CAICT 中国信通院　中国通信标准化协会 China Communications Standards Association

软件供应链安全思考与实践

主讲人：奇安信代码安全事业部 屈银

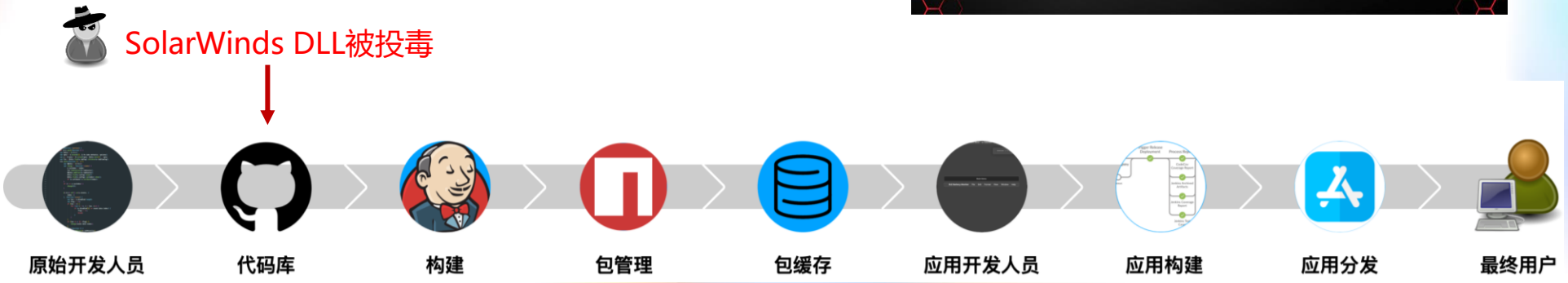
2021 可信云大会
2021 TRUSTED CLOUD SUMMIT
数字裂变　可信发展

演讲目录

一、背景情况

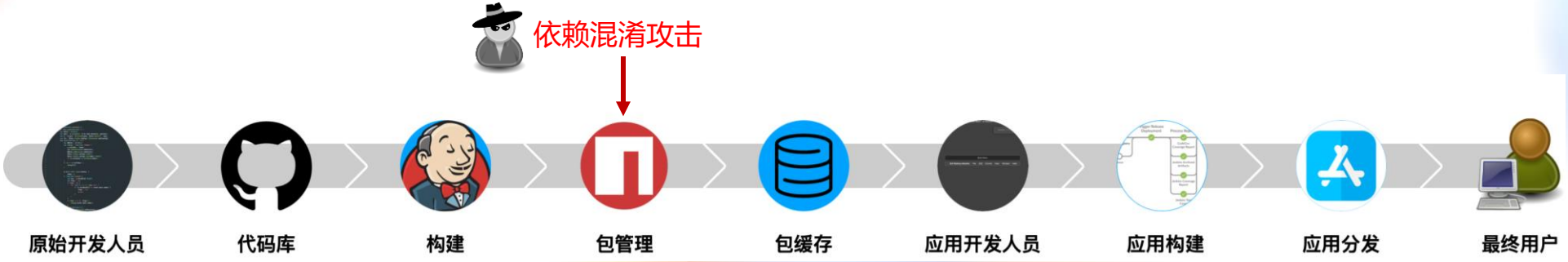
事件：SolarWinds攻击

2020年12月13日，全球最著名的网络安全管理软件供应商SolarWinds遭遇国家级APT团伙高度复杂的供应链攻击并植入木马后门。该攻击直接导致包括美国关键基础设施、军队、政府在内的18000+企业客户受到影响：可任由攻击者完全操控



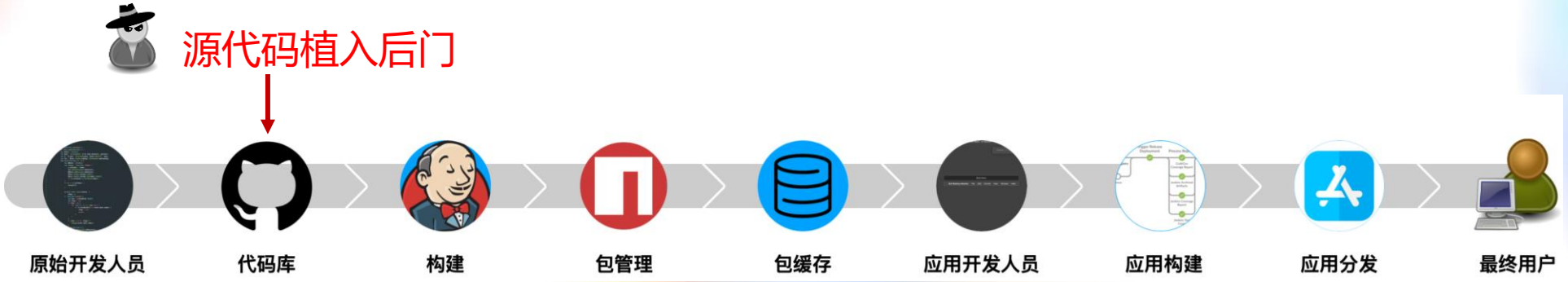
事件：35家国际大型科技公司被供应链攻击攻破

- 2021年2月，一名安全研究员通过一种新颖的软件供应链攻击方式--依赖混淆攻击，成功侵入了微软、苹果、PayPal、特斯拉、优步等35家国际大型科技公司的内网
- 开源生态的设计缺陷，给攻击者以可乘之机
  - 包管理器自动管理
  - 公有软件包优先私有软件包
  - 版本高的软件包优先版本低的软件包
  - ……
- 随后的数周内，NPM和 PyPi开源代码仓库涌入了超过五千个模仿此攻击方式的概念验证攻击包！

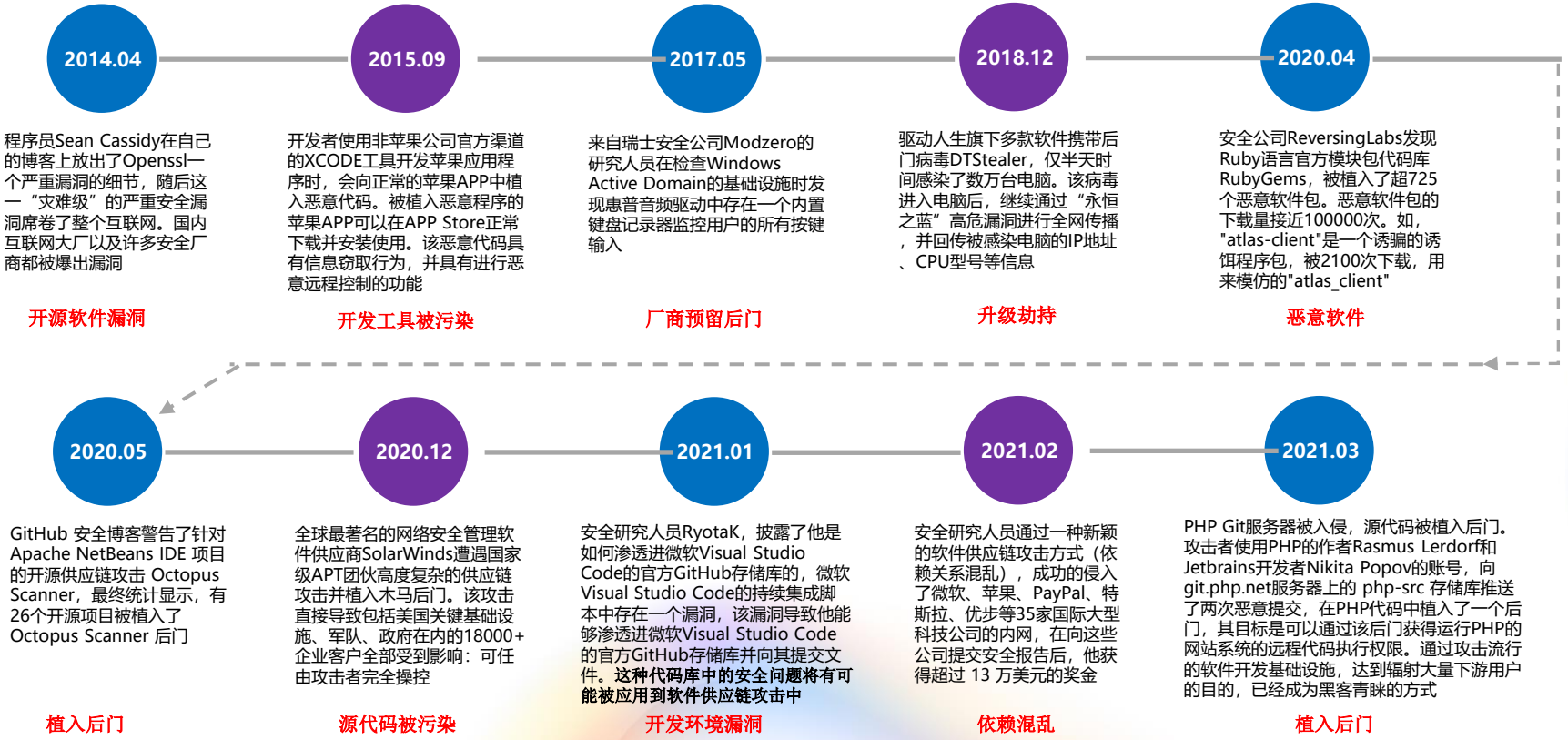


事件：PHP Git服务器被入侵，源代码被植入后门

- 2021年3月28日，攻击者使用PHP的作者Rasmus Lerdorf和Jetbrains开发者Nikita Popov的账号，向git.php.net服务器上的php-src 存储库推送了两次恶意提交，在PHP代码中植入了一个后门，其目标是可以通过该后门获得运行PHP的网站系统的远程代码执行权限。
- 作为此次事件后的预防措施，PHP 团队弃用官方 Git 服务器，PHP 代码库迁移到 GitHub
- 通过攻击流行的软件开发基础设施，达到辐射大量下游用户的目的，已经成为黑客青睐的方式。因软件供应链的复杂性，这种攻击常常难以发现和防范



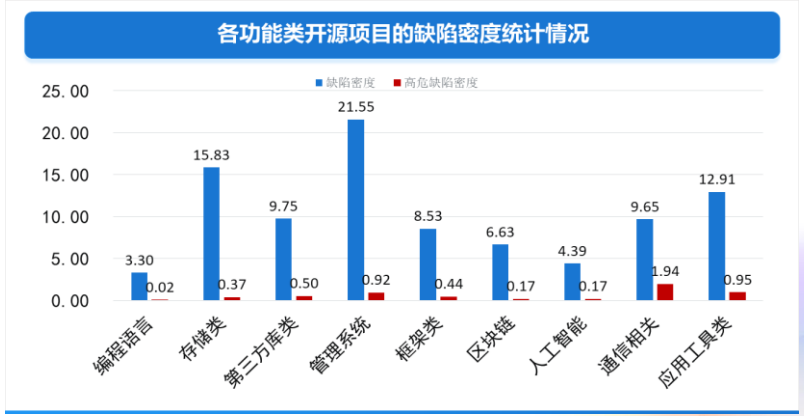
软件供应链攻击事件频发

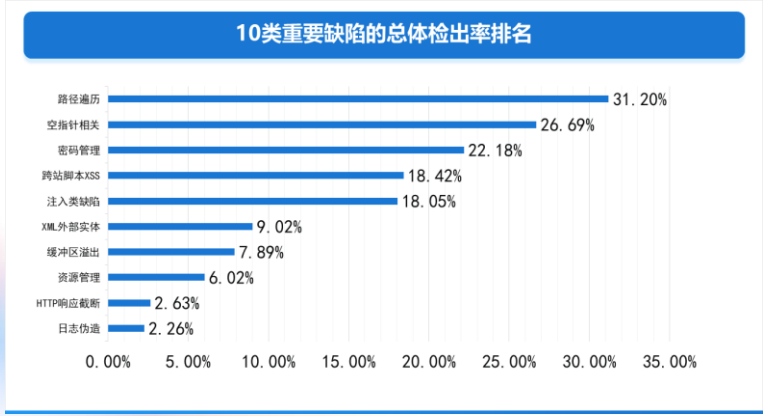


二、软件供应链安全实践

实践一：开源检测计划--开源软件自身安全状况堪忧

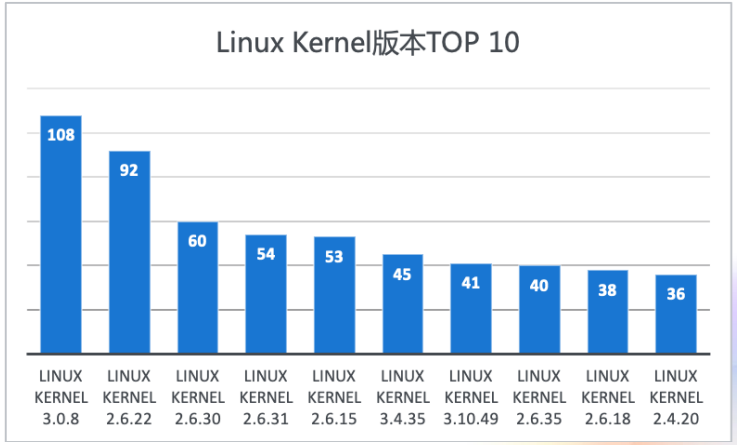
- 开源软件是软件开发最基础的原材料，位于软件供应链的源头，其自身的安全状况，直接影响最终软件的安全性。
- 2015年初，我司基于奇安信代码卫士产品和自身漏洞研究能力，发起了 “奇安信开源项目检测计划”，该计划目前已检测3000余款开源项目，积累了大量的开源软件安全缺陷基础数据
- 开源项目检测计划统计数据：
  - 缺陷密度：14.22个/千行，高危缺陷密度：0.72个/千行

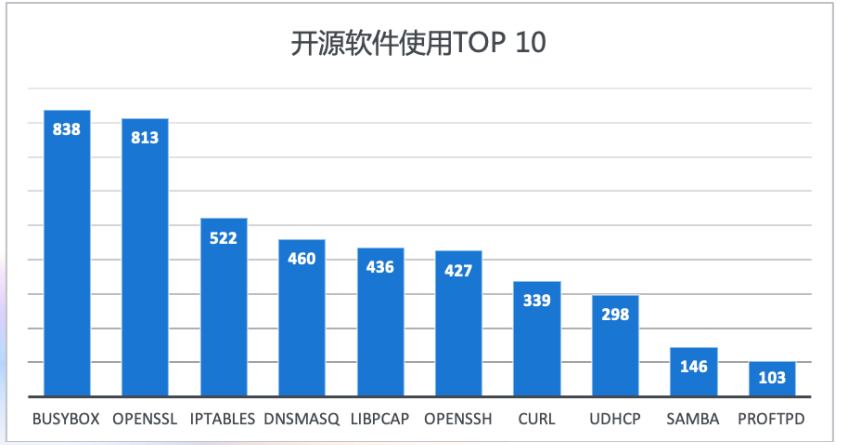




实践二：固件检测计划--联网设备供应链安全问题严重

- 基于奇安信固件卫士能力，2019年初奇安信发起固件安全检测计划，针对联网设备固件中引用的开源软件及其漏洞进行分析。选取了13个厂商935个设备的最新版固件进行分析（以无线路由器、智能摄像头等可公开获得固件的设备为主）
  - 89.6%基于Linux开源生态
  - 使用的开源软件版本五花八门，Linux内核版本50个，版本最多的开源软件是Openssl，存在77个版本

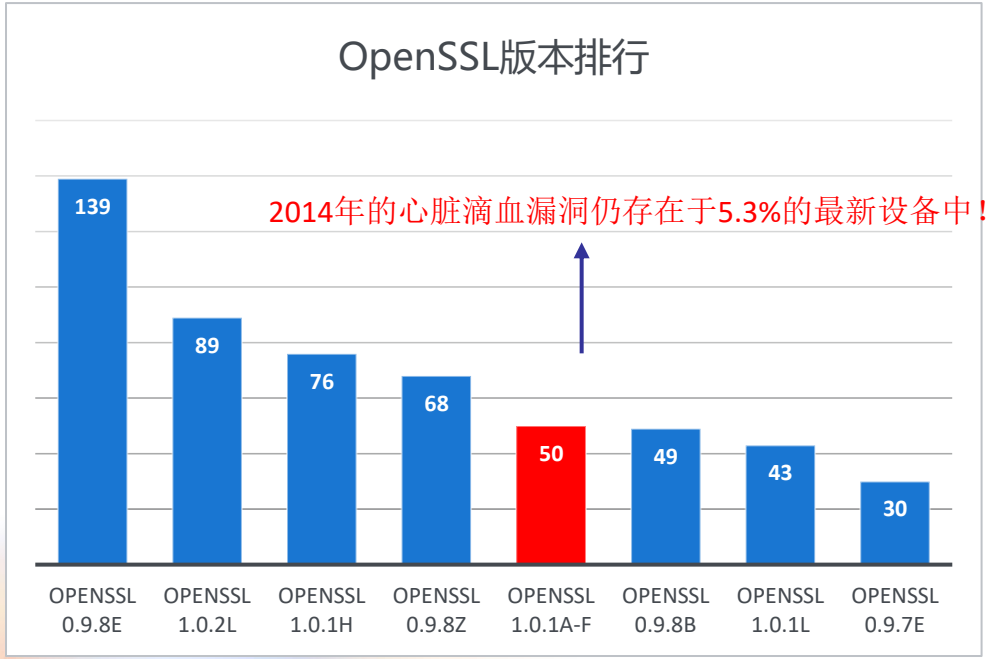




实践二：固件检测计划--联网设备供应链安全问题严重

- 86.4%的设备的最新固件存在至少一个老旧开源软件漏洞
- 漏洞最多的固件存在74个老旧开源软件漏洞

开源软件	CVE漏洞数	漏洞影响固件数	固件总数
OpenSSL	200	745	813
OpenSSH	92	291	427
curl	63	235	339
Dnsmasq	13	294	460
BusyBox	12	808	838



实践三：企业软件开发调研--广泛使用开源软件且混乱

使用奇安信开源卫士分析了2188个企业软件开发项目

具体分析内容：

1、开发中有否使用开源软件，使用了哪些开源软件？

2、使用的开源软件有没有漏洞？

实践三：企业软件开发调研--广泛使用开源软件且混乱

- 100%使用开源软件
  - 2188个项目均使用了开源软件，无一例外
  - 使用的开源软件数量，最多的项目使用了2104个，最少的1个，平均135个
  - 被使用最多的开源软件出现在581个项目中

使用开源软件最多的项目 TOP 5

项目	使用的开源软件数量
项目1	2104
项目2	2035
项目3	1969
项目4	1944
项目5	1908

被使用最多的开源软件 TOP 5

开源软件名称	被使用的项目数量
Apache Commons Collections	581
Apache Commons Lang	573
Java Servlet API	489
Commons Logging : Commons Logging	483
Simple Logging Facade for Java (SLF4J)	479

实践三：企业软件开发调研--广泛使用开源软件且混乱

- 2188个项目中，被检测出114862个开源软件漏洞（涉及2123个唯一CVE编号）
  - 平均每个项目存在52.5个开源软件漏洞
  - 漏洞最多的项目存在415个开源软件漏洞
  - 影响面最大的开源软件漏洞出现在973个项目中

漏洞最多的项目 TOP 5

项目	存在的开源软件漏洞数量
项目1	415
项目2	395
项目3	380
项目4	373
项目5	357

影响面最大的开源软件漏洞 TOP 5

漏洞名称	CVE编号	影响的项目数量
Spring Framework 安全漏洞	CVE-2020-5421	973
FasterXML Jackson Databind 代码问题漏洞	CVE-2020-25649	850
Google Guava 访问控制错误漏洞	CVE-2020-8908	839
Apache Log4j 信任管理问题漏洞	CVE-2020-9488	783
FasterXML jackson-databind 代码问题漏洞	CVE-2020-8840	751

实践三：企业软件开发调研--广泛使用开源软件且混乱

- 2188个项目中，被检测出114862个开源软件漏洞（涉及2123个唯一CVE编号）
  - 平均每个项目存在52.5个开源软件漏洞
  - 漏洞最多的项目存在415个开源软件漏洞
  - 影响面最大的开源软件漏洞出现在973个项目中

漏洞最多的项目 TOP 5

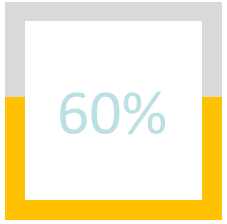
项目	存在的开源软件漏洞数量
项目1	415
项目2	395
项目3	380
项目4	373
项目5	357

影响面最大的开源软件漏洞 TOP 5

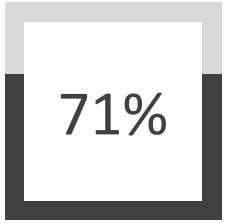
漏洞名称	CVE编号	影响的项目数量
Spring Framework 安全漏洞	CVE-2020-5421	973
FasterXML Jackson Databind 代码问题漏洞	CVE-2020-25649	850
Google Guava 访问控制错误漏洞	CVE-2020-8908	839
Apache Log4j 信任管理问题漏洞	CVE-2020-9488	783
FasterXML jackson-databind 代码问题漏洞	CVE-2020-8840	751

实践三：企业软件开发调研--广泛使用开源软件且混乱

- 2188个项目中，存在开源软件漏洞的项目1695个，占比77.5%
  - 存在超危漏洞的项目1319个，占比60.3%
  - 存在高危漏洞的项目1559个，占比71.3%



1319个项目存在
超危开源软件漏洞



1559个项目存在高
危开源软件漏洞

1695个项目存
在开源软件漏洞

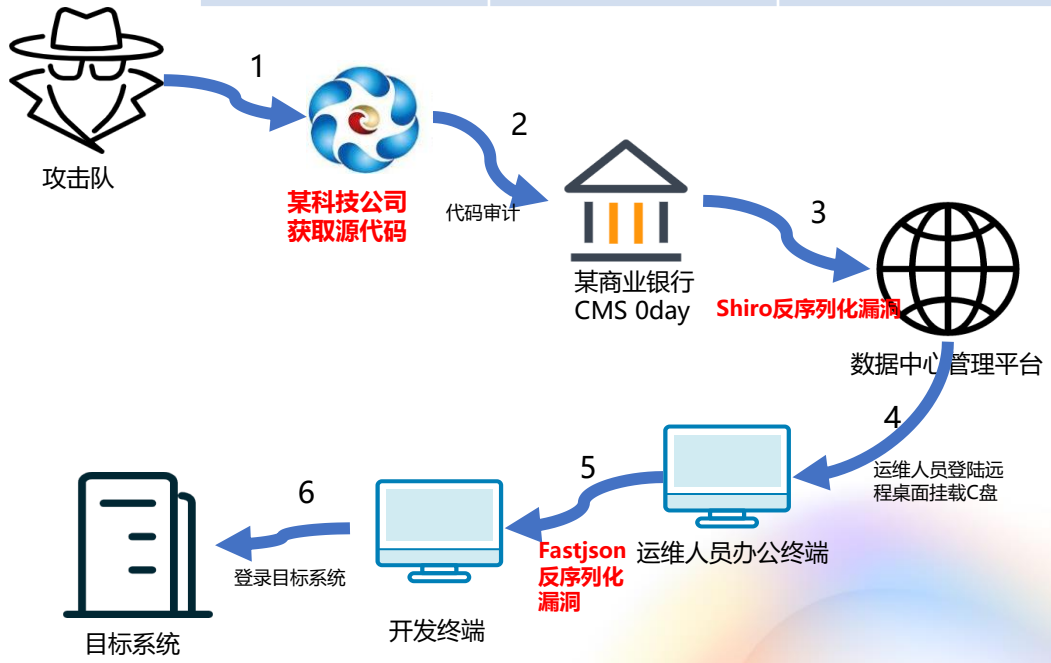
实践四：流行应用软件测评--供应链安全问题严重

- 使用奇安信开源卫士针对某流行Windows桌面应用软件进行了检测，发现该软件中使用了开源软件87个，部分检测结果概要如下：

序号	开源软件名称	开源软件版本	漏洞情况
1	OpenSSL	1.0.2h	高危:5,中危:10,低危:23
2	libpng	1.2.33	高危:4,中危:19,低危:9
3	libraw	0.18.2	高危:4,中危:14,低危:23
4	curl	7.43.0	高危:2,中危:17,低危:38
5	OpenJPEG	1.5.2	高危:2,中危:11,低危:27
6	Expat XML Parser	2.1.0	高危:2,中危:6,低危:2
7	LibIDN	1.2	高危:1,中危:4,低危:2
8	HarfBuzz	0.9.39	高危:1,中危:2,低危:2
9	libpng	1.6.17	高危:1,中危:2,低危:7
10	WavPack	4.80.0	中危:7,低危:11

实践五：HW实战--软件供应链成为常见攻击短板

攻防演习数量	攻陷目标数量	软件供应链攻击数量
244	1900	200



第一步	• 通过信息采集，某科技公司是银行系统的提供商，通过常规攻击手段获取到源代码。
第二步	• 通过源代码分析0day漏洞，入侵到某金融机构。
第三步	• 以此为跳板， Shiro反序列化漏洞横向渗透拿下数据中心管理平台。
第四步	• 通过平台反向给办公终端挂马，控制办公终端，尝试进一步横向渗透。
第五步	• Fastjson漏洞控制正在调试代码的开发人员办公终端。
第六步	• 通过浏览器历史记录直接登录目标系统。

实践六：某企业互联网应用开源软件安全治理实践

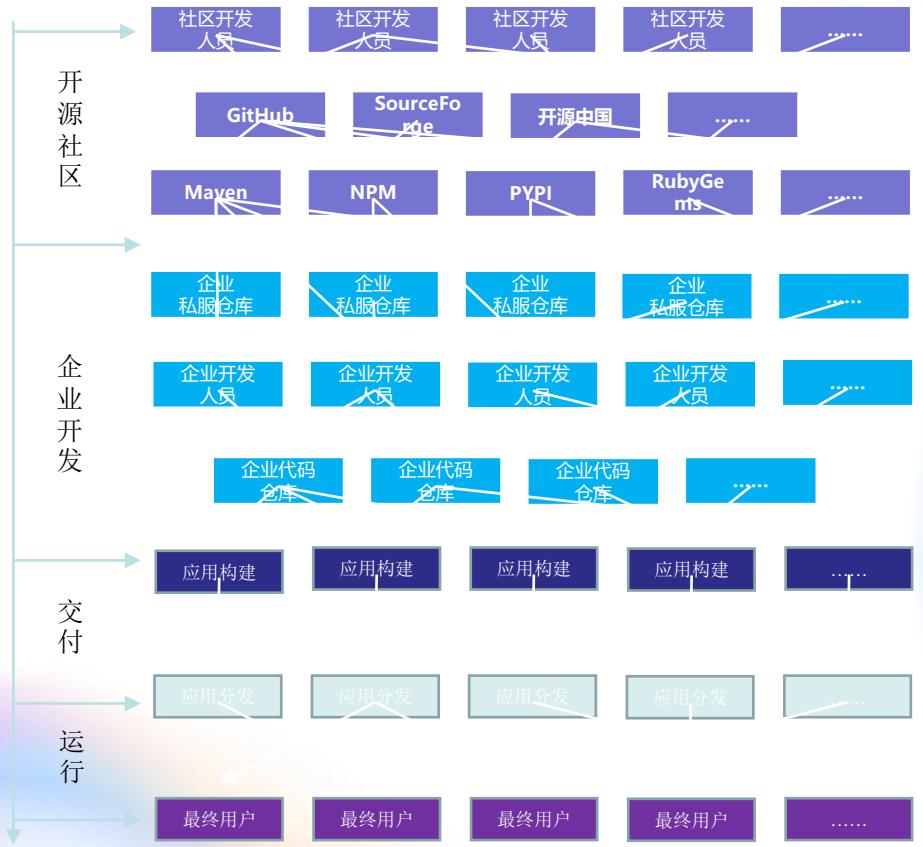
- **实践内容：**
  - 安全分析：通过奇安信开源卫士对某企业某互联网应用进行了安全检测，发现50个开源软件，12个开源软件漏洞， 存在已知poc漏洞4个
  - 漏洞验证：有poc的漏洞在测试环境进行人工验证
  - 修复优先级：通过漏洞利用难度确定修复优先级，有poc验证成功 > 有poc验证失败 > 无poc超危 > 无poc高危
  - 漏洞修复建议：推荐升级版本、漏洞缓解措施、防护策略

- **实践经验总结：**
  - 开源软件资产的梳理，包括自研系统（源代码）、采购或外包软件（二进制）、容器、操作系统等
  - 框架类开源软件，需要架构研发组统一修复
  - 与编译环境相关的开源软件，开源软件升级同步考虑编译器升级，兼容性问题
  - 漏洞修复优先级：从攻击视角看开源软件漏洞的修复优先级，exploit 的可获得性、漏洞的严重性、漏洞的披露日期等
  - 漏洞修复办法：升级、防护、特定缓解措施、精准修复

三、软件供应链安全风险分析与应对

软件供应链安全风险分析

- 软件供应链安全涉及的环节
  - 软件供应链可划分为开源社区、企业开发、软件交付、软件运行几个大的环节，每个环节都可能会引入供应链安全风险，上游环节的安全问题会传递到下游环节
- 软件供应链安全风险分析
  - 开源社区
    - 代码托管平台的访问控制风险、公共仓库的访问控制风险、源代码缺陷/后门、开源软件漏洞、恶意代码
    - 企业开发
    - 老旧开源软件、开发工具被污染、厂商预留后门、外包/自研开发缺少安全审查
    - 软件交付
    - 捆绑下载、非官方渠道下载、下载劫持
    - 软件运行
    - 升级劫持、供应商不具备安全响应能力



企业软件供应链安全风险应对建议

- 开源软件安全治理作为软件供应链安全的首要事
  - 建立企业开源软件安全治理制度和规范，来源控制、统一版本、评估和准入流程等
  - 通过工具建立应用-组件-漏洞-情报之间的关联关系，针对漏洞情报可以进行及时响应
  - 开源不等于免费，企业需要关注开源软件知识产权风险
  - 软件供应商的要求
  - 评估供应商的安全能力，并与供应商签署安全责任协议
  - 要求供应商提供其软件产品中所使用的第三方软件/开源软件的清单， 并明确要求供应商，一旦这些第三方软件/开源软件出现安全漏洞，需承担安全责任

奇安信软件供应链安全相关解决方案-开源卫士

风险分析与报告

- 漏洞等级
- 漏洞利用难度
- 补丁情况
- ……

漏洞风险分析

- 侵权风险
- 协议冲突
- 协议变更
- ……

授权协议风险分析

- 发布时间
- 最新版本情况
- 推荐版本
- ……

运维风险分析

- 组件排行
- 漏洞排行
- 报告导出
- ……

报告与报表

二进制成分分析

Windows、Linux、银河麒麟 KYLIN、中标麒麟 NeoKylin、UOS、docker、PE、elf、JAR/WAR and EAR

源代码成分分析

C/C++、Java、.NET、php、JS、Swift、python、GO、Perl、Scala、ERLANG、R、Ruby

开源软件安全情报库

maven、npm、Github、The Apache Software Foundation、开源中国 oschina.net、…

4000万+开源软件基础信息

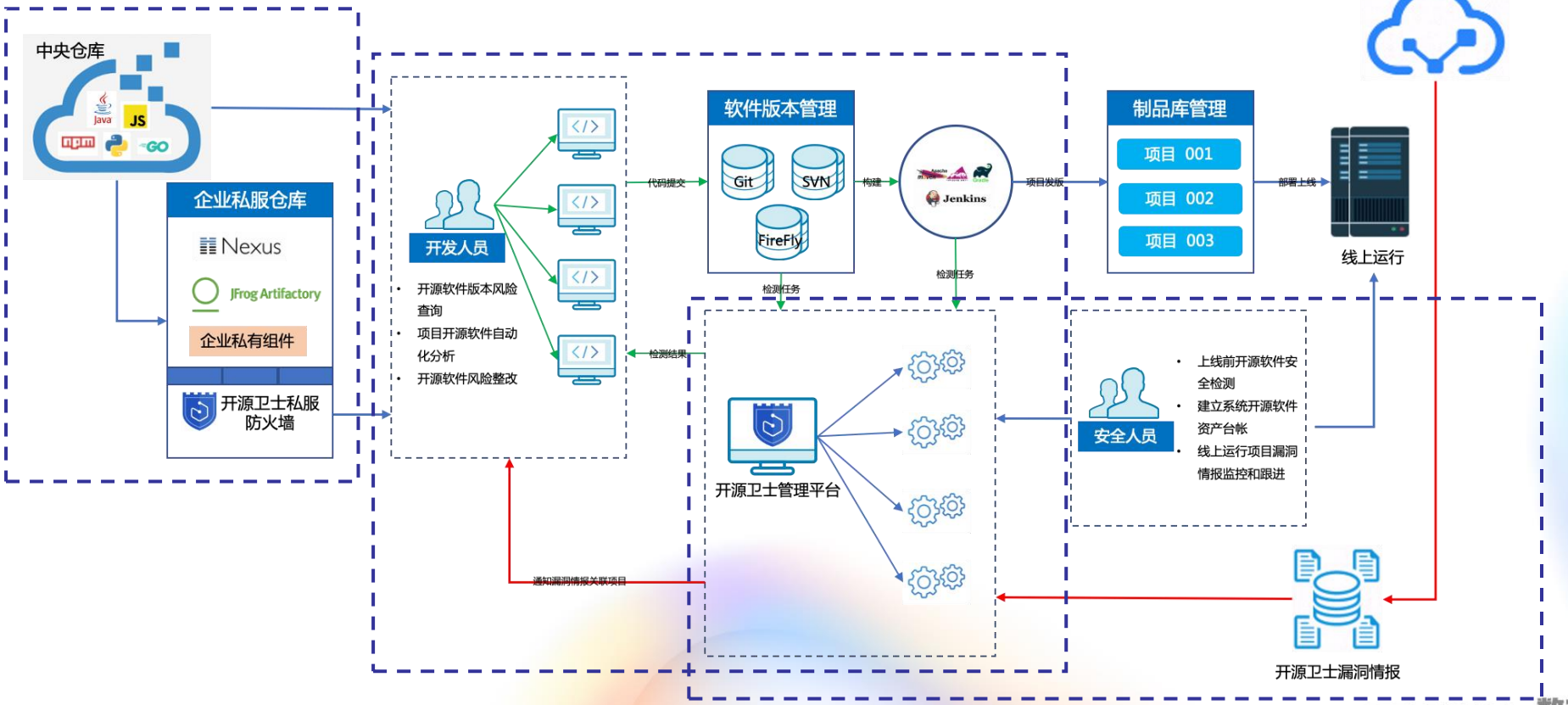
CNNVD 国家信息安全漏洞库、NVD 国家信息安全漏洞共享平台、奇安信代码安全实验室、CNVD、…

500万+开源软件安全信息

GPL、BSD、Apache、MIT、…

500+开源软件协议信息

奇安信软件供应链安全相关解决方案-开源卫士



THANKS!

2021
TRUSTED CLOUD
SUMMIT