華東師範大學
EAST CHINA NORMAL UNIVERSITY

开源合规和许可证

Leo Wang

Leo Wang

- *Shanghai*
- *开源爱好者，Java开发者*

BLACKDUCK

2016

开源之道播客

2020

BLACKDUCK BY SYNOPSYS

Now

1 开源许可证艺术

2 为什么开源合规可信越来越重要？

3 企业开源软件合规治理实践

开源许可证艺术

为什么开源合规可信越来越重要 ？

企业开源软件合规安全治理实践

开源的发展历程-许可证

快速交付 → 可靠软件 → 安全可信软件

BSD	GPL	Linux	ASF	OSI	Android / iPhone	GitHub	RedHat
1970	1984	1991	1995	1998	2007	2017	2018

1950 1960 1970 1980 1990 2000 2010 2020

ENIAC

1946

PDP-8

1965

Lisa

1983

Internet

1995

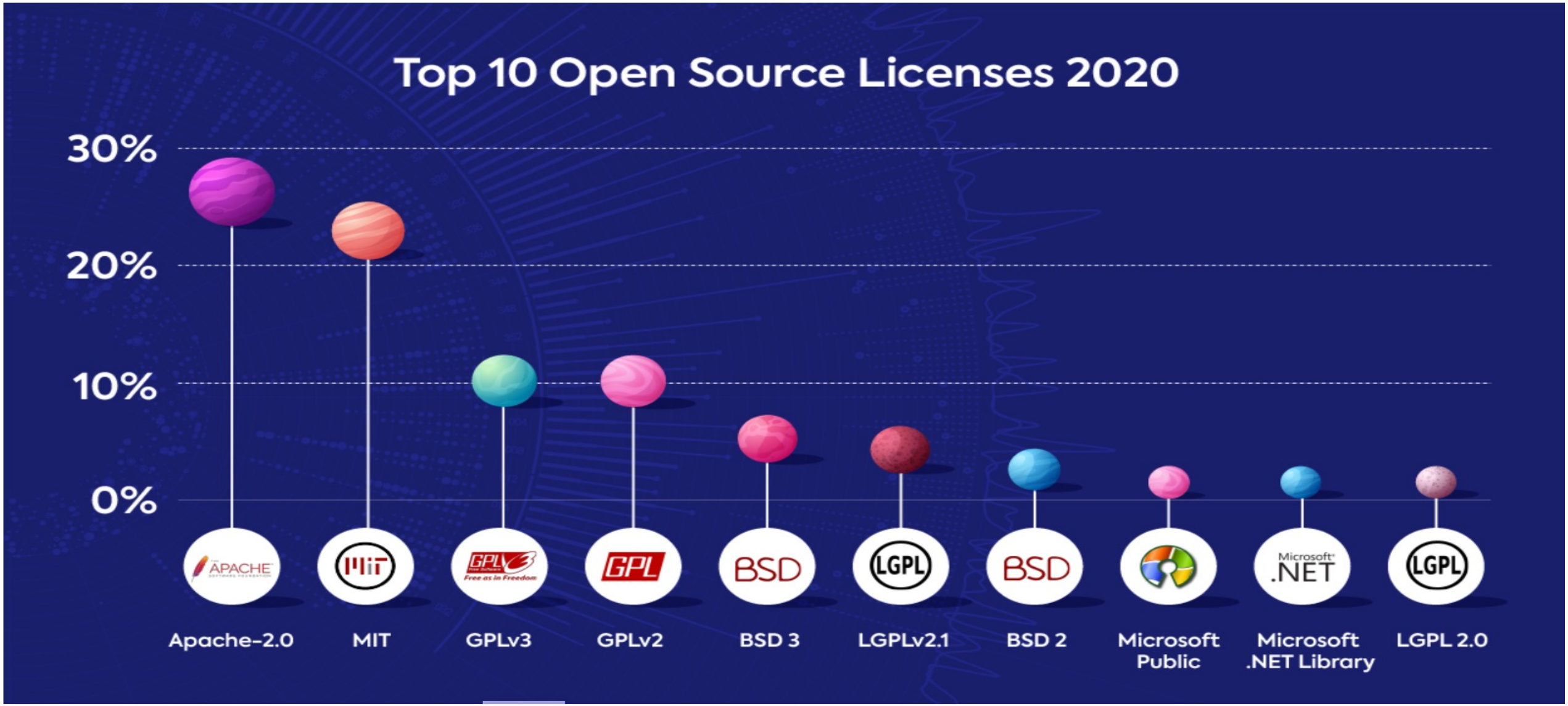
AWS EC2

2006

AI

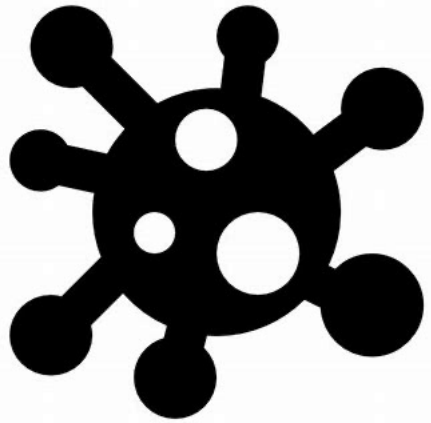
2016

Top 10 Open Source Licenses 2020

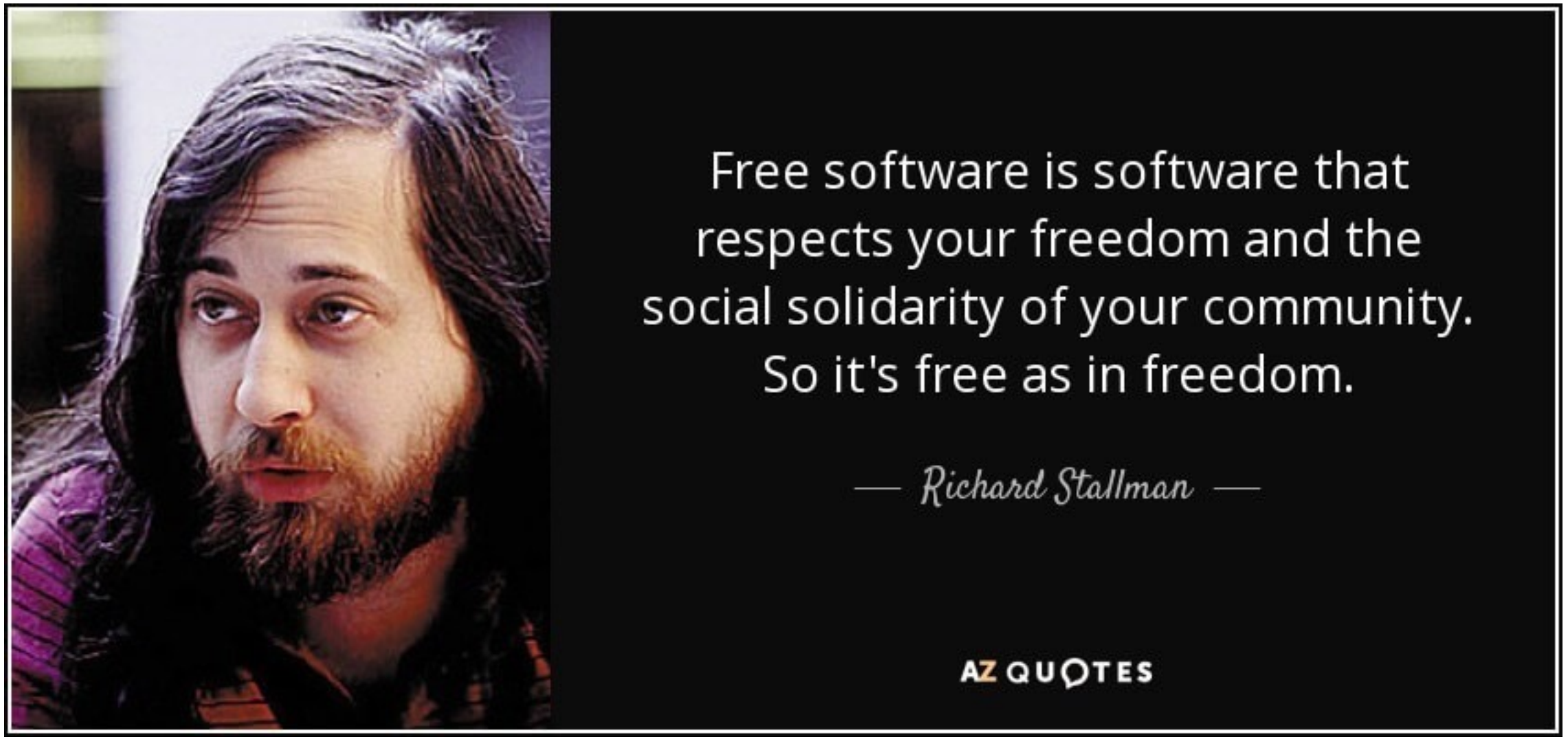


GPL not Virus

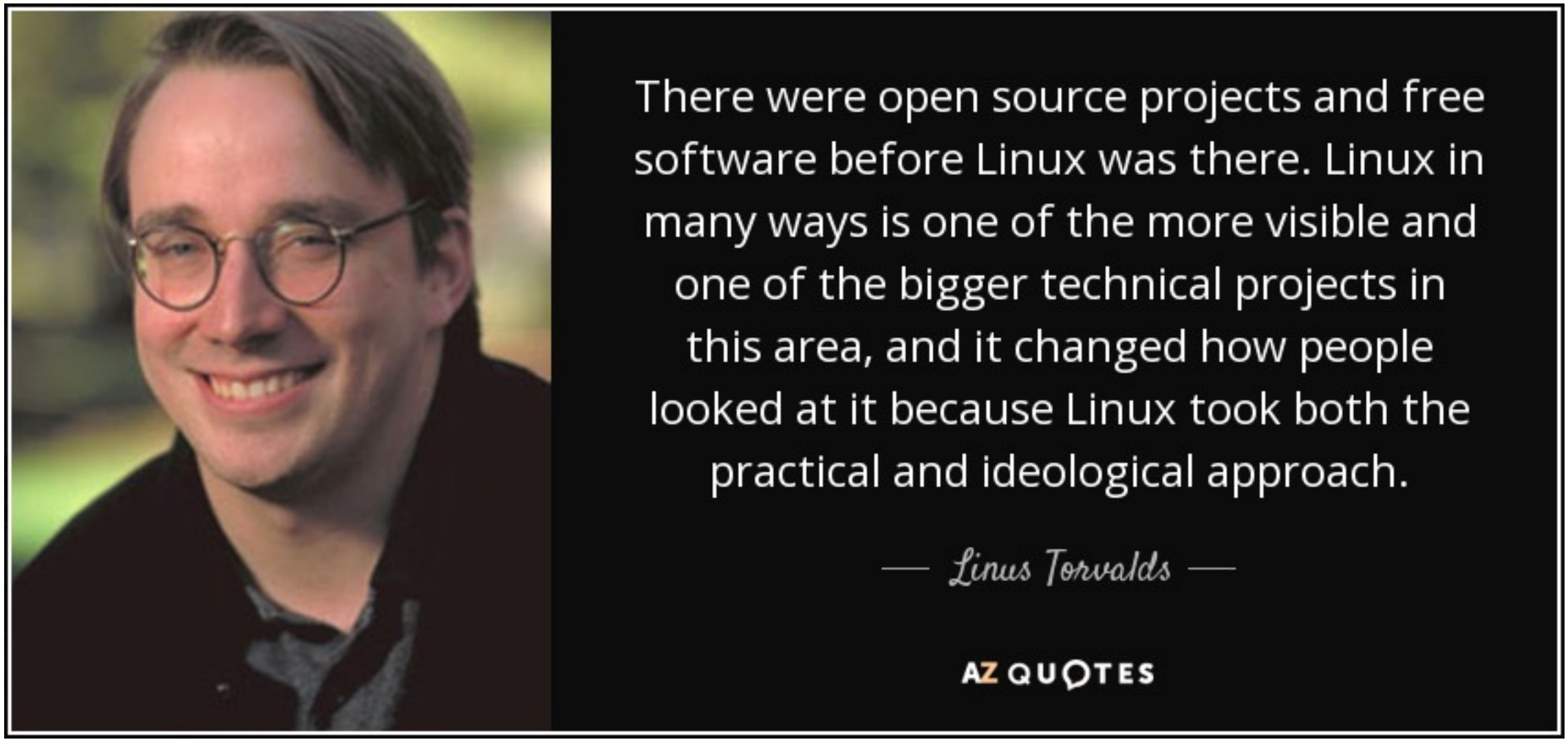
≠



Free as in Freedom-若为自由故



Linux 之父

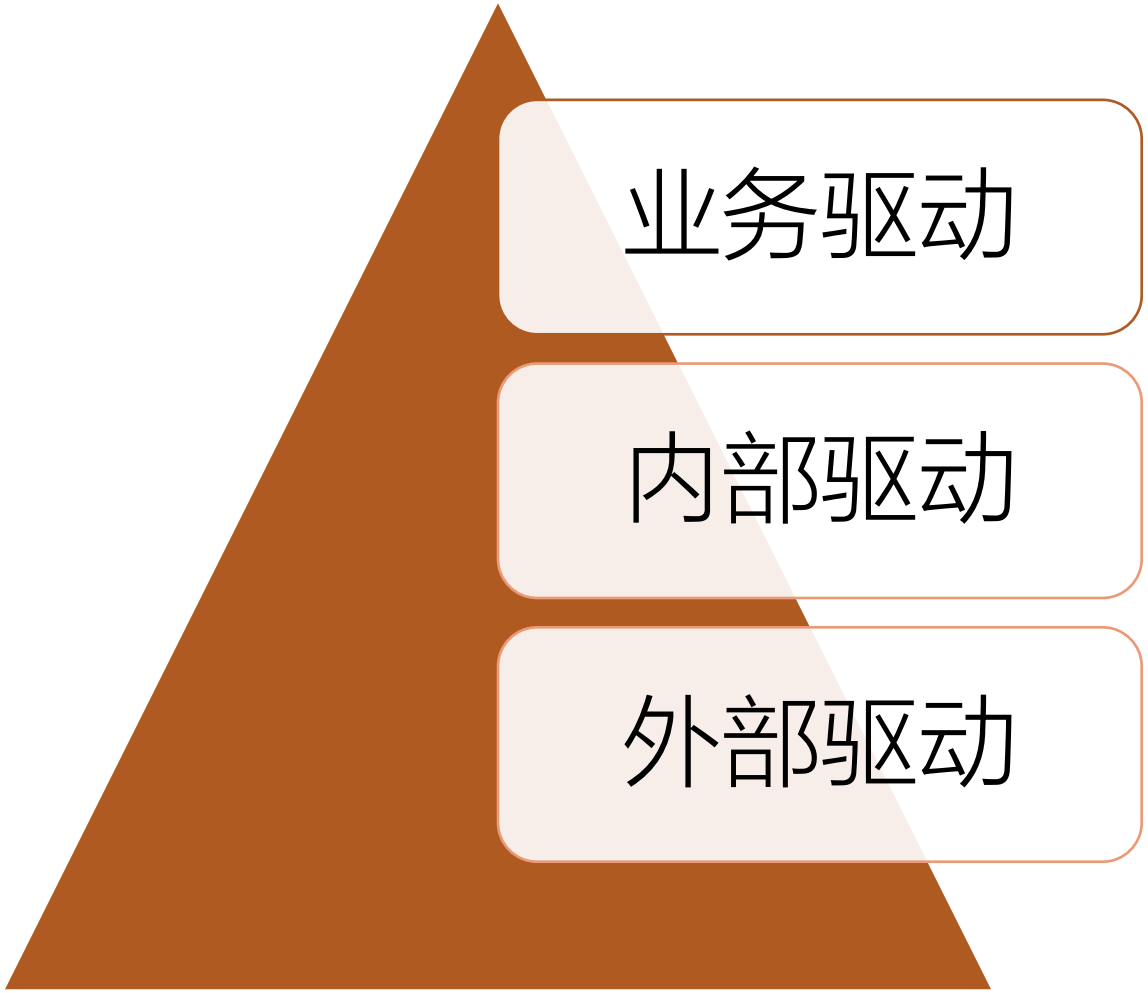

There were open source projects and free software before Linux was there. Linux in many ways is one of the more visible and one of the bigger technical projects in this area, and it changed how people looked at it because Linux took both the practical and ideological approach.
— Linus Torvalds —
AZ QUOTES

开源许可证艺术

为什么开源合规可信越来越重要 ？

企业开源软件合规安全治理实践

为什么需要开源治理



类型	内容
业务驱动	• 推动创新 • 开源生态 • 开源战略 • 商业模式
内部驱动	• 安全左移 • 合规左移 • 开源治理委员会 • **DevSecOps**
外部驱动	• 供应商 • **EAR** • 合规 • 专利保护 • 上市或者收购尽调 • 黑客攻击事件 • 红黑榜 --

开源软件在云计算和大数据时代，已经成为事实的标准 --崔宝秋

开源治理外部驱动-合规

202012: ISO/IEC 5230:2020 开源合规国际标准

https://www.openchainproject.org/

OPENCHAIN

We define effective open source compliance

- Know Your Free and Open Source (FOSS) Responsibilities [i.e., “Policy and Training”]
- Assign Responsibility for Achieving Compliance
- Deliver FOSS Content Documentation and Artifacts
- Review and approve FOSS content
- Understand FOSS Community Engagement
- Certify Adherence to OpenChain Requirements

开源治理外部驱动-EAR合规

https://www.commerce.gov/

美国商务部工业和安全局(BIS)-美国出口管理条例(EAR)合规

美国出口要求

美国软件出口法规来自美国商务部工业和安全局（ BIS ）。 具体规定称为出口管理条例（ EAR ）。 加密的根基是基于国家安全：我们不希望坏人能够入侵我们的加密通信。

这些法规的细节很复杂，属于专家领域。 基本原则是你需要告诉BIS你导出的任何软件中的组件使用的**加密算法**是什么， 该机构对这些要求非常认真，并且已经知道要执行这些要求，特别是2014年Wind River罚款750,000美元（尽管Wind River自愿披露他们自己发现的问题）。

开源治理外部驱动-开源和专利-GPL3.0

https://www.gnu.org/licenses/gpl-faq.html#v3PatentRetaliation

第 11 节：专利

GPLv3 提供以下两项专利承诺：

1.禁止向下游分发对象主张专利权：**GPLv3 §10 明确规定不可施加附加条件来要求被许可方的直接分发对象接受专利许可或支付专利许可费**。此条款制定了有关 GPL 软件专利权用尽的统一规则，不考虑任何特定法律体系或区域法律下的国内专利法。

2.贡献者版本中的专利许可：第 11 节指出，**任何向 GPL 软件贡献代码的人都需要将其中涉及的专利许可授予用户**。此规定旨在防止社区内的成员以激进方式向用户主张自己所修改的代码部分的专利权，即防止社区"内部人员叛变"。如果引入修改代码可导致修改后的软件构成侵犯贡献者专利权，贡献者会将原软件中的专利权许可授予所有后续用户、软件修改人或软件衍生作品的修改人，但不会授予代码修改部分中属于他人的专利权许可。此条款还规定，"贡献者版本"完成后获得的专利权也会在版本获得或完成时授予用户。如果某个拥有众多此类专利权的公司收购或聘用了程序修改者，则根据本条款，收购者已获得和后续获得的专利权也会自动传递。例如，微软公司收购诺基亚后，微软基于诺基亚曾修改的任何 GPLv3 程序的任何贡献者版本当前或以后获得的此类专利权都会自动向下游授予许可。微软收购诺基亚导致 GPLv3 程序的微软专利诉讼量整体下降这一现象至今未在行业内得到充分关注。

开源治理外部驱动-GDPR

Article 25: Data protection by design

- 建立政策支持合规
- 制定控制和政策来管理风险非常重要
- 具有自动化策略执行和集成等功能
- 使安全和法律团队能够支持GDPR合规性
- 防止易受攻击的开源组件进入
- 基于变量的结构政策
- 开发阶段，部署模型，漏洞严重程度，
- 组件版本和发布日期。

Article 32: Security of processing

- 开发和运维的风险管理
- 限制应用程序安全风险的最佳方法是在开发阶段发现和管理开源漏洞
- 通过整合您的风险管理，使用您的开发和操作工具的解决方案
- 团队用来创建，测试和部署您的应用程序持续发现和洞察潜在的风险
- 由开发人员引入并提供操作的组件将他们所需的数据组合在一起以保护生产中的软件

Article 35: Data protection impact assessment

- 生成开源组件清单后，您必须评估您的安全风险态势和分类软件漏洞。虽然公共消息来源像国家漏洞数据库（NVD）提供了高级摘要开源漏洞，影响指标和可利用性，
- 专用安全团队的专有数据源可以提供深入，策划的洞察力和补丁指导。仅在那之后
- 您可以优先考虑您的风险暴露提示采取补救措施，减少你的攻击面。

开源治理外部驱动-IPO,M&A尽调

https://ipo.org/wp-content/uploads/2013/03/opensourcewhitepaper.pdf

- Open source due diligence is a crucial part of your software due diligence. it is a time consuming process because most companies do not have the required visibility into their open source dependency usage.
- Why OSS Diligence for M & A is Important Open Source Software (OSS) licenses1 are ubiquitous in nature and have become a very common way to license software. Given this ubiquitous nature, OSS licenses may impact the valuation of Intellectual Property (IP) transferred during the course of a Merger or Acquisition (M & A) transaction. The classic example of how OSS may impact this valuation is by reducing the value of IP that was otherwise considered to be licensable under a proprietary license, but for its licensing under an OSS license. For the purpose of this whitepaper, we will be discussing the impact of the GNU General Public License (GPL)2 on M & A transactions, and specifically the provision3 A. A Hypothetical of GPL that allows for the automatic licensing of downstream recipients of copyrighted technology licensed under GPL

名声很重要

开源治理外部驱动-开源红黑榜

Software Licensing Violations: Non-profit to B2B

Software Freedom Law Center

- Cisco
- Verizon
- Monsoon Multimedia
- Xterasys
- High-Gain Antennas
- Bell Microproducts
- Super Micro Computer
- Westinghouse Digital

gpl-violations.org

- Sitecom
- Fortinet
- Motorola
- Acer
- Skype
- D-Link
- BT
- Fantec

Others

- Jacobsen v Katzer
- ASUS PC laptop
- Diebold
- Oracle v Google
- Twin Peaks v Red Hat
- Versata/Ameriprise/XimpleWare
- Hellwig v. Vmware
- McHardy v. Everyone
- Wix and Wordpress
- Artifex v. Hancom
- Co-Kinetic Systems v. Panasonic Avionics

Infringement
Valuation
Negative publicity
Revenue Loss / Injunctions
Support costs

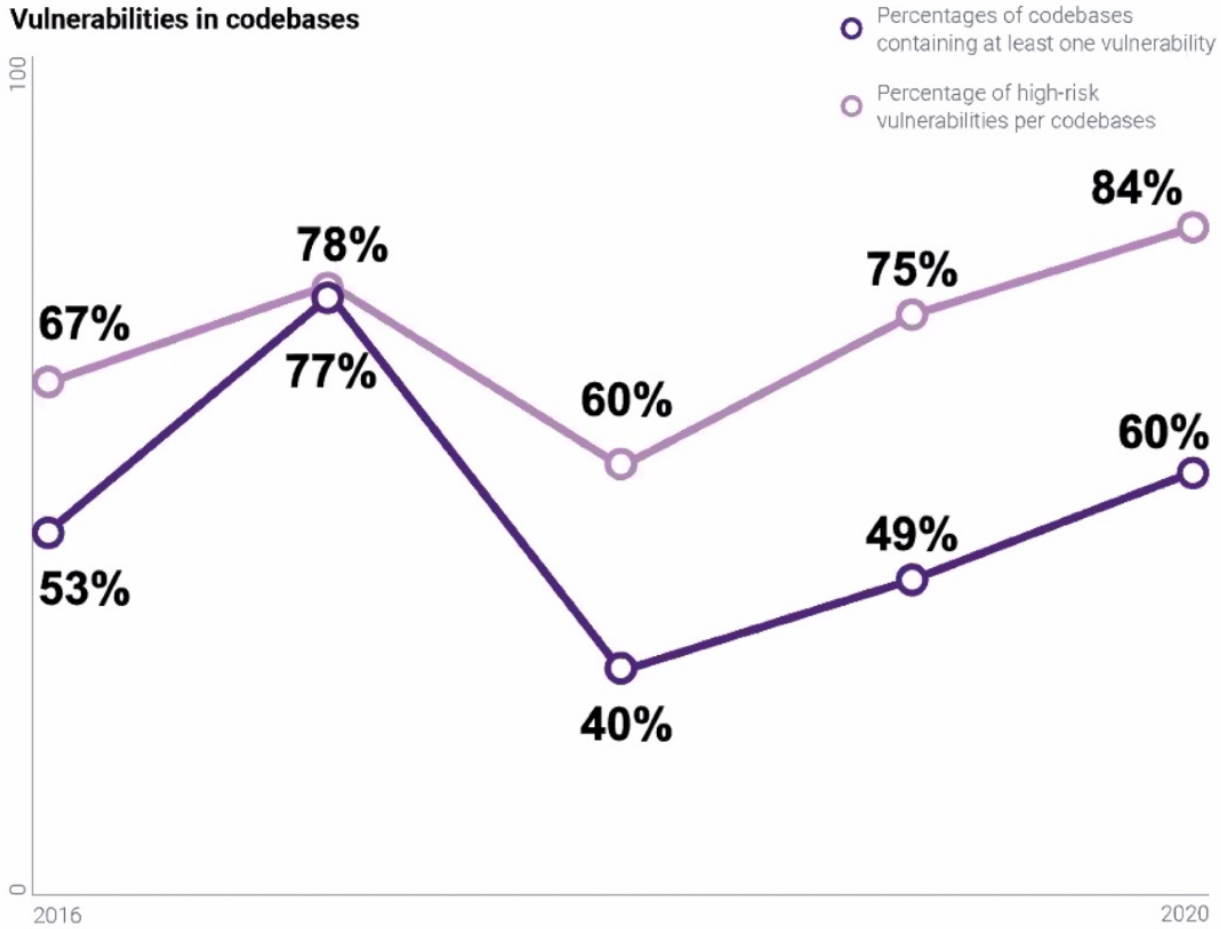
Who is Next?

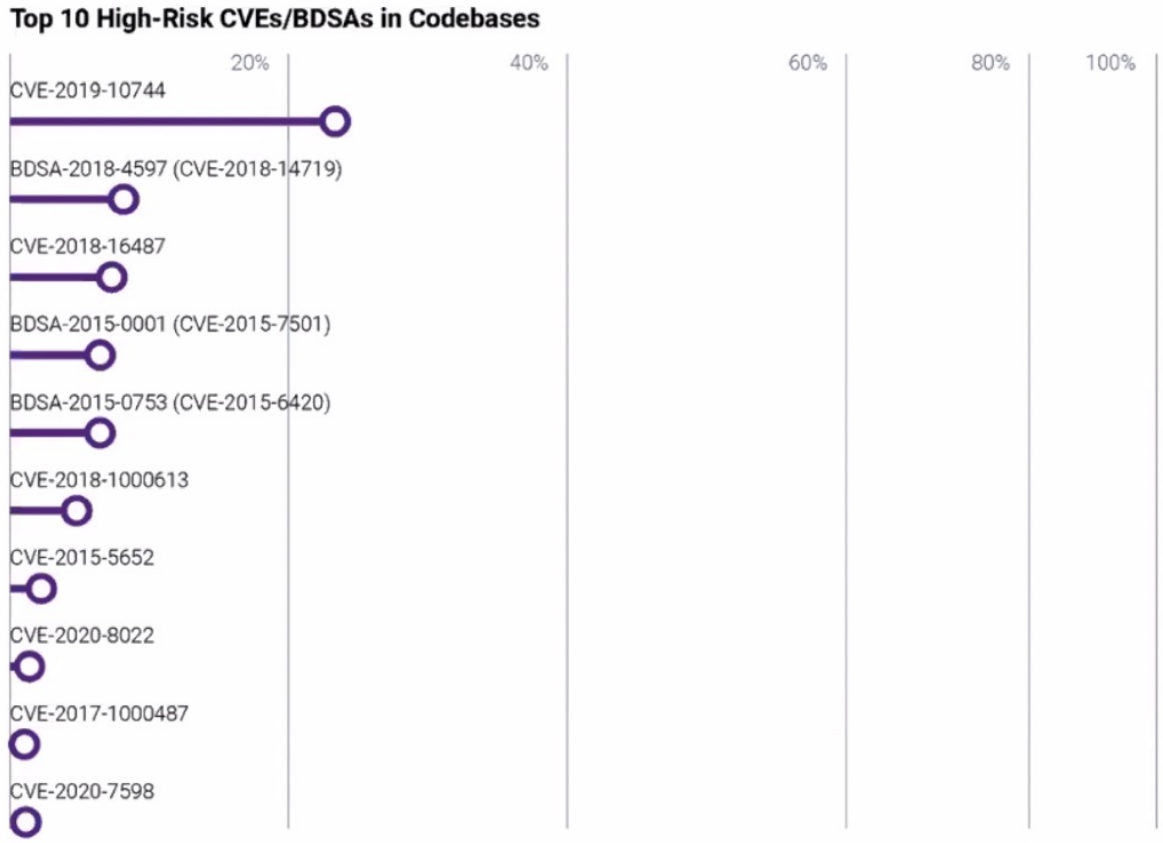
开源许可证艺术

为什么开源合规可信越来越重要 ？

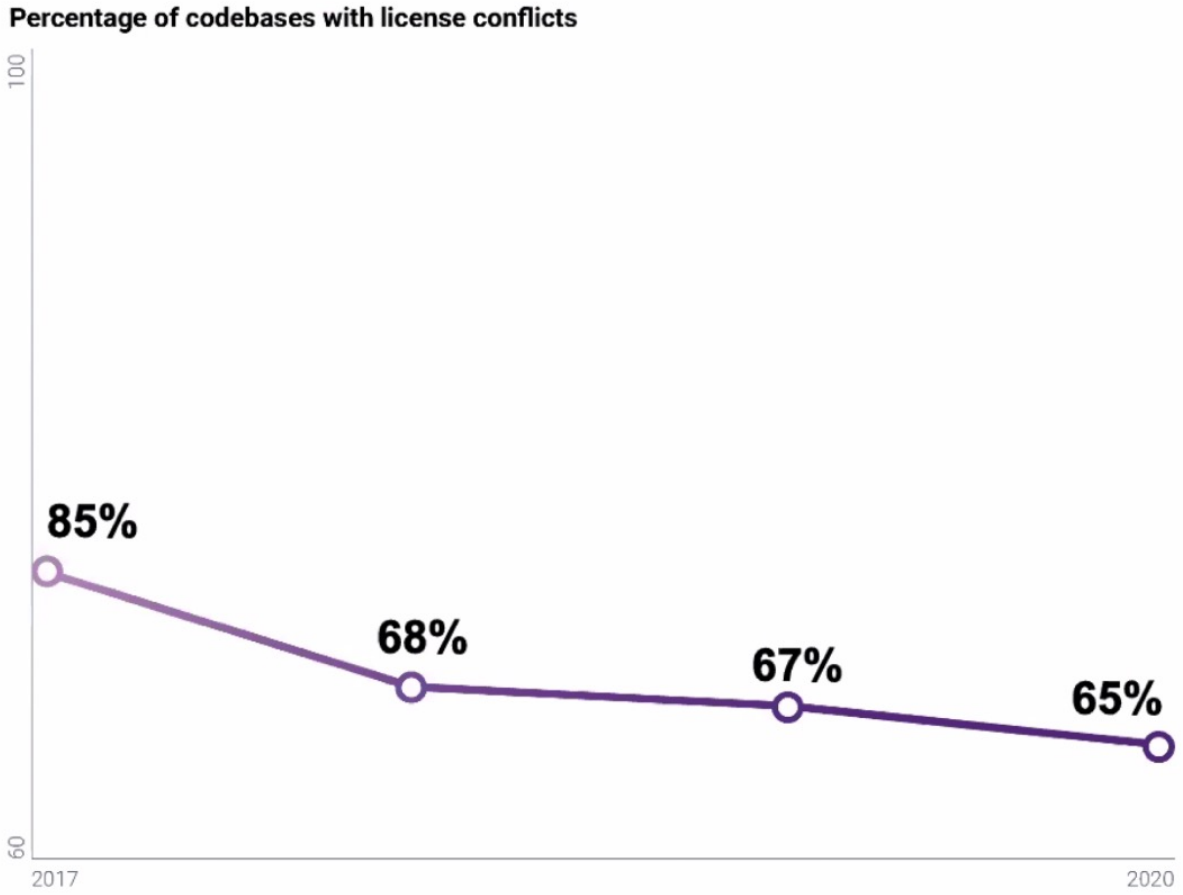
企业开源软件合规安全治理实践

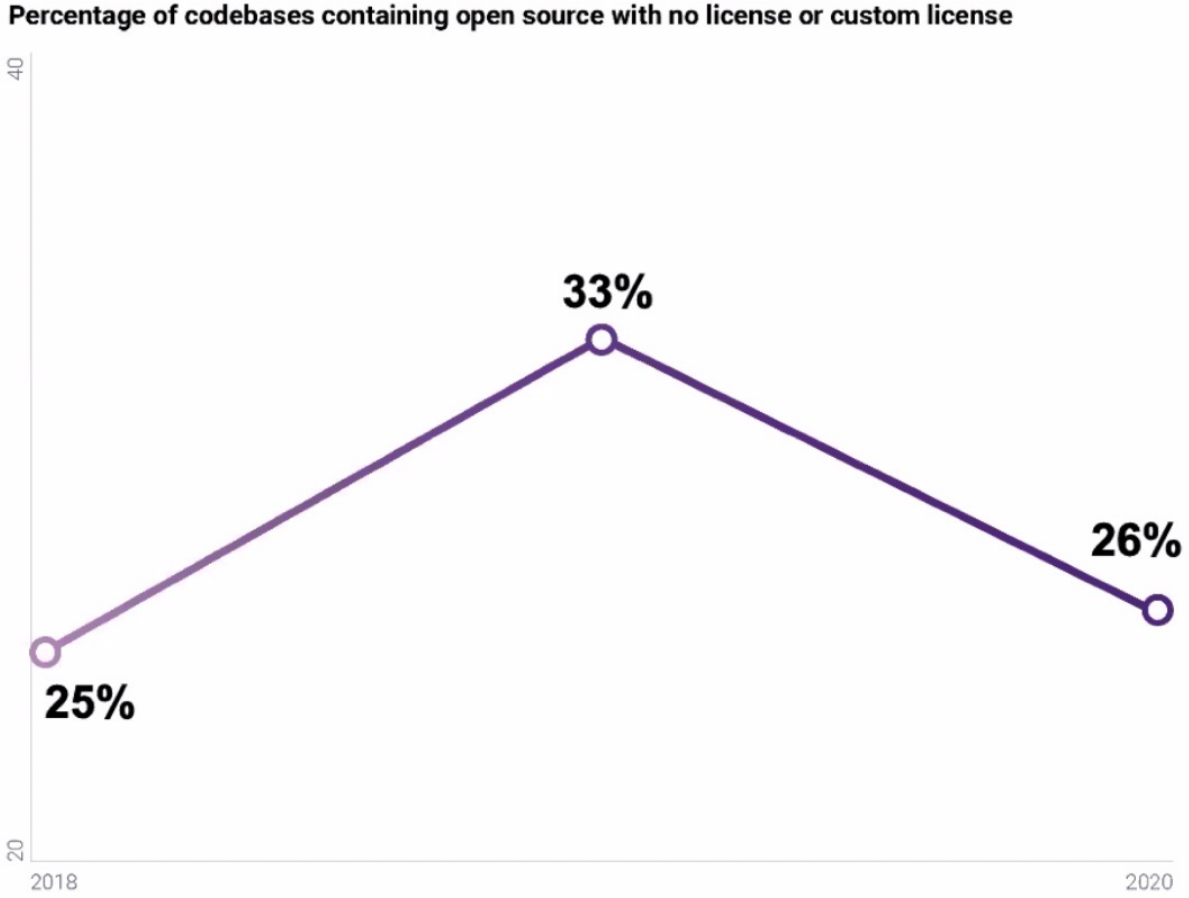
漏洞比例与日俱增


Vulnerabilities in codebases
Percentages of codebases containing at least one vulnerability
Percentage of high-risk vulnerabilities per codebases
100
0
2016
2020
67%
78%
60%
75%
84%
53%
77%
40%
49%
60%


Top 10 High-Risk CVEs/BDSAs in Codebases
20%
40%
60%
80%
100%
CVE-2019-10744
BDSA-2018-4597 (CVE-2018-14719)
CVE-2018-16487
BDSA-2015-0001 (CVE-2015-7501)
BDSA-2015-0753 (CVE-2015-6420)
CVE-2018-1000613
CVE-2015-5652
CVE-2020-8022
CVE-2017-1000487
CVE-2020-7598

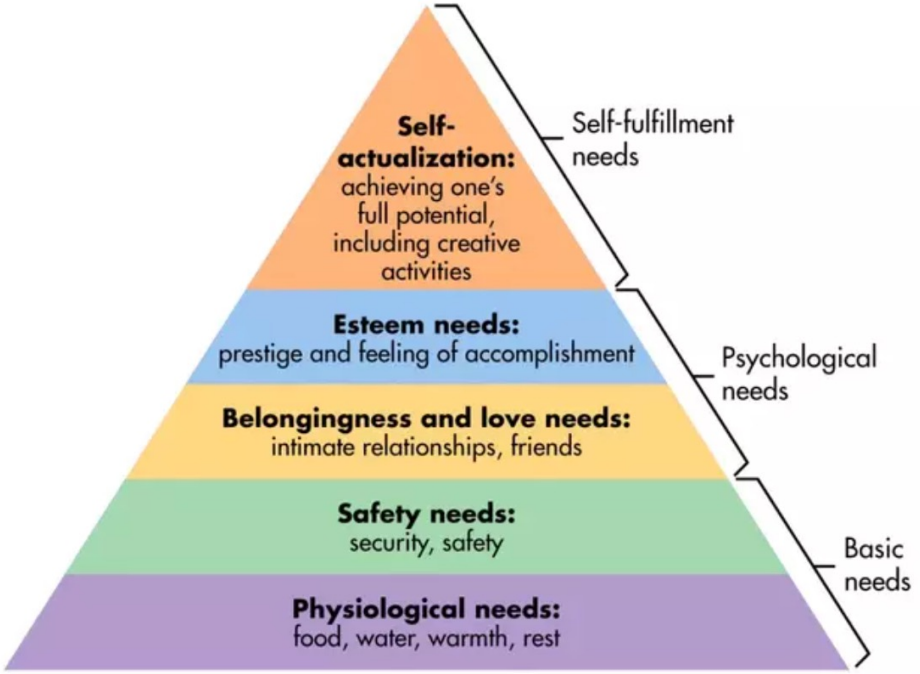
合规风险不容乐观


Percentage of codebases with license conflicts
100
60
85%
68%
67%
65%
2017
2020


Percentage of codebases containing open source with no license or custom license
40
20
25%
33%
26%
2018
2020

谈一谈最佳实践

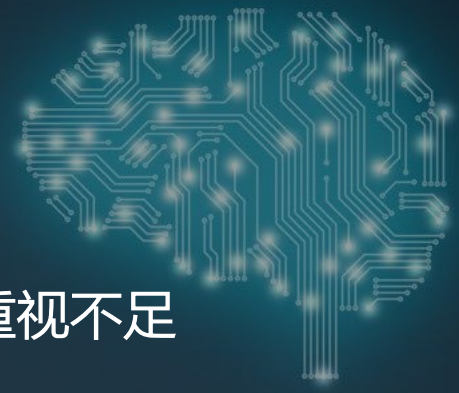
- **Best Practices is nothing but is really depend on you feeling**
- **Quick and adopt the solution from 0 to 1**
- **Best Practices is not the end just starting the journey**
- **Respect, Open Mind and Gratitude**
- **Coummunication , Coummunication, Coummunication**



Customer foucs is the Best practices is the right postural!

企业使用开源面临的常见挑战

- 开源组件缺乏透明度
- 对开源使用风险认识有限
- 缺乏开源治理政策和框架
- 管理层重视不足
- 与开源社区缺乏互动，运维困难
- 企业内部缺乏沟通，各自管理、评估



衡量开源安全可信的8个维度

#	维度	活动		
1	发现	实施带有预审许可证的开源目录	针对何为可接受的开源组件提供指导	
2	审查和选择	实施开源审批流程，以洞悉法律、架构和安全风险		
3	供应链	制定供应商的安全治理审计计划	将软件供应商的开源使用事宜写进合同	
4	代码管理	设置开源组件持续扫描和监控流程，以识别出安全、许可证和运营风险	针对开源制定编码文档记录标准	
5	维护与支持	利用工具或订阅服务来监视新版本、更新或风险	跨域或域内的集中支持和维护将能防止和减少重复性支持活动	
6	合规管理	创建合规管理流程以在开发早期阶段洞悉合规义务和风险	在软件开发生命周期(SDLC)过程中设置正式的门限，以便对许可证合规性进行验证	将法务部门审查纳入到合规验证流程中，确保使用开源许可证的项目履行适当的义务
7	社区互动	制定正式指南，指导员工参与开源社区交流	设立社区贡献监督流程	建立内部开源社区，拥抱开源
8	高管监督	高管参与开源管理流程和政策的制定	结合开源使用情况和合规状态指标，提供月度管理报告	

开源成熟度等级

VALUE TO BUSINESS

	1 Reactive	2 Enabled	3 Participating	4 Driving
Characteristics	• No defined governance for open source • Individual or teams assess their own needs across capabilities • Varying repeated efforts	• Basic policy and governance process specified • Divisions or Business units assess and manage Open Source capabilities • Some organizational awareness of risks associated with using source	• Executive level sponsorship • Standardized process and policy enforcement across division or business units • Organization wide visibility and risk awareness • Awareness of Supply Chain Risk	• Maximizing Value • Business Alignment • Open Source Innovation • Active Involvement and Investment in open source communities
Focus	• Personal preferences when it comes to open source activities • Individuals or teams self support themselves • Small / Medium scale open source usage	• Basic governance • Medium scale open source usage • Education • Existence of basic internal support and structures	• Large scale open source usage with inventory and catalogue • Risk assessment and minimization • Semi automated processes that are consistent • Minimizing duplication of effort	• Competitive advantage & Business metrics • Automated, integrated processes • Involvement in the communities • Transformative Business Strategies • Strategic OSS Investments

Strategic

Operational

CAPABILITY

Basic

Advanced

企业治理实践

开源治理审查委员会（ OSRB ）

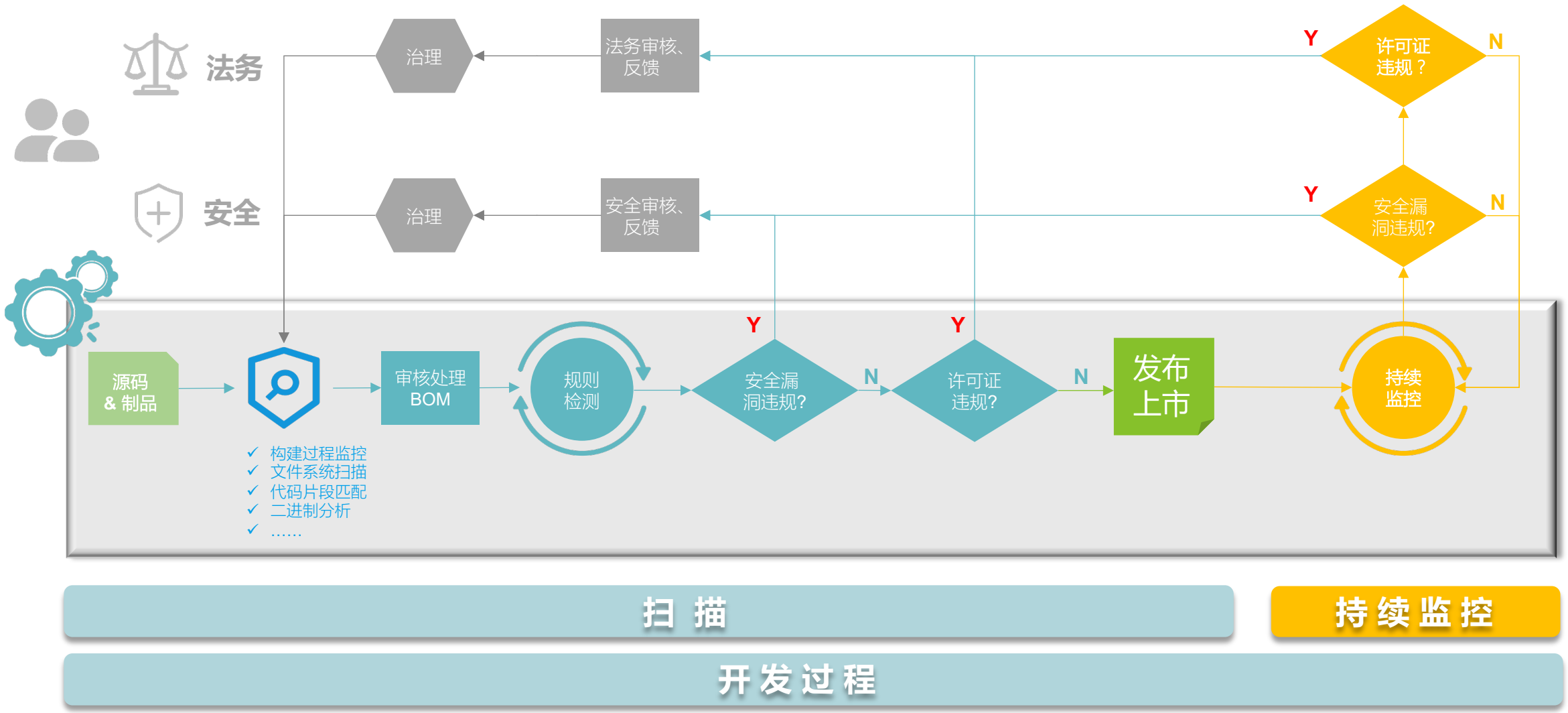
制定、管理企业的开源政策

批准开源软件的修改、分发

Strategic

Operational

企业治理实践 – [轻量级] 解决方案



企业治理实践 – [中长期] 解决方案

合规

- 自动生成Notice file
- 动态自动识别许可证风险
- 可定义的许可证类型
- 基于组件的加密算法信息，协助完成ECCN报告

安全

- BDSA安全漏洞修复建议
- 0 Day 安全漏洞告警
- CVSS2.0/CVSS3.0
- 漏洞的验证脚本信息

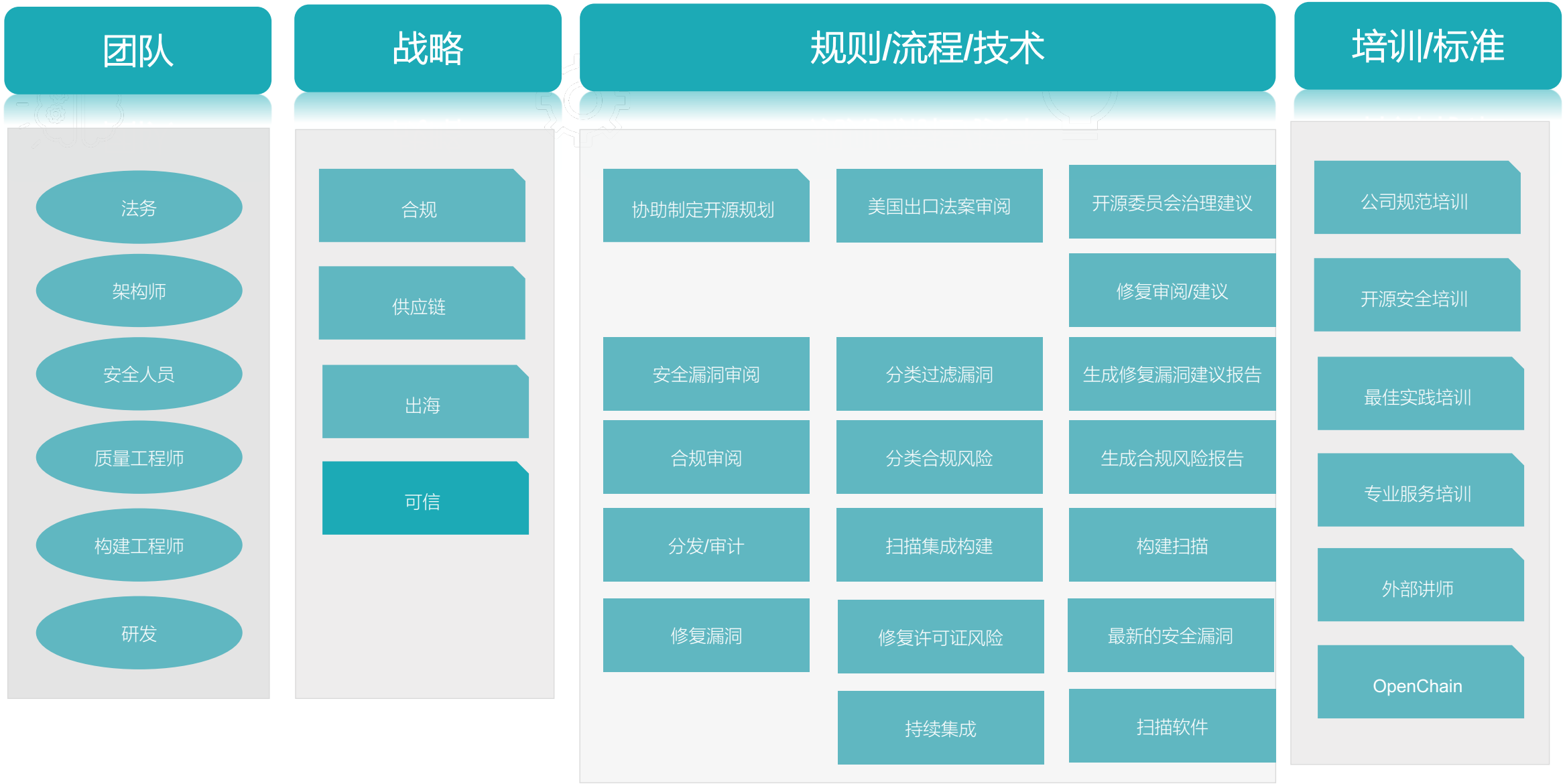
管理

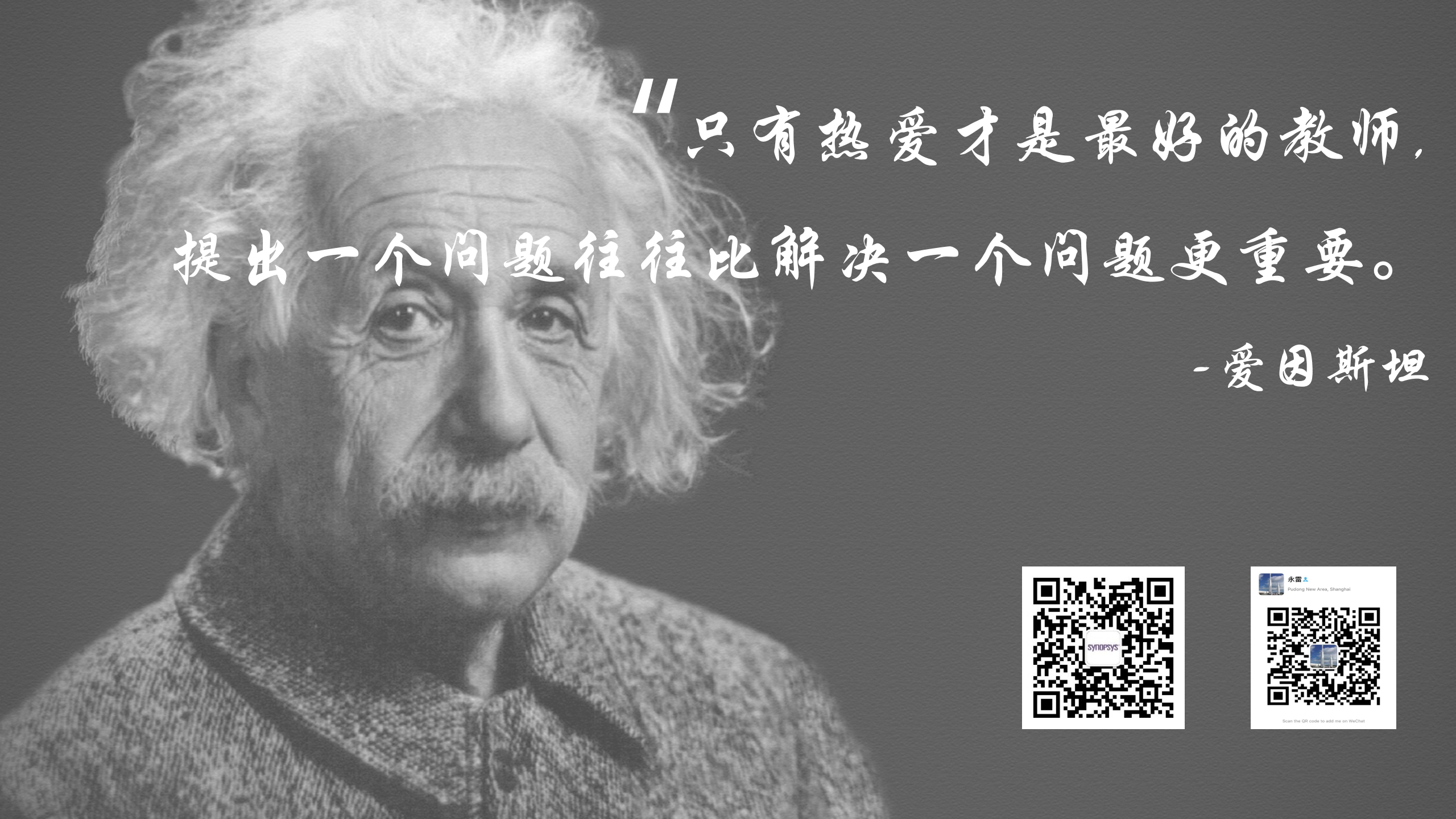
- 自定义规则集合
- 自动以白名单/黑名单
- 自定义开源组件
- Clone项目

方案

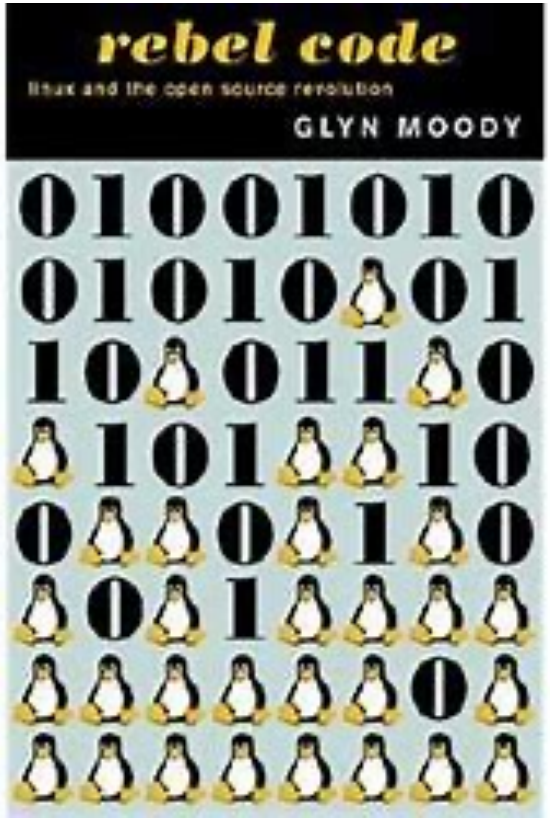
- 高可扩展，高可用
- 灾备
- 负载均衡

案例开源治理框架


团队
法务
架构师
安全人员
质量工程师
构建工程师
研发
战略
合规
供应链
出海
可信
规则/流程/技术
协助制定开源规划
美国出口法案审阅
开源委员会治理建议
修复审阅/建议
安全漏洞审阅
分类过滤漏洞
生成修复漏洞建议报告
合规审阅
分类合规风险
生成合规风险报告
分发/审计
扫描集成构建
构建扫描
修复漏洞
修复许可证风险
最新的安全漏洞
持续集成
扫描软件
培训/标准
公司规范培训
开源安全培训
最佳实践培训
专业服务培训
外部讲师
OpenChain


"只有热爱才是最好的教师，
提出一个问题往往比解决一个问题更重要。
-爱因斯坦
synopsys
永雷
Pudong New Area, Shanghai
Scan the QR code to add me on WeChat

Rebel Code



历史在机缘巧合中缓缓而来，计算机的前辈们在代码的革命中追寻着自己的脚步，这个一部波澜壮阔的历史，也是值得我们去细细评味的历史

--Leo

shopen 上海开源信息技术协会
SHANGHAI OPENSOURCE INFORMATION TECHNOLOGY ASSOCIATION