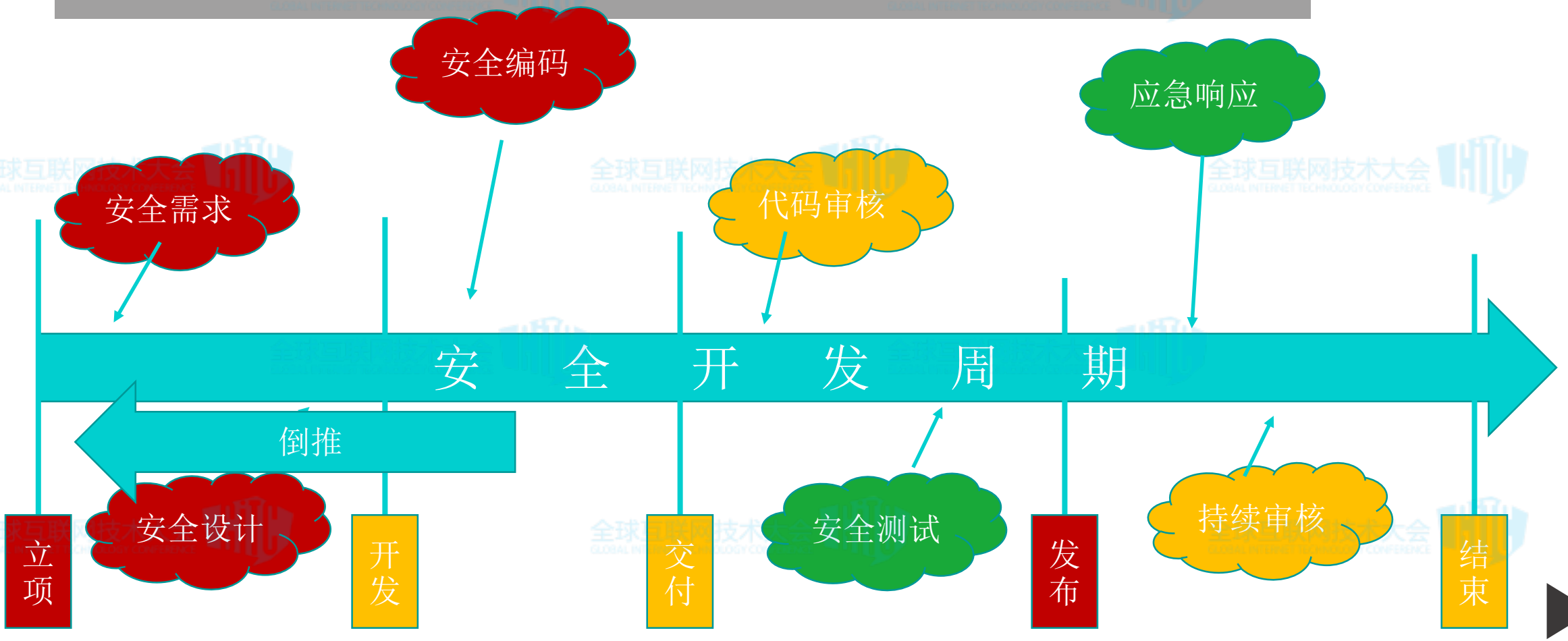
接口可调用、自服务化

监控模式也可以进行自动化

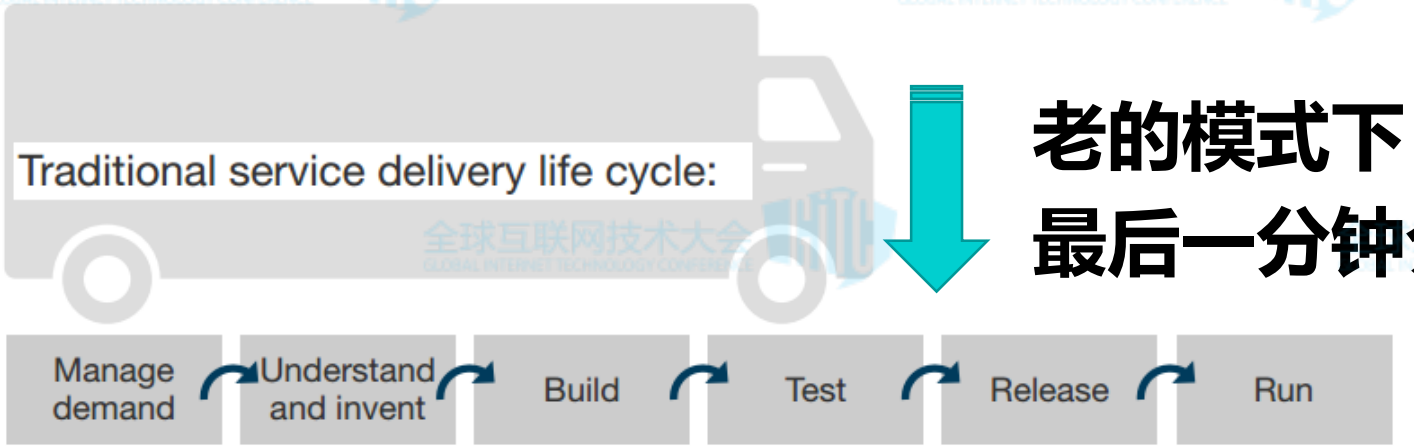
第七法则:向左 shift Left

经典生命周期防护SDL倒推

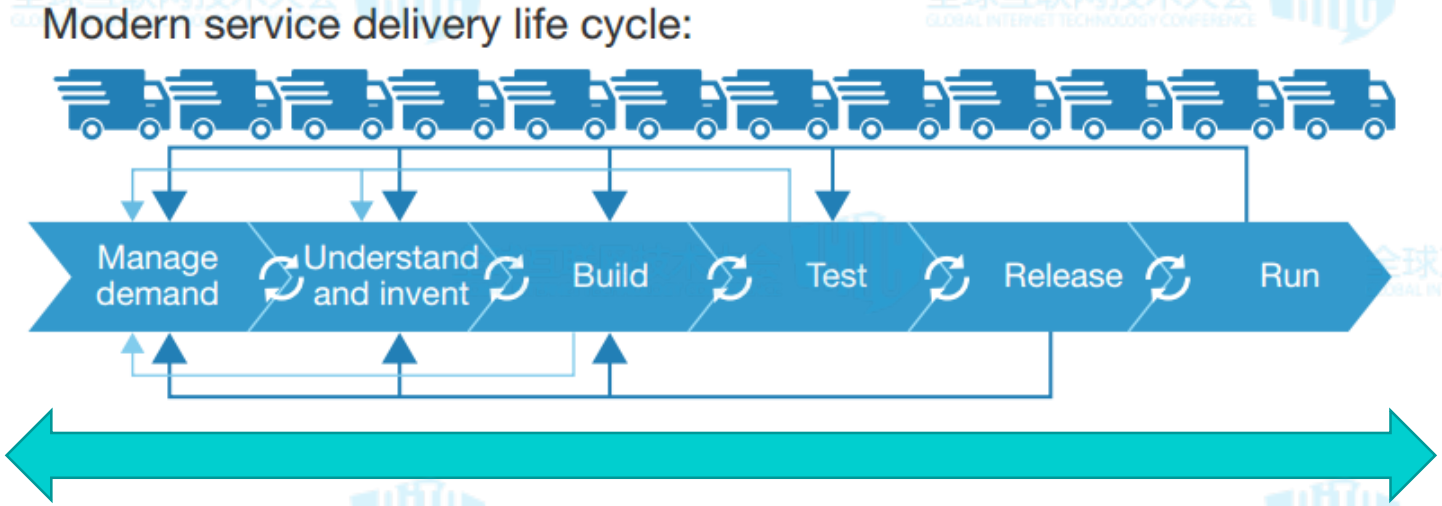
- 无点可卡
- 永不结束



全站Shift Left



老的模式下，
最后一分钟介入



新模式下，安全植入每一个集成的周期，倒推

- Source: “DevOps Makes Modern Service Delivery Modern” Forrester report.

DevOps模式下安全的7条法则

王志刚

18601331421

michael7736@.com

THANK YOU PRESENTATION