DevSecOps工具链实践

张嵩　　华泰证券信息安全总监

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原“中国互联网安全大会”）

安全地软件开发中的挑战

组织与文化

- 开发运维人员缺少安全技能、意识
- 安全专业人员很有限
- 第一道防线安全往往在运维的基础架构类职能下，地位不高，很难对等的协同
- 开发、运维的壁垒，安全职能难以嵌入进IT生命周期的各个阶段
- 开发交付团队，甚至管理层过度地强调“速度”，在与速度的平衡中，对安全风险的机会主义风险偏好过大

过程与控制

- 漏洞多是在上线前一刻被发现，而不是持续在开发的“管道”PIPELINE中被识别—修复成本过高
- 控制点或审计点过于滞后或缺失
- 安全需求、要求、架构设计的持续交付得不到保障
- 缺少全链条各阶段的风险视角和风险管理能力

技术与架构

- 老的、不标准的架构与应用系统
- 最佳实践和架构PATTERN积累有限
- 环境标准化发放和维护程度低

技能与工具

- 安全人员技能欠缺，安全“运营”的程度低
- 安全工具自动化不足或集成程度不高

增加开发人员的责任！！！

DevSecOps ?

什么是DevSecOps? Why?

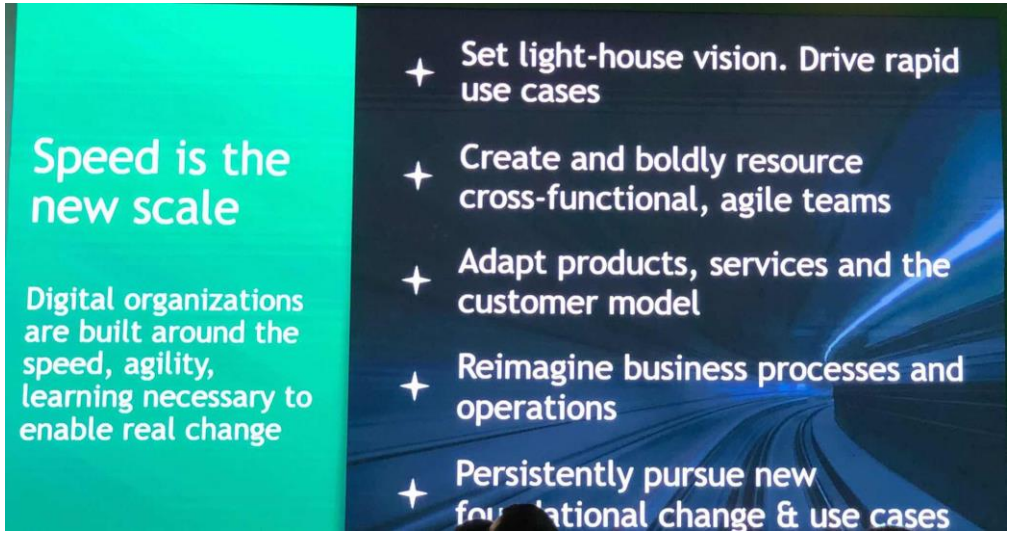
- Gartner 2012年在一份报告中提出的概念。在这份报告中，Gartner提出**信息安全专业人士需要更主动地融入DevOps的实践中，秉承DevOps的精神，拥抱“团队协作、敏捷和职责共担的哲学”**。
- 基于Gartner的调研，估计少于20%的企业安全架构师参与到DevOps的项目中，主动和系统性地将信息安全融入DevOps项目，更少的组织达到了DevSecOps所需的安全自动化程度。
- Gartner认为**通过采用一些良好实践，安全架构师可以设计一系列可集成的控制措施，优化安全活动，同时，并不损害DevOps的敏捷和协作精神**。

安全，从 “守门人”(Gatekeeper) 演变到，赋能(enable)各团队,缺省就处于安全的状态

Security shifts from being a gatekeeper to enabling teams to be secure by default.

CSO适应“快速”

安全需要在适应快速交付的背景下实现协同、保障，提供持续反馈和风险管理能力



BCG：Speed is the new scale

传统安全活动需要太多人，安全测试太慢

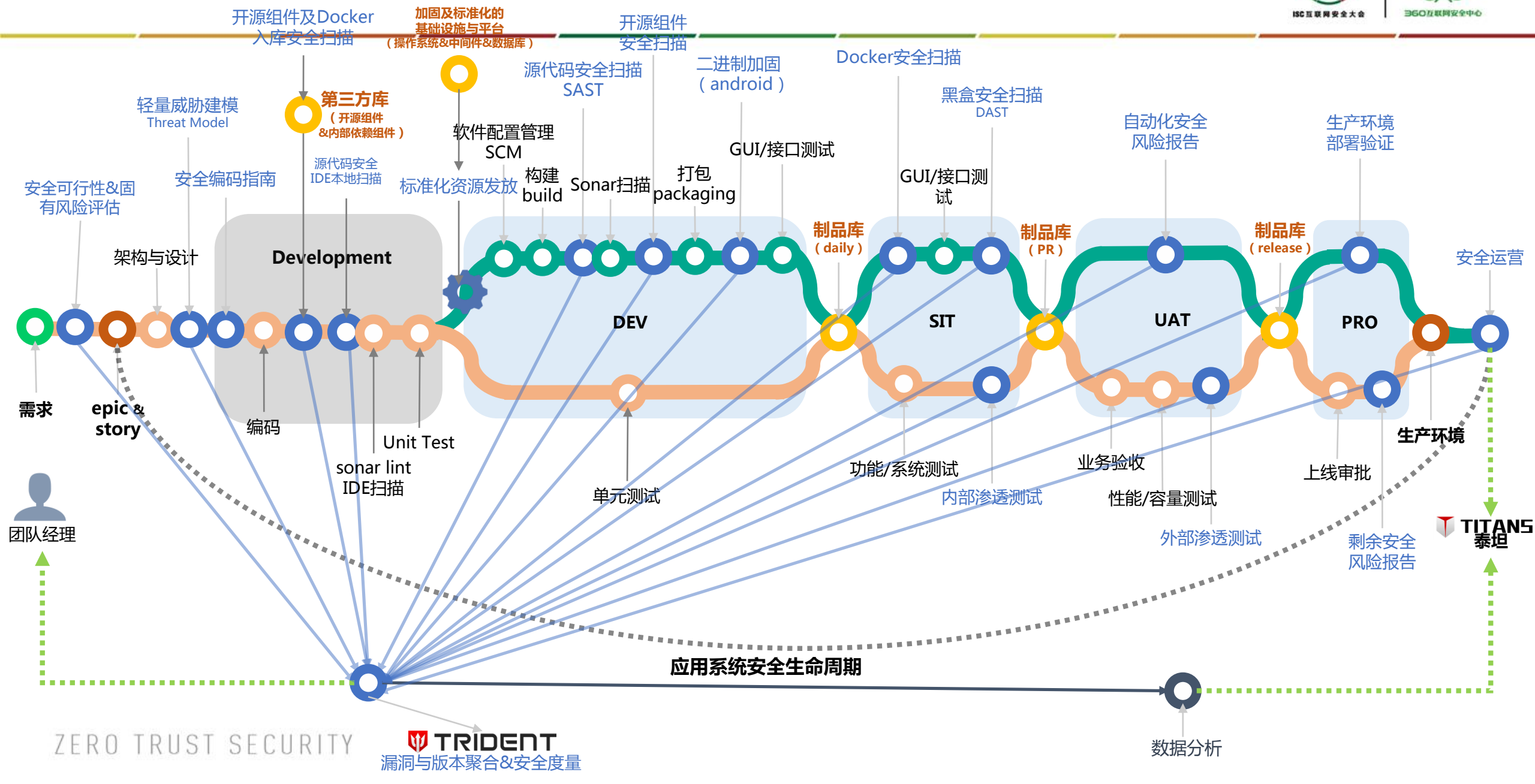
开发应用就像做三明治

自动化！！！

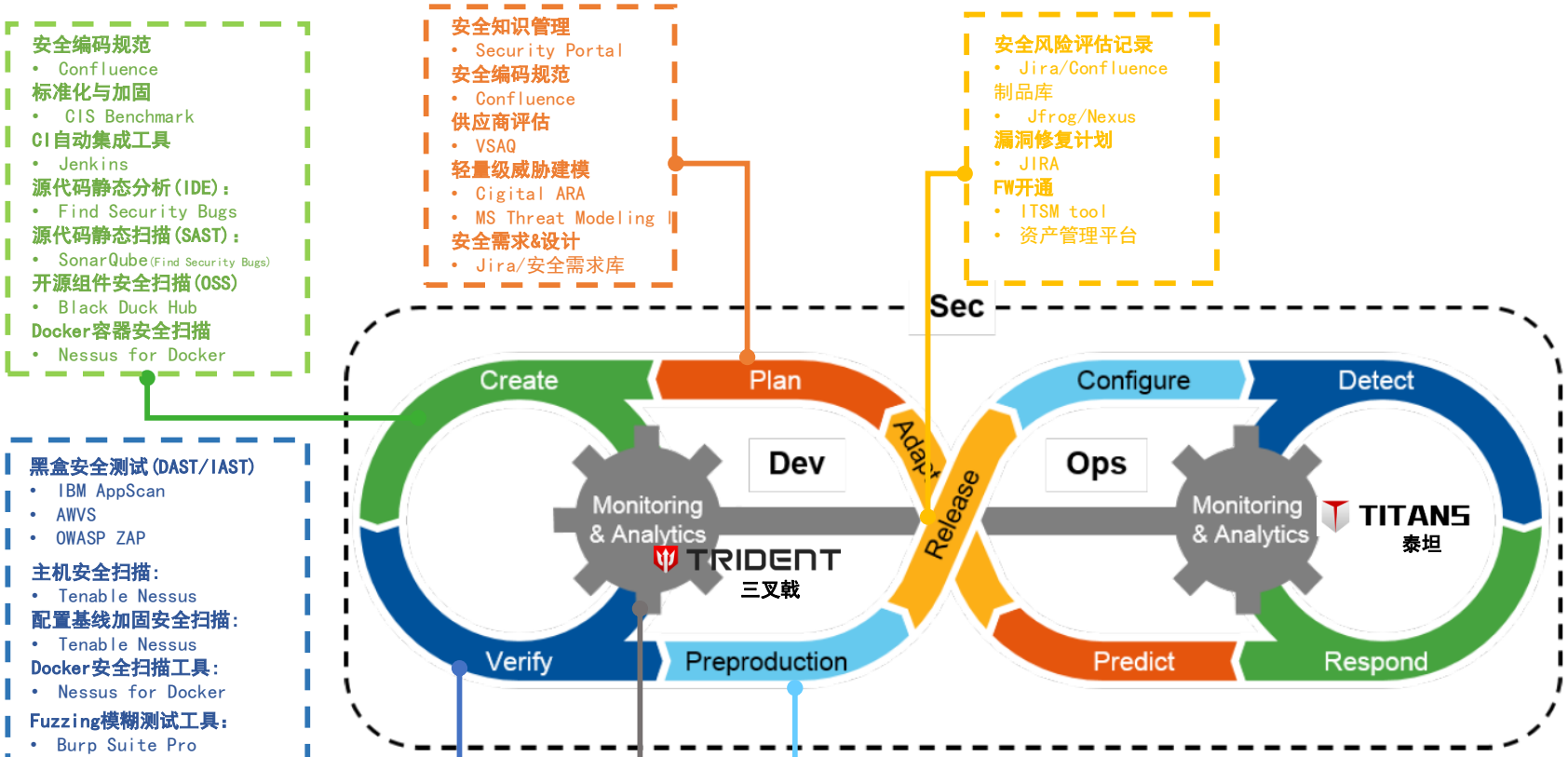
OWASP Glue

ZERO TRUST SECURITY

BUILD SECURITY IN-开发过程的安全嵌入



DEVSECOPS 中可以集成的工具



持续度量与可视化：

缺陷密度、漏洞数、风险问题

走过的路...

30天+

- 找懂开发、应用架构的人
- 在IT项目初期固化引入安全官(ISO)的模式，基于项目优先级确定参与程度
- 全靠人的安全督导和扎口，ISO使用开发人员 友好和偏好的（工作流）工具日常沟通、协作和记录流转，如JIRA
- 引流，再引流，宣传，再宣传，让更多的目标范围的项目组流经ISO
- 开始确定项目需要的最关键、最必要（不做不得上线）的安全活动，往往在生命周期右侧，如PATCH LEVEL，渗透测试

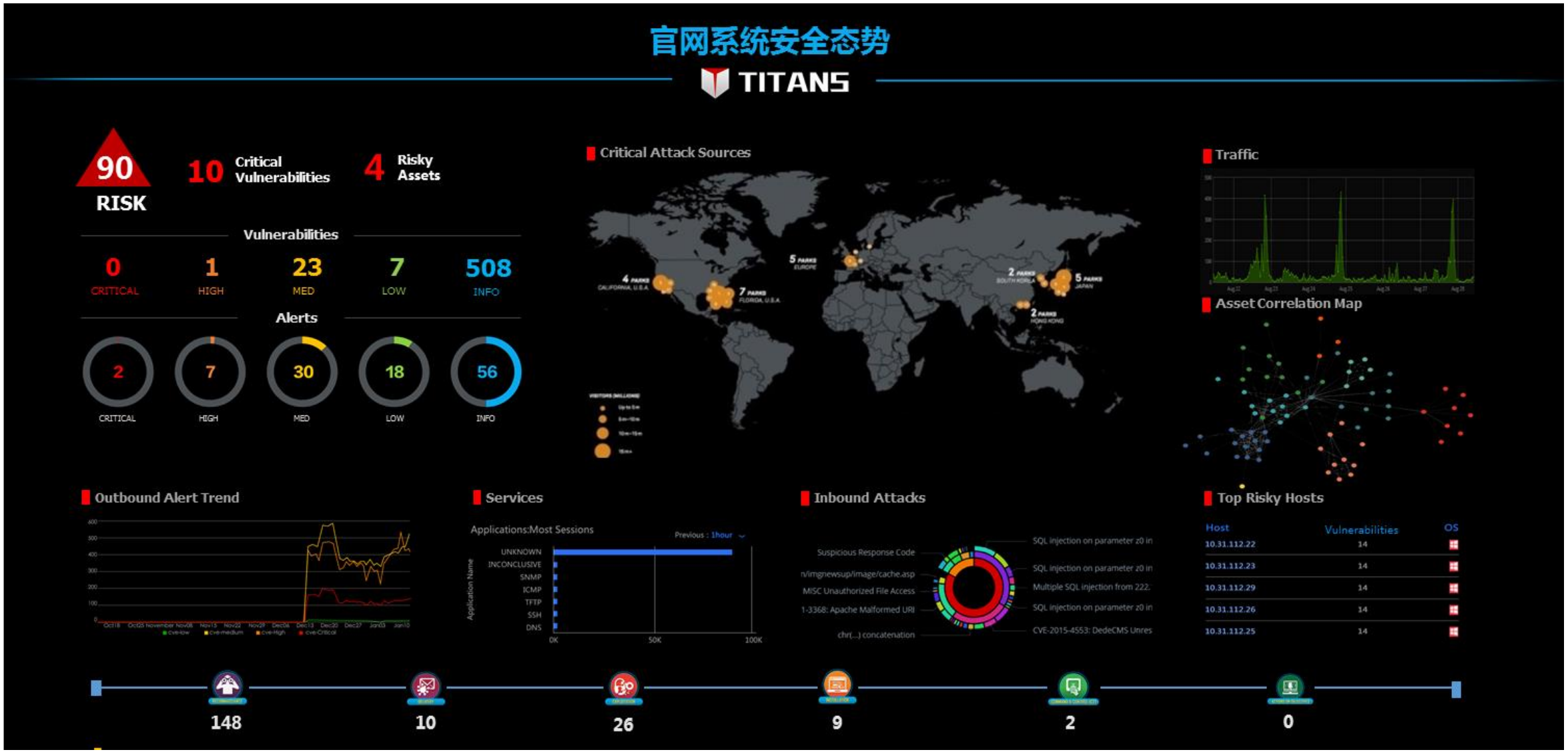
90天+

- 找擅长攻防和渗透测试的人
- 解决资源发放环节的安全，并尽可能自动化，如“黄金镜像”制作和更新，解决PATCH LEVEL，标准化OS、中间件和数据库等基础设施（发行版和版本）
- 借助CIS基线实现加固的自动化和配置标准化
- 提高上线验证测试环节的自动化程度，如自助式WEB黑盒和主机层漏洞扫描
- 引入多源外部渗透测试服务提供方或者众测在SIT、UAT环境进行
- 总结积累黑盒扫描器和渗透测试发现的问题和防御编码，持续实时反馈给开发
- 持续控制措施“左移”
- 参考BSIMM，确定同行“都在做”的
- 探索实践“轻量威胁建模”

180天+

- 与研发质量管理的人协同
- 推动开发管理统一质量静态测试工具链，尽可能使用开发常用工具上安装安全插件，保证体验的一致性，静态检测前置到IDE
- 使用与研发质量管理一致的质量跟踪机制，并建立“度量驱动”的文化和沟通，持续风险问题反馈与安全知识积累
- 与架构师协同，使用统一、一致的架构、框架，从架构治理上降低使用高危框架、组件的几率，关注API安全
- 建立基于项目的分级安全评估和咨询机制，固化各阶段主要安全交付物与活动，确保系统全生命周期的风险问题跟踪机制和基于风险的发布决策（业务和IT产品负责人是主要的决策者）
- 开始关注DOCKER与开源/第三方组件安全，检查漏洞与恶意程序
- 持续提升安全工具自动化和易用程度，开始探索集中化第三方仓库，制品库治理与门限(GATING)，开始规范化“环境”

DEVSECOPS 态势感知能力演进：面向应用资产的安全感知



ZERO TRUST SECURITY

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原“中国互联网安全大会”）