聚力·引领
软件安全学术论坛

建设软件安全开发体系
是保障国家网络安全的重要基础

王颉
开源网安

关于我

王颉

- 英国拉夫堡大学网络安全专业博士
- 开源网安创始人之一
- OWASP中国区域副主席
- 致力于应用安全与软件安全开发理念和技术的推广

聚力·引领
软件安全学术论坛

目录Catalog

01.

国家网络安全战略

聚力·引领

软件安全学术论坛

国家网络安全战略

“没有网络安全就没有国家安全” 	《中华人民共和国网络安全法》 	国家网络安全人才与创新基地 	网络安全等级保护技术2.0版 
习主席2014年2月27日，在“中央网络安全和信息化领导小组第一次会议”上的讲话	2017年6月1日起施行。标志着国家网络安全将拥有更为完善的法律基础和保障。	2017年8月23日，动工开建，标志着国家网络安全人才与创新基地进入实质性建设阶段。	2019年5月13日正式公开发布，并将于2019年12月1日开始实施。

国家网络安全战略

典型政策

《网络安全法》	第三十四条，关键信息基础设施的运营者应当定期对从业人员进行网络安全教育、技术培训和技能考试。
中央网信办《关于加强网络安全学科建设和人才培养的意见》	第三条“加强网络安全教材建设”。国家加强引导，鼓励出版社、企业和社会资本支持网络安全教材编写。适应网络教学、远程教学发展，加大对网络教材的支持力度。 第六条“加强网络安全从业人员在职培训”。鼓励并规范社会力量、网络安全企业开展网络安全人才培养和在职人员网络安全培训。
国家教育部《2018年教育信息化和网络安全工作要点》	第三部分第（八）条“提升网络安全人才培养能力和质量”。第24点：“加强网络安全人才培养”。第25点：“强化网络安全宣传教育”。

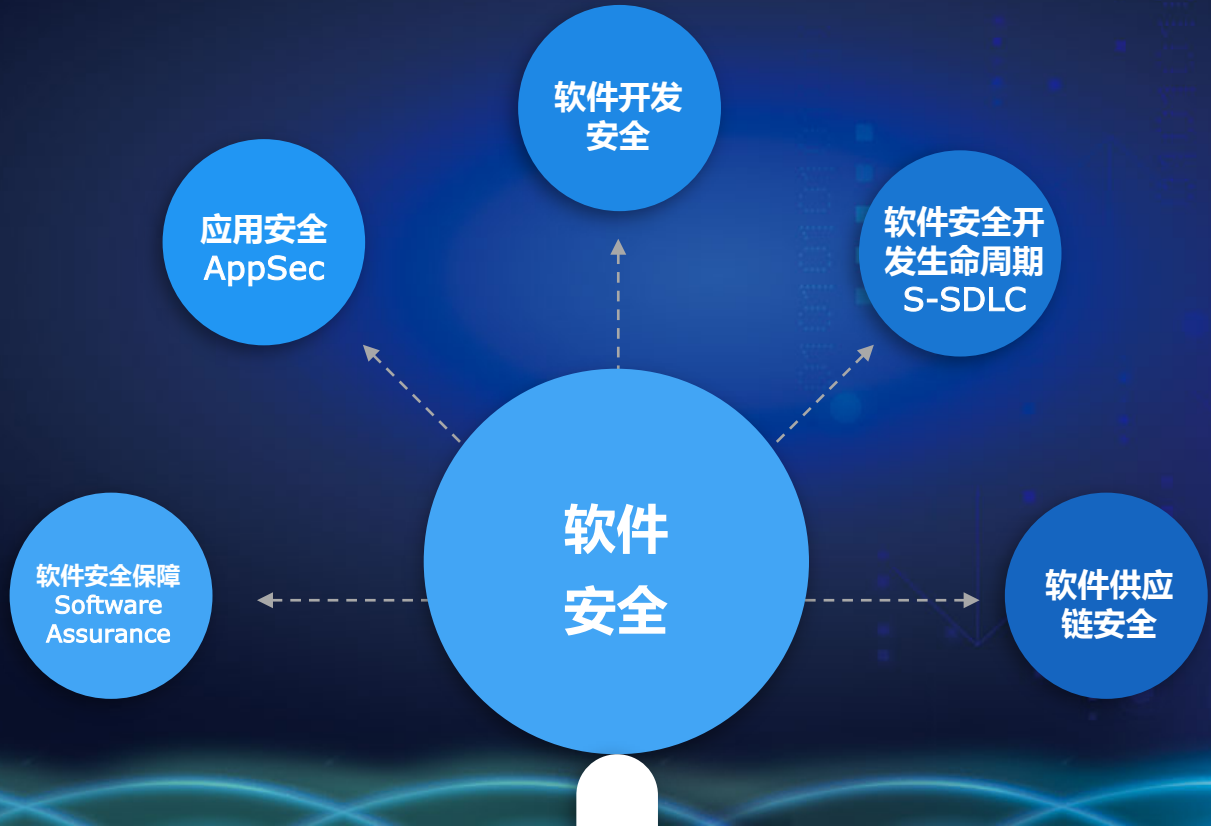
02.

全球软件安全态势

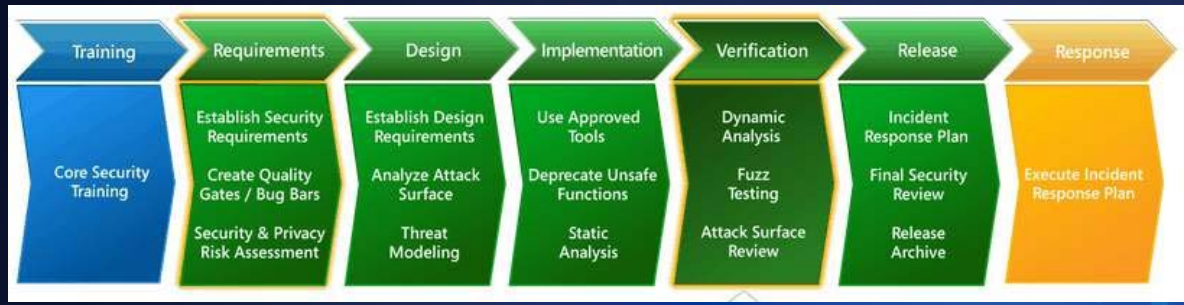
聚力·引领
软件安全学术论坛

对于软件安全的定义

对于软件安全的定义


软件开发安全
应用安全 AppSec
软件安全开发生命周期 S-SDLC
软件安全
软件安全保障 Software Assurance
软件供应链安全

国外知名软件安全方法论



Microsoft Secure Development Lifecycle (SDL)

BSIMM

Synopsys Build Security Inside Maturity Model (BSIMM)

OWASP
Open Web Application Security Project

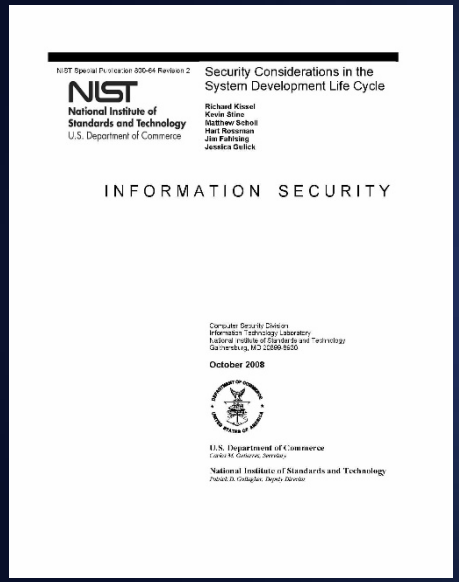
OWASP Software Assurance Maturity Model (SAMM)

国外知名软件安全标准——行业

2017年版《OWASP Top 10》
A1:2017 – 注入
A2:2017 –失效的身份认证
A3:2017 –敏感信息泄漏
A4:2017 – XML外部实体（XXE
A5:2017 – 失效的访问控制
A6:2017 – 安全配置错误
A7:2017 – 跨站脚本（XSS）
A8:2017 – 不安全的反序列化
A9:2017 –使用含有已知漏洞的组件
A10:2017 – 不足的日志记录和监控

全球应用安全、软件安全、网络安全领域的重要参考！

国外知名软件安全标准——发达国家


NIST Special Publication 800-64 Revision 2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Security Considerations in the System Development Life Cycle

Richard Kissel
Kevin Stine
Matthew Scholl
Hart Rossman
Jim Fahlsing
Jessica Gulick

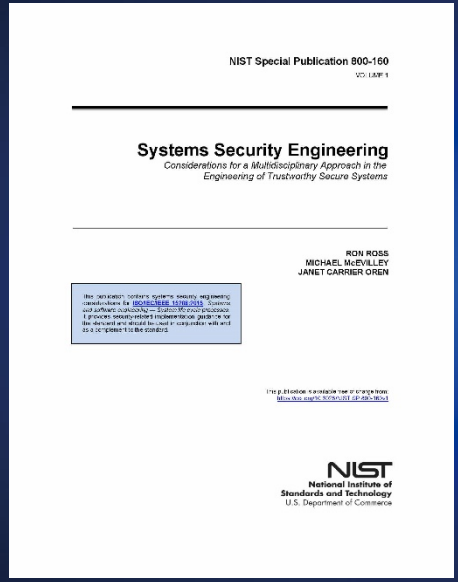
INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director


NIST Special Publication 800-160

Systems Security Engineering

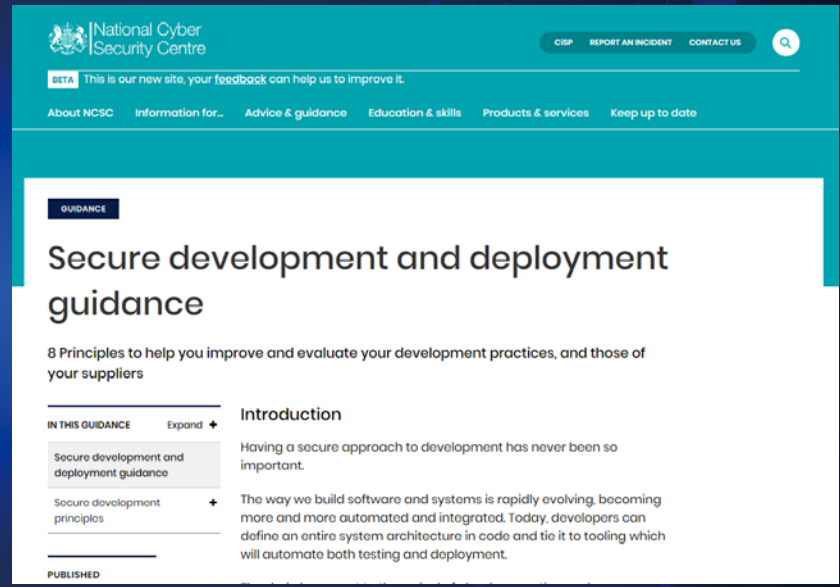
Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

RON ROSS
MICHAEL McEVILLEY
JANET CARRIER OREN

This publication contains systems security engineering considerations for ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes. It provides security-related implementation guidance for the standard and should be used in conjunction with and as a companion to the standard.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-160v1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


National Cyber Security Centre

CISP REPORT AN INCIDENT CONTACT US

BETA This is our new site, your feedback can help us to improve it.

About NCSC | Information for... | Advice & guidance | Education & skills | Products & services | Keep up to date

GUIDANCE

Secure development and deployment guidance

8 Principles to help you improve and evaluate your development practices, and those of your suppliers

IN THIS GUIDANCE Expand +

Secure development and deployment guidance

Secure development principles +

PUBLISHED

Introduction

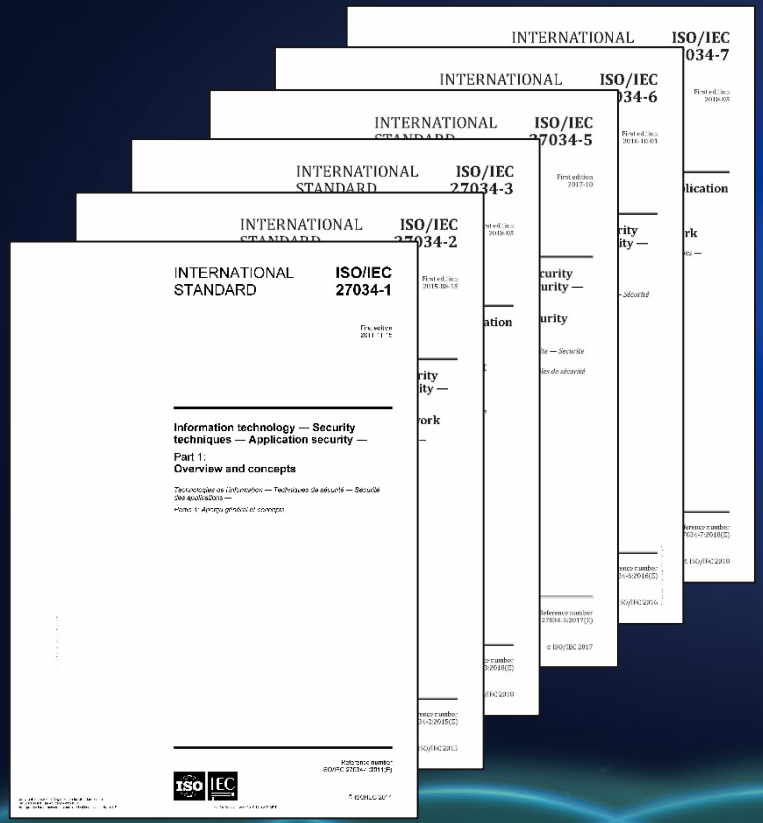
Having a secure approach to development has never been so important.

The way we build software and systems is rapidly evolving, becoming more and more automated and integrated. Today, developers can define an entire system architecture in code and tie it to tooling which will automate both testing and deployment.

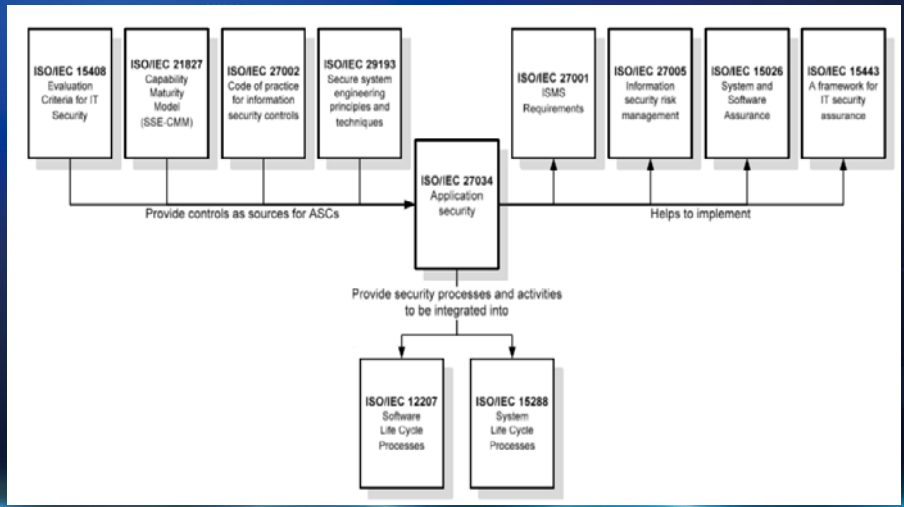
美国国家标准和技术研究院（NIST）
NIST SP800-64和NIST SP800-160

英国NCSC发布的
安全开发和部署的8大原则

国外知名软件安全标准——ISO27034



ISO 27034提供了面向企业落地应用安全生命周期的指导框架，其本质目的是指导企业如何通过标准化的方式把安全融合进入软件生存周期。ISO 27034本身并不是一个应用软件的开发标准或软件开发生命周期标准；并且，ISO 27034不提供有关度量的控制机制或实践，也不提供有关应用软件开发语言的安全编码规范。



全球软件安全企业

根据全球顶级应用安全组织OWASP的发布，全球范围内重视应用安全技术、支持应用安全发展的企业包括：

03.

软件安全的影响

聚力·引领
软件安全学术论坛

现代软件开发的模式

- 现代软件不是被"开发"出来的，而是"组装"出来的；
- 软件开发中，大量的代码来源于开源代码或开源组件；
- 敏捷开发，DevOps与安全融合，形成DevSecOps。

超过10%（351000个）的组件至少包含一个已知漏洞。

开源软件（源代码）安全

开源软件源代码安全缺陷分析报告

原创：CNCERT软件安全 CNCERT风险评估 前天

开源软件源代码安全缺陷分析报告

——物联网软件专题

1、概述

随着软件技术飞速发展，开源软件已在全球范围内得到了广泛应用。数据显示，99%的组织在其IT系统中使用了开源软件。开源软件的代码一旦存在安全问题，必将造成广泛、严重的影响。为了解开源软件的安全情况，CNCERT持续对广泛使用的知名开源软件进行源代码安全缺陷分析，并发布季度安全缺陷分析报告。

自2005年国际电信联盟（ITU）正式提出"物联网（IoT）"这一概念以来，物联网在全球范围内迅速获得认可。随着物联网技术的发展创新，大量智能家居和可穿戴设备进入了人们的生活，"万物互联"成为全球网络未来发展的重要方向。根据Gartner报告预测，2020年全球物联网设备数量将高达260亿个。然而，由于安全标准滞后，以及智能设备制造商缺乏安全意识和投入，物联网已经埋下极大隐患，为个人隐私、企业信息安全甚至国家关键基础设施带来严重的安全威胁。

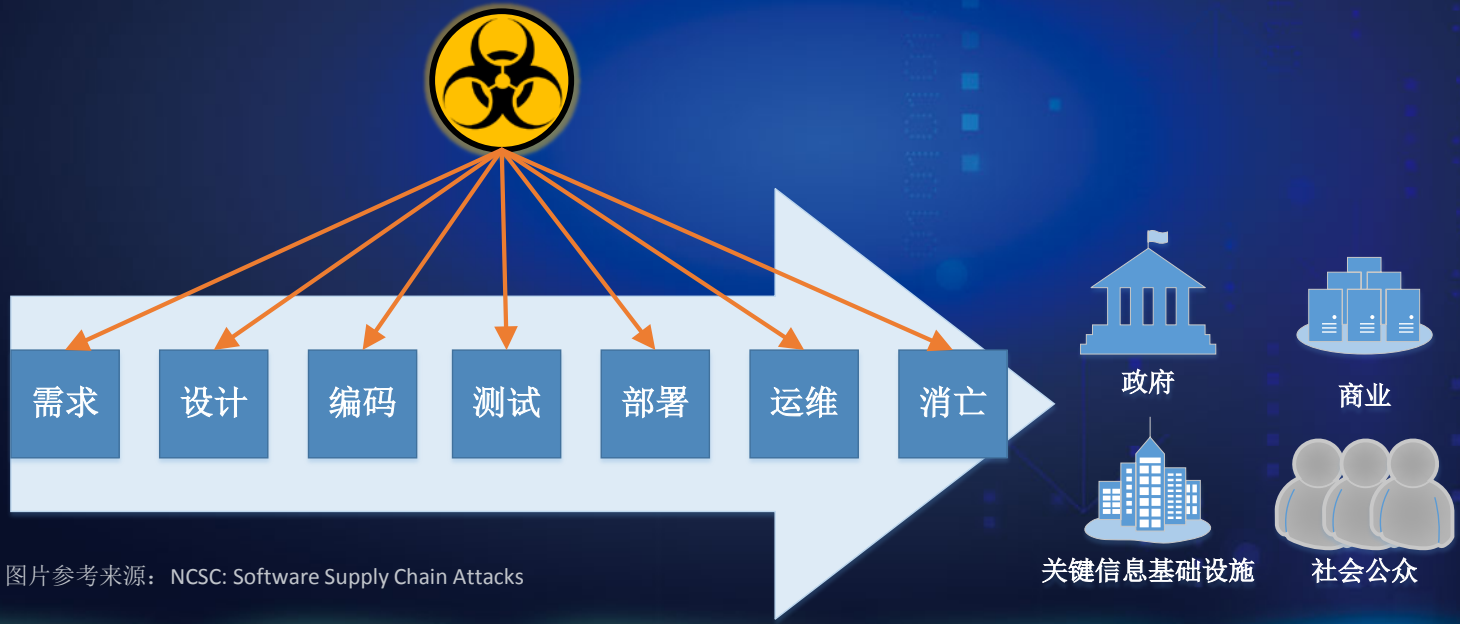
本期报告选取全球20款知名物联网软件进行源代码安全缺陷分析，结合缺陷分析工具和人工审计的结果，评估项目的安全性。从测评结果来看，与往期其他领域开源软件相比，物联网类软件的安全缺陷较多，潜在的安全问题不容忽

安全缺陷种类：

1、输入验证
2、API使用
3、安全特性
4、并行计算
5、错误和异常处理
6、代码质量
7、封装和隐藏
8、代码运行环境

参考来源：CNCERT风险评估， 2019年1月10日，开源软件源代码安全缺陷分析报告——物联网软件专题

- 通过软件供应链上任何阶段对软件代码的恶意行为，影响或破坏最终用户的信息安全。



图片参考来源：NCSC: Software Supply Chain Attacks

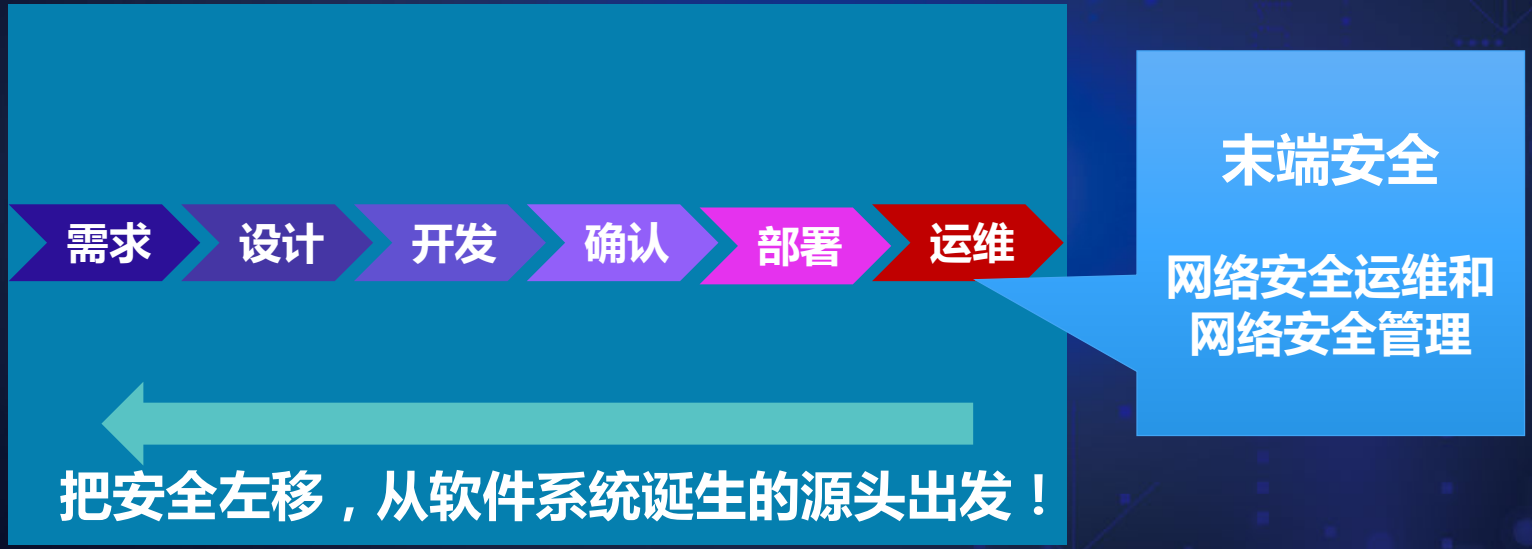
软件供应链安全/攻击

图片参考来源：NCSC: Software Supply Chain Attacks

软件供应链安全/攻击


•软件规模越来越大，程序逻辑越发复杂，设计缺陷、深层漏洞更难发现。
难以发现
•对软件算法或代码的重复使用。
重复使用
能力不足
•软件开发过程的质量保障能力不足；
•不具备软件安全开发的能力。
轻视安全
•软件开发商更多从产品投入产出效益上考虑，注重产品功能而轻视安全性

全球行业共识：把安全左移

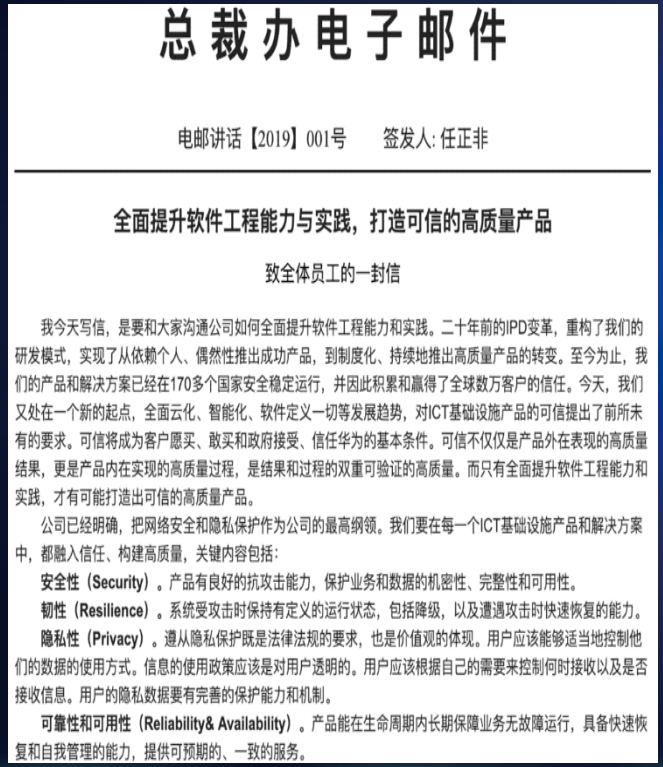


安全开发对企业的益处

- 在产品开发过程中，越早修复安全漏洞，成本投入越低。

源: Ponemon Institute Research

安全开发对企业的益处



总裁办电子邮件

电邮讲话【2019】001号　　签发人: 任正非

全面提升软件工程能力与实践，打造可信的高质量产品

致全体员工的一封信

我今天写信，是要和大家沟通公司如何全面提升软件工程能力和实践。二十年前的IPD变革，重构了我们的研发模式，实现了从依赖个人、偶然性推出成功产品，到制度化、持续地推出高质量产品的转变。至今为止，我们的产品和解决方案已经在170多个国家安全稳定运行，并因此积累和赢得了全球数万客户的信任。今天，我们又处在一个新的起点，全面云化、智能化、软件定义一切等发展趋势，对ICT基础设施产品的可信提出了前所未有的要求。可信将成为客户愿买、敢买和政府接受、信任华为的基本条件。可信不仅仅是产品外在表现的高质量结果，更是产品内在实现的高质量过程，是结果和过程的双重可验证的高质量。而只有全面提升软件工程能力和实践，才有可能打造出可信的高质量产品。

公司已经明确，把网络安全和隐私保护作为公司的最高纲领。我们要在每一个ICT基础设施产品和解决方案中，都融入信任、构建高质量，关键内容包括：

安全性（Security）。产品有良好的抗攻击能力，保护业务和数据的机密性、完整性和可用性。

韧性（Resilience）。系统受攻击时保持有定义的运行状态，包括降级，以及遭遇攻击时快速恢复的能力。

隐私性（Privacy）。遵从隐私保护既是法律法规的要求，也是价值观的体现。用户应该能够适当地控制他们的数据的使用方式。信息的使用政策应该是对用户透明的。用户应该根据自己的需要来控制何时接收以及是否接收信息。用户的隐私数据要有完善的保护能力和机制。

可靠性和可用性（Reliability& Availability）。产品能在生命周期内长期保障业务无故障运行，具备快速恢复和自我管理的能力，提供可预期的、一致的服务。

- 我们要转变观念，追求打造**可信的高质量产品**，不仅仅是功能、特性的高质量，也包括**产品开发到交付过程的高质量**。
- 我们要从最基础的**编码质量**做起，视高质量代码为尊严和个人声誉。
- 我们要深刻理解架构的核心要素，基于可信导向来进行**架构与设计**。
- 我们要重构腐化的架构及不符合软件工程规范和质量要求的**历史代码**。
- 我们要深入钻研**软件技术**，尤其是**安全技术**。
- 我们要遵守过程的**一致性**。
- 为此，我们**要改变行为习惯，追求精品**。我们要开放透明、积极和勇于揭示问题并主动推动改进。

04.

建设软件安全开发体系

聚力·引领
软件安全学术论坛

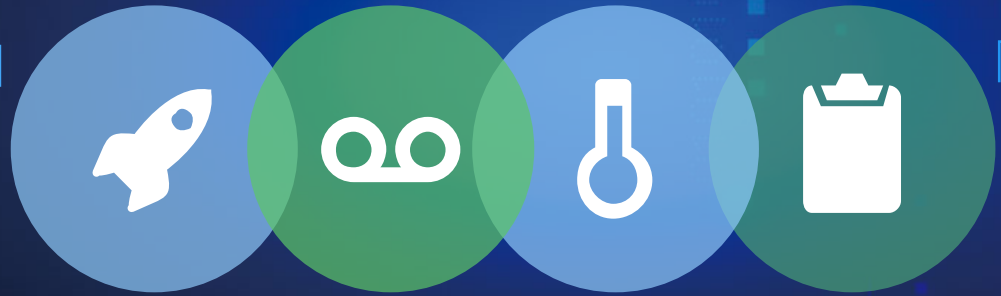
建设我国软件安全体系的思路

国家主管部门

- 制定综合应对战略，统筹推进相关政策法规、标准规范的建设与应用；
- 鼓励和引导自主可控信息技术领域对软件供应链安全技术的应用和保障；
- 加强软件供应链安全的监管；
- 推动国家软件安全专业人才培养；
- 推动测评机构有效开展软件安全与软件供应链安全的测评工作。

软件安全服务供应商

- 加强软件供应链安全技术的研究与创新；
- 配合国家主管部门开展软件安全公共服务；
- 支持国家开展软件安全专业人才培养；
- 协助软件开发供应商和软件使用单位消除软件安全威胁。



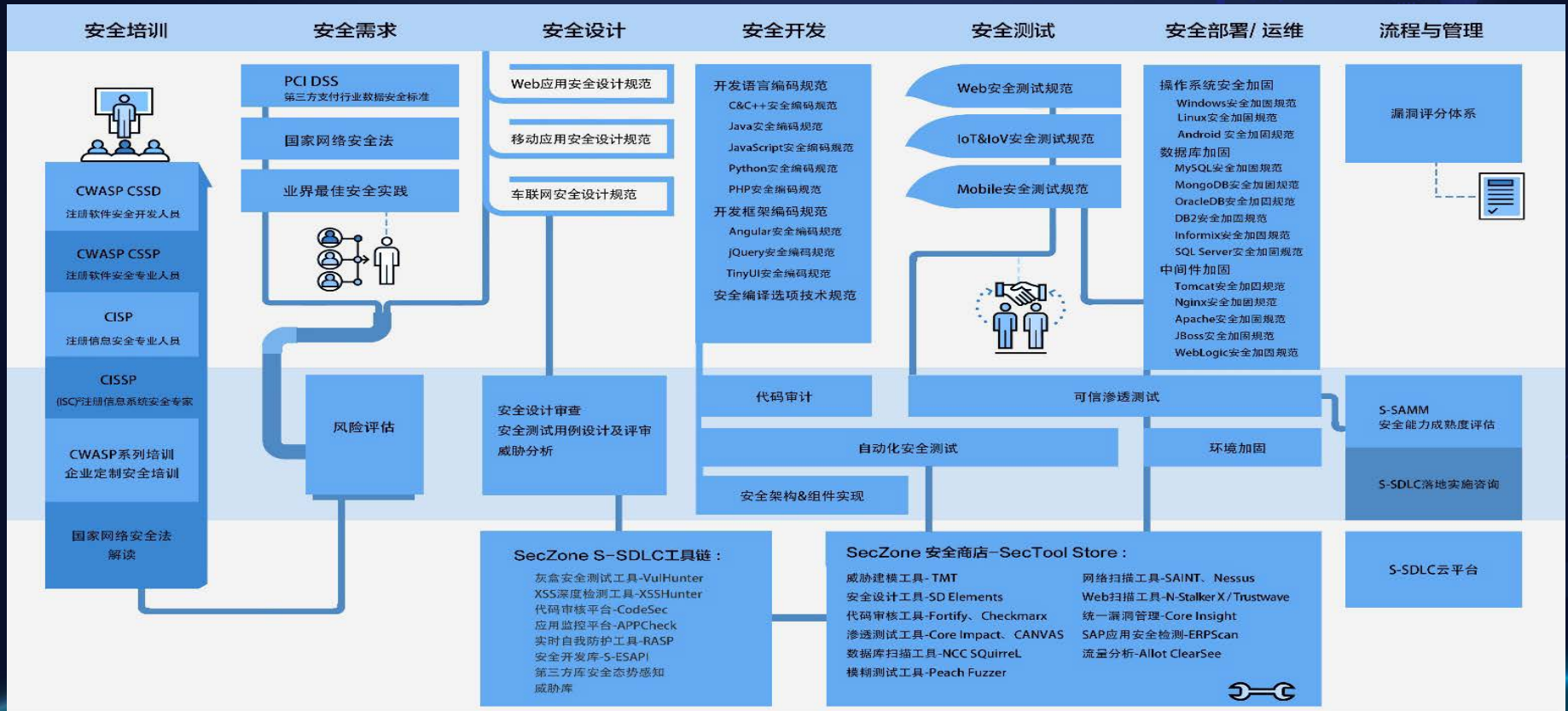
软件开发供应商

- 加强自身软件供应链安全的责任要求；
- 完善自身软件安全开发与质量保障体系；
- 建设自身软件安全开发所需的能力；
- 在软件开发过程中落实安全开发举措。

软件使用单位

- 加大软件安全保障认知，明确软件安全保障的管理职责；
- 对软件开发供应商明确提出软件安全开发的要求；
- 依托专业机构开展软件供应链安全的审计。

软件安全开发体系


安全培训
安全需求
安全设计
安全开发
安全测试
安全部署/ 运维
流程与管理
CWASP CSSD
注册软件安全开发人员
CWASP CSSP
注册软件安全专业人员
CISP
注册信息安全专业人员
CISSP
(ISC)²注册信息系统安全专家
CWASP系列培训
企业定制安全培训
国家网络安全法
解读
PCI DSS
第三方支付行业数据安全标准
国家网络安全法
业界最佳安全实践
风险评估
Web应用安全设计规范
移动应用安全设计规范
车联网安全设计规范
安全设计审查
安全测试用例设计及评审
威胁分析
开发语言编码规范
C&C++安全编码规范
Java安全编码规范
JavaScript安全编码规范
Python安全编码规范
PHP安全编码规范
开发框架编码规范
Angular安全编码规范
jQuery安全编码规范
TinyUI安全编码规范
安全编译选项技术规范
代码审计
自动化安全测试
安全架构&组件实现
Web安全测试规范
IoT&IoV安全测试规范
Mobile安全测试规范
可信渗透测试
环境加固
操作系统安全加固
Windows安全加固规范
Linux安全加固规范
Android 安全加固规范
数据库加固
MySQL安全加固规范
MongoDB安全加固规范
OracleDB安全加固规范
DB2安全加固规范
Informix安全加固规范
SQL Server安全加固规范
中间件加固
Tomcat安全加固规范
Nginx安全加固规范
Apache安全加固规范
JBoss安全加固规范
WebLogic安全加固规范
漏洞评分体系
S-SAMM
安全能力成熟度评估
S-SDLC落地实施咨询
S-SDLC云平台
SecZone S-SDLC工具链：
灰盒安全测试工具-VulHunter
XSS深度检测工具-XSSHunter
代码审核平台-CodeSec
应用监控平台-APPCheck
实时自我防护工具-RASP
安全开发库-S-ESAPI
第三方库安全态势感知
威胁库
SecZone 安全商店-SecTool Store：
威胁建模工具- TMT
安全设计工具-SD Elements
代码审核工具-Fortify、Checkmarx
渗透测试工具-Core Impact、CANVAS
数据库扫描工具-NCC SQuirreL
模糊测试工具-Peach Fuzzer
网络扫描工具-SAINT、Nessus
Web扫描工具-N-Stalker X / Trustwave
统一漏洞管理-Core Insight
SAP应用安全检测-ERPScan
流量分析-Allot ClearSee

软件安全开发体系落地

- 企业必须自上而下推行S-SDLC实施，且有相应的组织结构支撑；
- S-SDLC要与企业的质量管理体系相结合；
- 建立合适的人员培训体系；
- 用度量体系将S-SDLC实施效果可视化；
- 产品的安全目标决定S-SDLC的过程；
- 威胁模型可以使产品避免大的设计风险；
- 安全特性组件化可尽量避免编码漏洞；
- 管理第三方软件的风险；
- 安全服务化和自动化是实施DevSecOps的基础；
- S-SDLC工具链。

软件安全人才培养

确认培养目标

软件开发与网络安全的有机融合

- 掌握软件安全意识，了解因不安全开发过程所产生的软件，是导致网络安全事件的技术根本原因；
- 理解软件安全开发的方法论；
- 掌握必要的软件安全专业知识和开发技能。

高校人才培养

人才定位与发展趋势的有机融合

- 国内少数高校已对软件安全的发展和重要性产生意识；
- 多数以软件开发和软件工程专业为主体，融入软件安全的专业知识；
- 但较网络安全专业，更加缺乏具有相当知识与技能水平的讲师和教材。

社会人才培养

行业积淀与社会认知的有机融合

- 国内信息技术行业对软件安全觉醒；
- 总结行业实践，融合国外知识，形成适用于国内的学习材料；
- 线下培训为主，但逐步与互联网教育相结合。

软件安全技术应用

安全检测技术

静态检测

Static Application Security Testing，简称SAST。通常在编码阶段分析应用程序的源代码或二进制文件的语法、结构、过程、接口等来发现程序代码存在的安全漏洞。

动态检测

Dynamic Application Security Testing，简称DAST。DAST是在测试或运行阶段分析应用程序的动态运行状态。通过模拟黑客攻击，收集和判断应用程序做出的反应，从而确定应用程序是否存在缺陷。

交互式应用程序安全测试

Interactive Application Security Testing，简称IAST。是2012年Gartner公司提出的一种新的应用程序安全测试方案，并在2014年被Gartner公布为十大信息安全技术。

SAST技术和DAST技术结合

软件安全技术创新

软件组件分析
自动识别程序代码中开源组件及其安全缺陷。

API安全检测
自动识别程序代码中API风险。

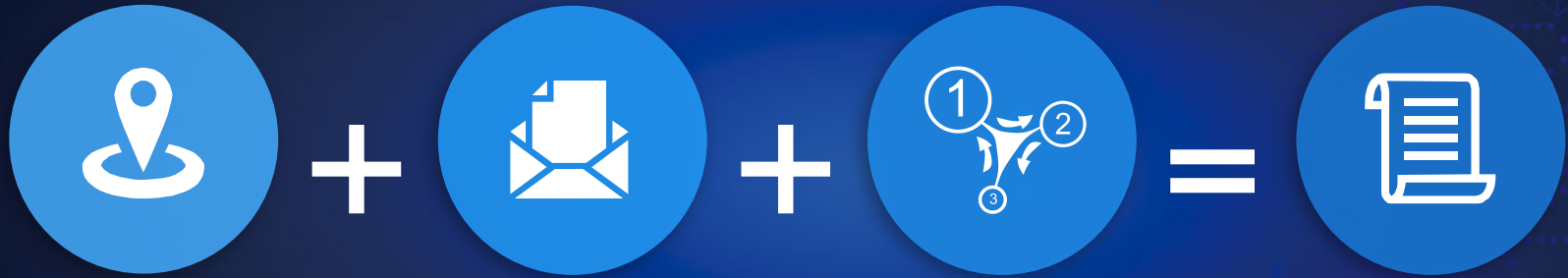
无服务器安全
自动识别和检测应用软件在无服务器环境中的安全风险。

实时响应与保护技术
自动识别并响应应用软件的安全事件。

恶意自动化程序安全检测
针对恶意自动化程序的安全检测和安全防护技术。

IoT安全技术和区块链安全技术

建设软件安全开发体系，是保障国家网络安全的重要基础



软件安全开发
技术应用与创新

软件安全开发
人才培养

软件安全开发
流程实践

从软件诞生的源头
保障国家网络安全

谢 谢

感谢您的聆听

THANK YOU FOR LISTENING

聚力·引领

软件安全学术论坛