GOPS 2019 shenzhen

GOPS 全球运维大会 2019

-AIOps 风向标

深圳站

指导单位：

主办单位：

大会时间：2019年4月12日-13日

大会地址：深圳市南山区圣淘沙大酒店（翡翠店）

下一代软件工程的思考和探索

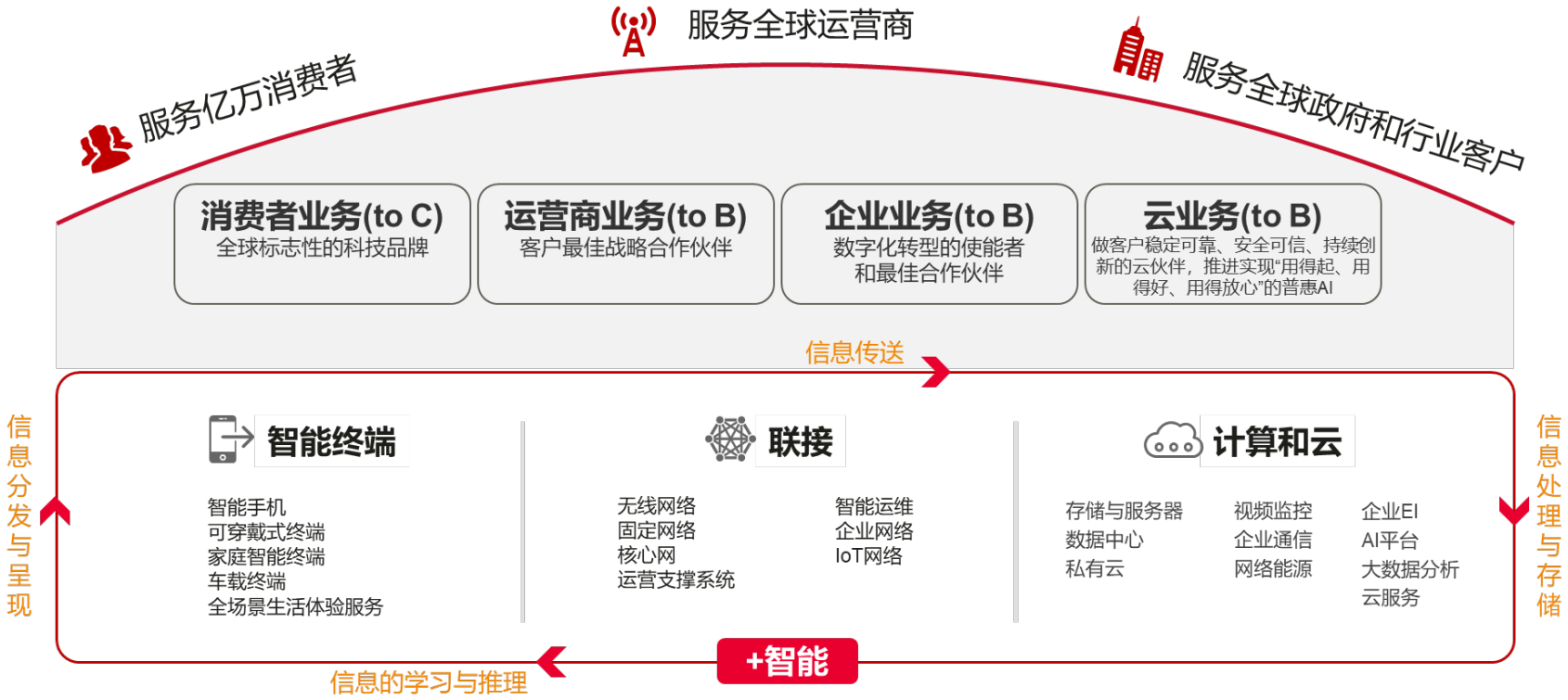
刘恒 华为云DevCloud

目录

1 我（们）的思考

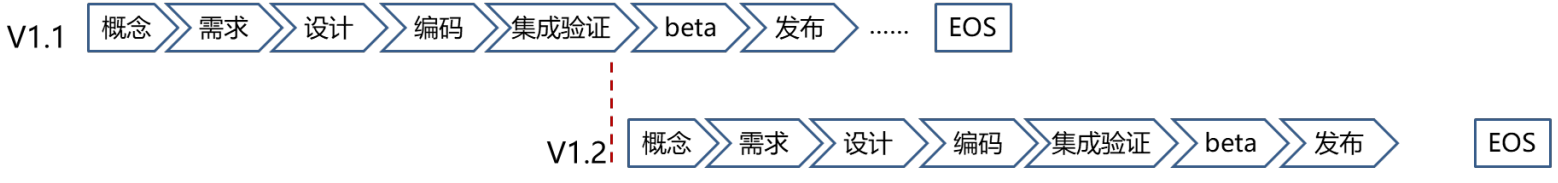
2 我（们）实践探索

华为的特点：多种商业模式

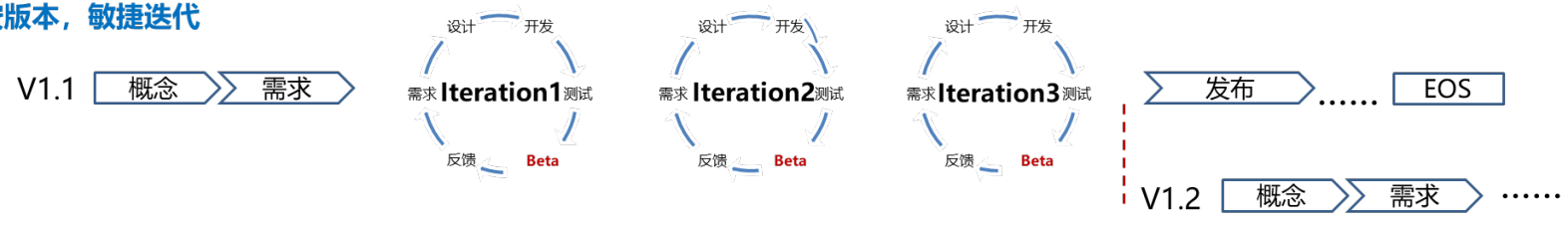


华为的特点2：匹配不同的商业和交付模式，多种研发模式

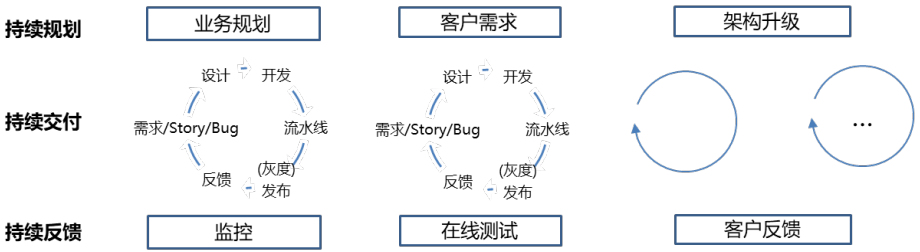
1. 按版本，瀑布



2. 按版本，敏捷迭代



3. 无版本，DevOps持续交付



我(们)的经历和经验：虫眼，鹰眼，弄脏双手后的思考、实践

Eagle Eye
(俯视，全局)

研发变革
（ALM、敏捷、DevOps...）

研发变革
（...）

产品经理，布道，服务客户
（弄脏双手，下地干活）

Insect Eye
(贴近，细节)

开发
设计、编码、交付、维护

软件工程的回顾：“主旋律公式”的变化

借鉴硬件制造，管理偏差

尝试解决软件开发

质量、可控、有序问题

Chaos + Delay → Stability + Reliability

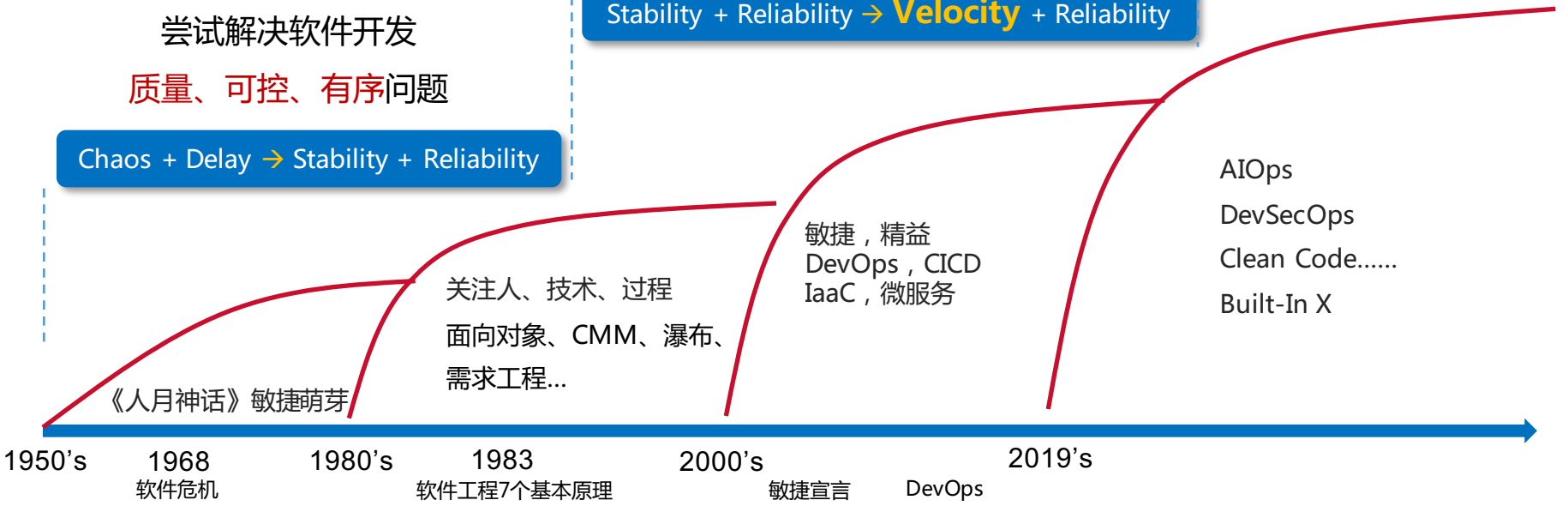
回归软件本质，响应市场

尝试解决软件开发的效率/速度问题

Stability + Reliability → Velocity + Reliability

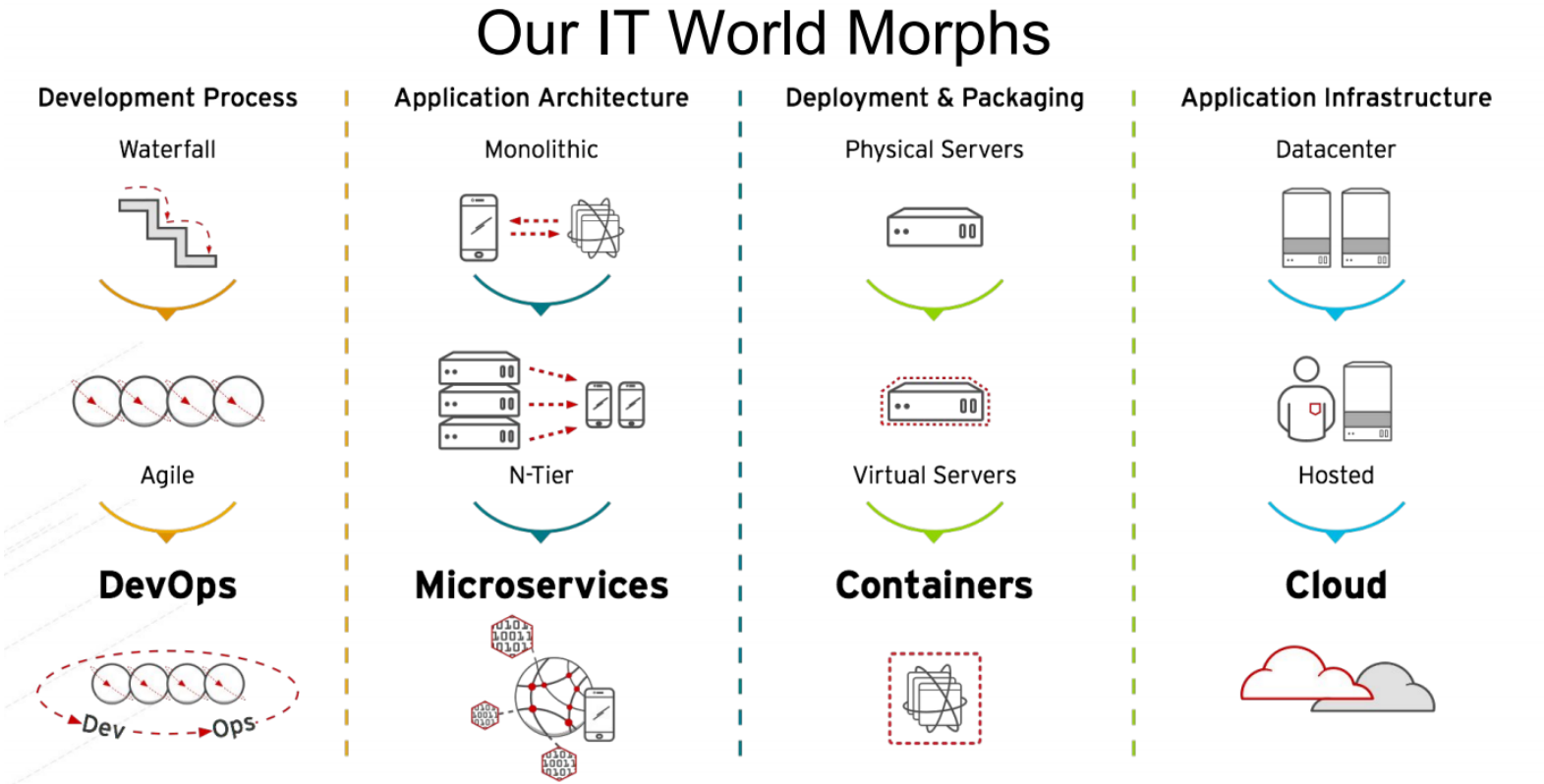
解决软件开发的??？问题

Velocity + Reliability → ???

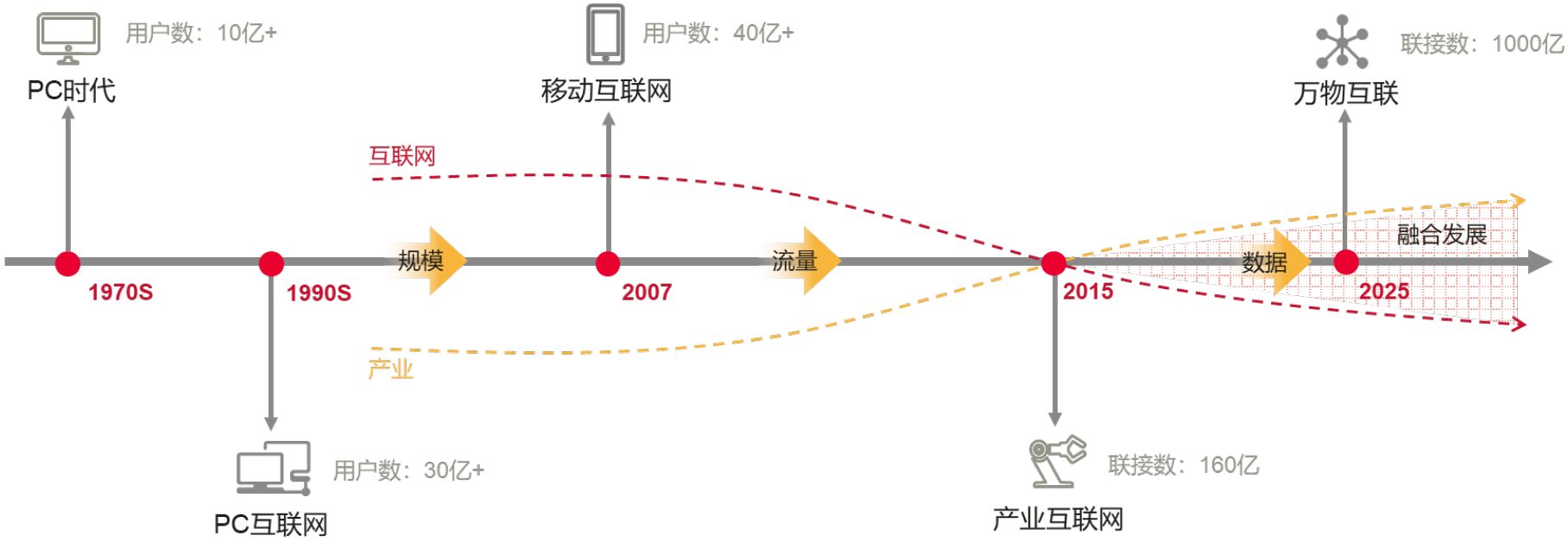


当下已经在发生什么？

From Rafael Benevides RED HAT DEVELOPERs



未来将发生什么？



从消费互联网到产业互联网，最终实现万物互联

下一代软件工程要尝试解决的问题：万物互联下的可信赖

可信软件是指能按照预期（需求）运行的软件，并且不会在环境改变时带来重大安全和隐私风险。

- Managing the complexity of today’ s systems and being able to claim that those systems are trustworthy and secure means that first and foremost, there must be a level of confidence in the feasibility and correctness-in-concept, philosophy, and design, regarding the ability of a system to function securely as intended.【NIST SP 800-160】
- In software engineering, **software trustworthiness** would deliver a complete assurance that it will execute its required functions under all probable situations, will do so on time, and will never implement any activities that have significances of security risk in software for a specific time-duration.【wikipedia】

• Safety: The ability of the system to operate without harmful states; • Reliability: The ability of the system to deliver services as specified; • Availability: The ability of the system to deliver services when requested; • Resilience: The ability of the system to transform, renew, and recover in timely response to events; • Security: The ability of the system to remain protected against accidental or deliberate attacks.	• 安全性：系统在没有有害状态的情况下运行的能力; • 可靠性：系统按规定提供服务的能力; • 可用性：系统在请求时提供服务的能力; • 弹性：系统在及时响应事件时转换，更新和恢复的能力; • 安全性：系统保持免受意外或故意攻击的能力。

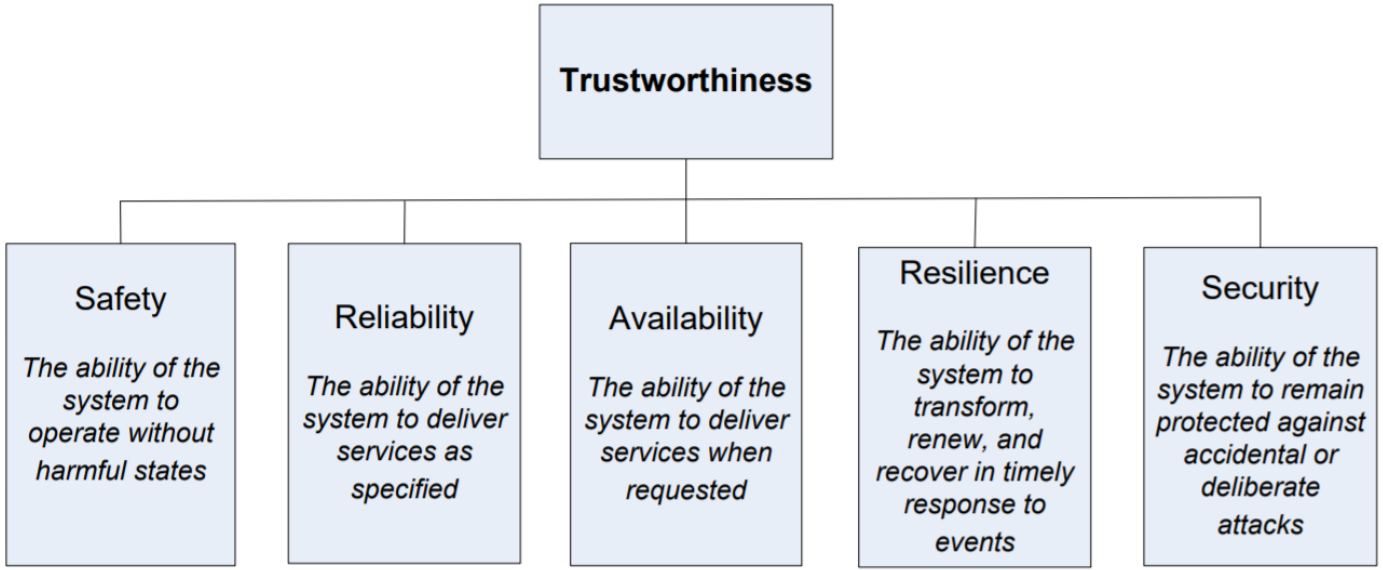
10th edition

我们发现，客户/业界对于可信、安全的诉求在变化

- 业界乃至客户，不仅仅要求结果可信（运行时可信），还要求软件开发过程的可信（开发时可信）
- 企业客户选择云供应商，排在首要位置的是：安全
  - 基础设施安全（数据、网络）
  - 服务安全（权限控制，防攻击、防侵入）
  - 运营运维安全（安全事件的响应，漏洞管理，开源、第三方安全管理）
- 云厂商越来越强调安全左移，Build-In Sec in DevOps
  - 强调自动化，可监控，封闭防篡改，可重复
  - 安全运营团队参与代码级的测试验证

下一代软件工程的思考：Velocity + Trustworthiness

Velocity + Reliability → Velocity + **Trustworthiness**

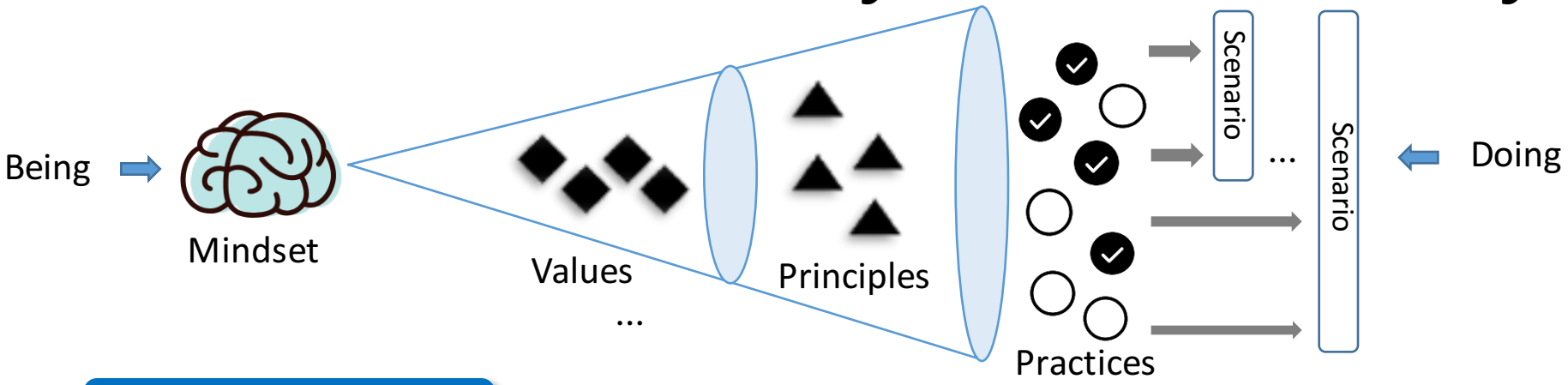


目录

1 我（们）的思考

2 我（们）实践探索

如何开展：Be Trustworthy and Do Trustworthy



软件工程

可信工具链（Built in Security，自动化，可度量）

基础能力、标准、认证

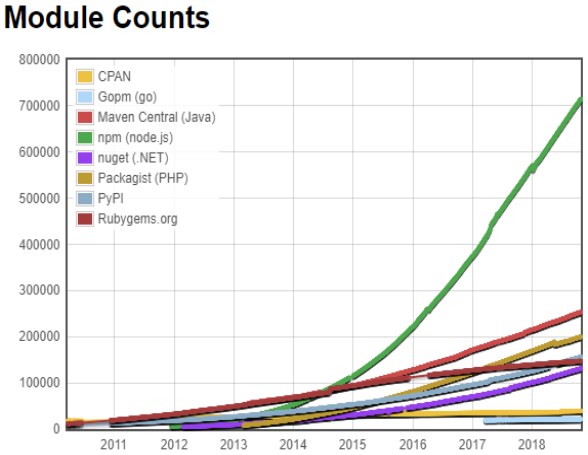
ISO/IEC 、BSI、NIST、DevSecOps ...

土壤和氛围

组织支持 可信的软件文化（鼓励Clean Code） ...

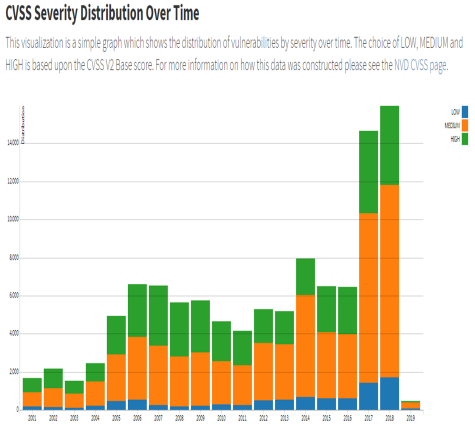
最现实的问题，开源组件的可信

各语言开源组件生态发展迅速
现代软件开发已离不开开源



- 开源组件增长迅速，主流开发语言开源组件数量已达200万+，其中nodejs组件排名第一（约70万），java组件第二（约30万），PHP组件第三（约20万）持续发展上。
- Synopsy发布的《2018 年开源代码安全和风险分析》（OSSRA）报告指出96%被扫描的应用中存在开源组件，每个应用中平均有257个开源组件

开源组件的漏洞问题日益迫切



- 开源组件使用上的安全、优选、合规已经是愈演愈烈的软件企业集体痛点和刚需，
- 美国NIST每年披露的开源组件漏洞持续增加，其中2018年披露了4142个高危险漏洞，10121个中等危险漏洞（CVSS等级）。
- 在sonatype过去两年研究的多个攻击案例中，表明针对开源生态系统的供应链攻击严重升级，攻击者将漏洞直接注入开源组件项目并故意危害下游的数百万应用开发者

一个案例

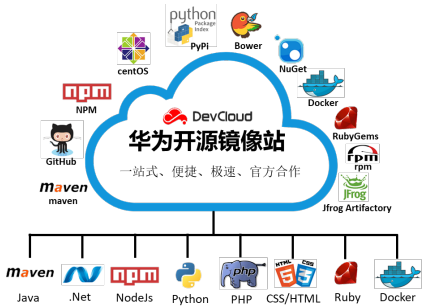
问题原因：网络犯罪分子利用开源组件Apache Struts的公开漏洞（**CVE-2017-5638**）获取文件。该漏洞在2017年**3 月份披露，**漏洞评分为最高分 10 分，Apache 随后发布 Struts 2.3.32 和 2.5.10.1 版本进行修复。但 Equifax 在漏洞出现的两个月内都没有修复，导致 5 月份黑客利用这个漏洞进行攻击，泄露其敏感数据。

背景：2017年5月中旬至7月，美国三大信用评估机构之一的EquIfax遭遇到黑客攻击，导致其系统中大量用户的姓名、社会安保号、生日和地址等私人信息泄露，数据泄漏规模可能涉及到1.43亿美国人，将近一半的美国人会暴露在个人重要私密信息泄漏的风险中（美国目前的总人口约为3.23亿人）。

影响：

- Equifax的股价下跌超30%，市值缩水约 53 亿美金
- CEO、首席信息官和首席安全官离职/退休

我们的一个针对性实践：探索可信的镜像仓管理，并对外孵化

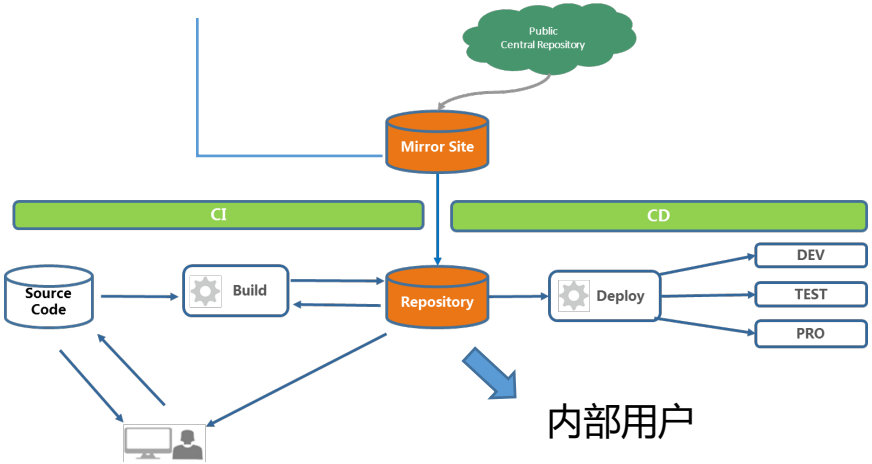


高速

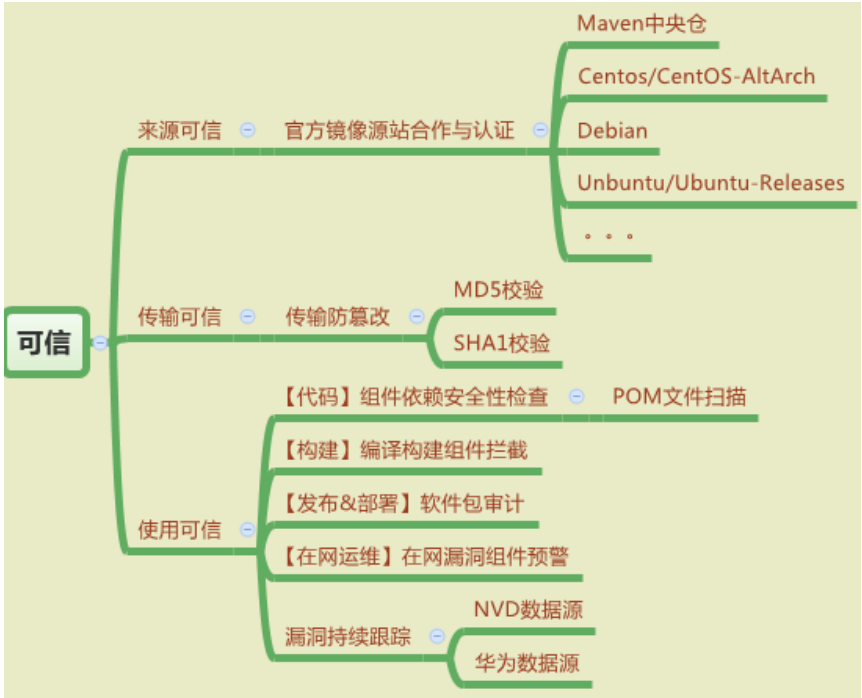
可信

外部用户

mirrors.huaweicloud.com



内部用户



To be continued...

加法？

Or

冲突？

Thanks

高效运维社区

开放运维联盟

荣誉出品

想第一时间看到高效运维社区的新动态吗？

高维在线