网络安全创新大会
Cyber Security Innovation Summit

DevSecOps软件供应链安全的机遇与挑战

陈钟　北京大学教授网络与信息安全实验室主任

个人介绍

陈钟 北京大学信息科学技术学院教授、网络与信息安全实验室主任

- 主要从事面向领域软件工程、网络与信息安全方向的教学、科研与社会服务，取得多项国家级教学与科研成果和奖励
- 北京大学软件与微电子学院创始院长（2002-2010）
- 计算机科学技术系主任（2011-2015）
- 教育部高等学校计算机类专业教学指导委员会副主任委员
- 中国软件行业协会副理事长及软件造价分会会长
- 信息技术新工科产学研联盟副理事长
- 中国开源软件推进联盟副理事长
- ISACA中国专家委员会委员
- .....

演讲目录

网络安全创新大会
Cyber Security Innovation Summit

软件供应链安全现状

面临的风险和挑战

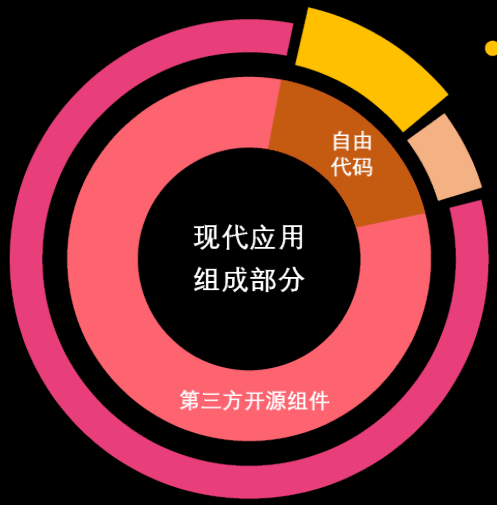
软件开源化的趋势，造就软件供应链的开源化

软件供应链开源化造成软件供应链安全问题开始呈现

软件供应链的安全威胁导致软件全生命周期存在永远无法消除的安全隐患

现代应用安全的风险面

针对现代应用全面风险审查应考虑从第三方开源组件、自研代码通用漏洞、自研代码业务逻辑漏洞等维度综合审计。



Web通用漏洞

SQL注入、命令执行、XXE、XSS等OWASP TOP10

业务逻辑漏洞

水平/垂直越权、短信轰炸、批量注册、验证码绕过等

开源组件缺陷

CNNVD、CNVD、CVE等

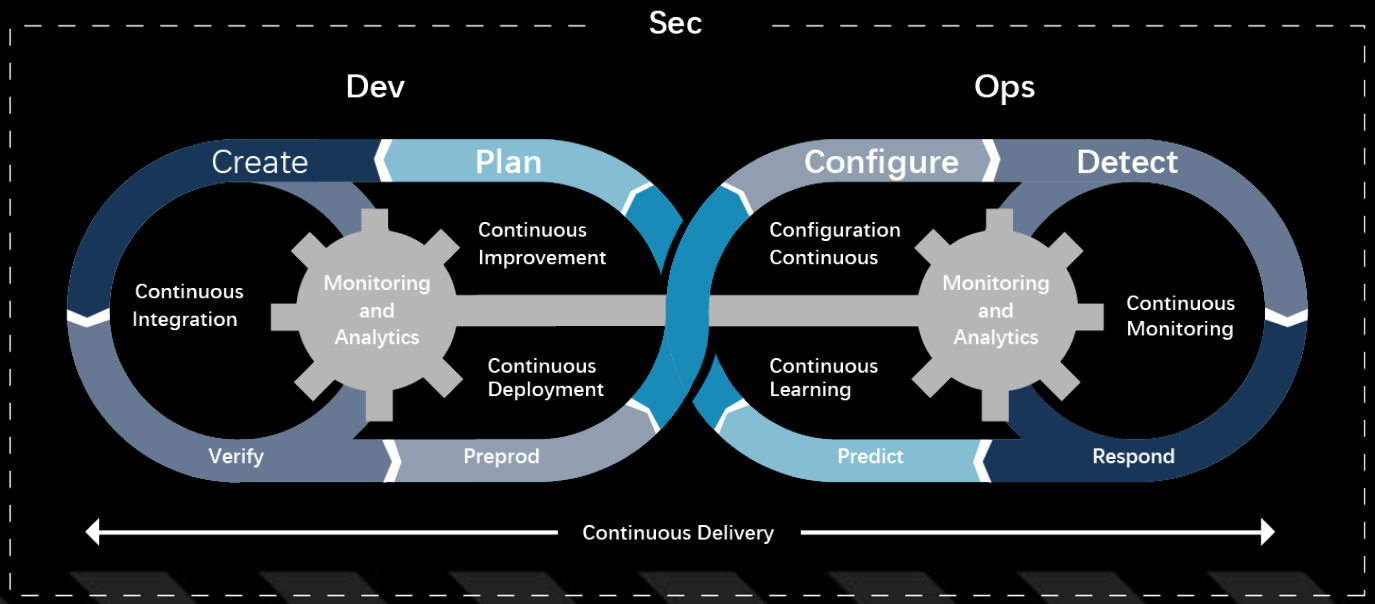
DevSecOps的引入

DevSecOps的引入

- DevSecOps（Development Security Operations）

核心理念：“安全是整个IT团队所有成员的责任，需要贯穿整个业务生命周期的每一个环节”

DevOps Is a Continuous Cycle



Source: Gartner
ID: 377293

DevSeOps的RSAC演进

历届RSAC上DevSecOps的演进

时间	里程碑	内容和意义
RSAC 2017	提出左移安全前置的思想	• 源头做安全治理 • 运营向开发的持续反馈调整
RSAC 2018	提出“Golden Pipeline”实践体系，强调 CI/CD 自动化工具链支撑	• 确定出一套适应CI/CD的软件流水线实践体系 • 工具链：稳定、可落地、安全
RSAC 2019	提出DevSecOps落地实践效果度量机制	• DevSecOps宣言 • 提升“简单领域”的自动化和集成程度，聚焦在业务领域的复杂问题上（组织、管控流程等） • DevSecOps的实践度量机制：六个阶段九个实践点：人工环节、架构设计、DevSecOps工具链、全流程漏洞管理、漏洞治理政策、攻防对抗演练
RSAC 2020	聚焦DevSecOps文化转型，强调人的因素	• 人的行为自始至终就与数据、威胁、风险、隐私及管理等因素交织在一起 • 让人成为安全的一环，而非问题的一环 • DevSecOps文化的转型，人是关键

从RSAC 2017年第一次设立DevSecOps day至今，DevSecOps体系日趋成熟，相关方法论、技术与实践经验都有了明显的提升，配套工具链技术也日趋完善，这其中多少要感谢一些国内外技术创新力量的贡献。

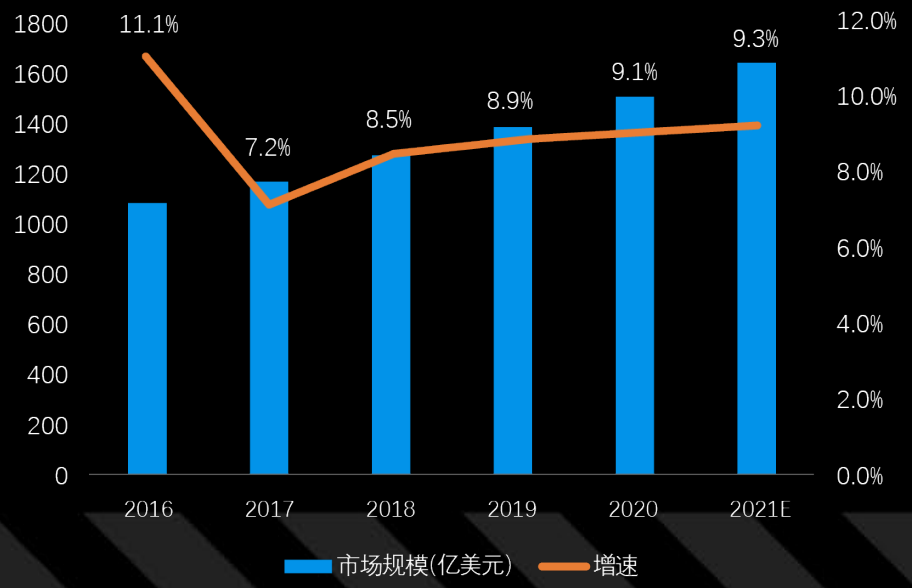
DevSecOps的机遇

开发安全市场全球需求稳步增长

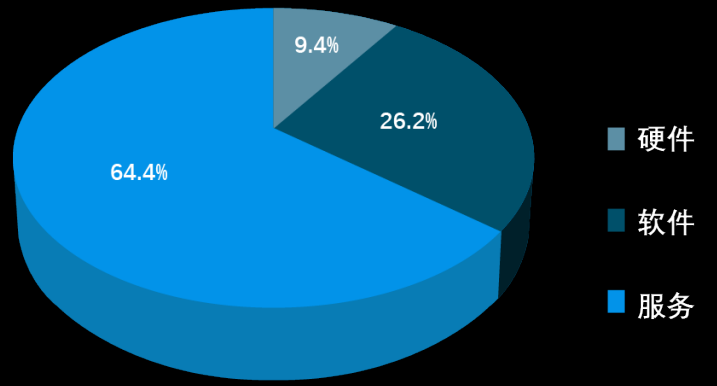
网络安全创新大会
Cyber Security Innovation Summit

- 2020年全球网络安全市场规模增长至9.1%
- 安全服务与软件安全占比达80.6%

全球网络安全市场规模



2018年全球网络安全市场结构



数据来源：公开资料整理

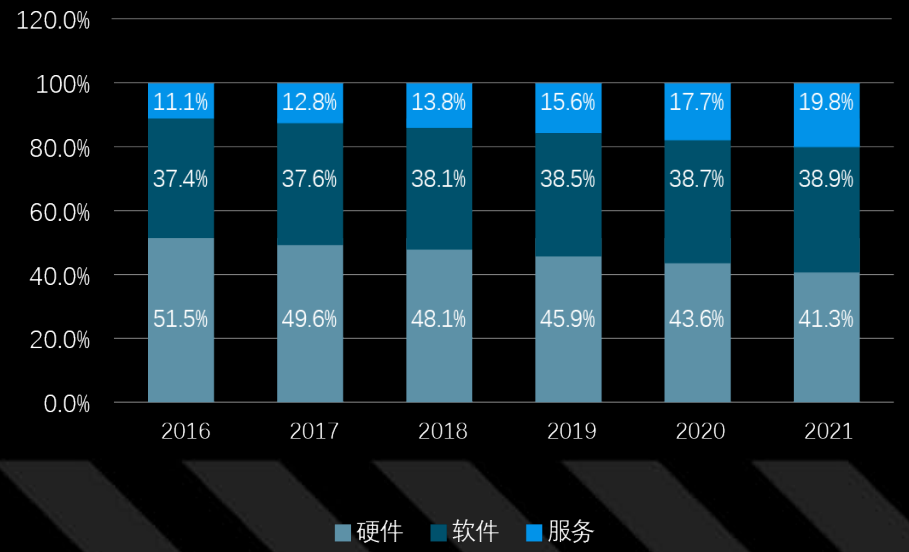
国内市场

网络安全创新大会
Cyber Security Innovation Summit

- 我国**网络安全市场迎来快速发展期**，网络安全应用市场广泛
- 政府、电信与金融领域应用网络安全产品和服务最多
- 很多细分领域的安全需求成为推动网安行业持续增长的动力
- 我国网络安全行业保持在20%以上的增长，**2020年市场规模达到749.2亿**，软件占比达到38.7%

中国网络安全市场与增速

中国网络安全市场结构



数据来源：公开资料整理

国家层面关注度（网络安全法、等保等）

网络安全创新大会
Cyber Security Innovation Summit

时间	政策文件	要点
2016年11月	**《网络安全法》**	强调了金融、能源、交通、电子政务等行业在网络安全等级保护制度的建设，是我国第一部网络空间管理方面的基础性法律
2017年1月	**《信息通信网络与信息安全规划（2016-2020年）》**	指导信息通信行业开展"十三五"期间网络信息安全工作，服务网络强国建设、国家安全和社会稳定的大局
2018年3月	**《关于推动资本市场服务网络强国建设的指导意见》**	推动网信事业和资本市场协调发展，保障国家网络安全和金融安全，促进网信和证券监督工作联动。
2019年5月	**《网络安全等级保护技术2.0版本》**	提出了对云计算安全、移动互联网安全、物联网安全和工业控制系统安全扩展要求。为落实信息安全工作提出了新的要求。
2020年4月	**《网络安全审查办法》**	关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照《办法》进行网络安全审查。

2016年至今部分重要网络安全政策

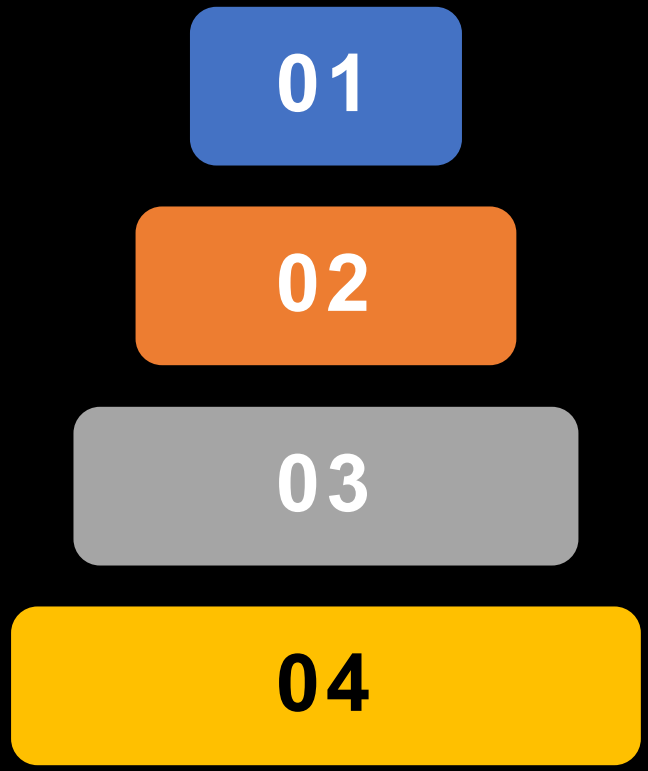
自2012年由Gartner 提出后，正逐步吸引业界的目光

- RSA大会上，2020年的10强中有三家企业和DevSecOps相关
- 国内围绕DevSecOps的讨论增多，十余家厂商聚焦在开发安全层面

DevSecOps关键工具链技术

DevSecOps的几点思考

如何落地实施？



01 开展全方位的软件供应链安全防护方法和技术研究

02 建立国家层面的软件供应链安全监管评测体系

03 提升网站中开源软件源代码的防篡改防伪造技术等防护水平

04 推动新技术在软件供应链安全领域的应用，从根本上可靠

关于DevSecOps的几点思考

- 本质是风险和信任的平衡
- 攻防对抗是安全的脉搏
- 人是安全的基本尺度
- 从源头做威胁治理

网络安全创新大会
Cyber Security Innovation Summit

THANKS