极牛网络安全通讯 • 社群期刊 2022 年 5 月 第 11 期

网安观察

P1 中国《网络安全法》
实施五周年

P12
工信部《APP收集使用个人信息最小必要评估规范》征集意见

P18 解构网络安全研发
P21 上千亿条冬奥相关日志不仅仅是“已阅”
P25 要快、要好、还要省？小孩子才做选择

第11期
2022年5月

极牛网

极牛网 网络安全行业媒体

致力于促进中国网络安全行业创新思维的交流与碰撞，搭建中国网络安全技术社区和交流平台



技术格局

网安工程师的成长，需要锻炼开阔的技术视野和统筹全局的战略高度，能够着眼现在思考未来，做懂业务懂策略的工程师。

管理之道

网安工程师随着职业发展，必然面临着向技术总监、CTO等管理角色转型，改变管理思维，建立属于自己的管理哲学。

人才梯队

作为技术管理者，如何建立一个稳固、高效的人才队伍是核心任务，更应该从人才梯队的角度，关注人才的培养的更迭。

企业战略

技术管理者应该建立技术以外的格局，经济形势、商业模式、投融资等等，才能助力企业发展，做与创始人同频的CTO。

产品运营

敢于拥抱和应对变化，敢于创新，在创新的基础框架下，寻找创新的实践方法论，激发技术人员创新能力，推动业务发展。

布道能力

作为技术工程师，需要重点培养自己的布道能力，能将自己的技术成果和理念传播出去，才能拓宽和升级自己的认知边界。

2022年6月1日
中国网络安全法实施五周年

2022年6月1日是《网络安全法》正式施行五周年。作为我国互联网领域第一部专门法律，《网络安全法》为构建网络安全法律法规体系提供了基础性依据。

继《网络安全法》实施后，《数据安全法》《个人信息保护法》等法律法规陆续出台，网络安全法治化进程不断演进，构筑了一张新时代的网络安全防护网。

“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”习近平总书记高度重视网络安全。党的十八大以来，总书记围绕筑牢国家网络安全屏障发表了一系列重要论述，“人民”二字贯穿始终。他反复强调，网络安全为人民，网络安全靠人民。

五年来，《网络安全法》成效显著，极大强化了网络运行安全。

网络运行安全最核心的是公共通信和信息服务，是能源、交通、水利、金融、公共服务、电子政务等重要行业和领域中事关国家安全、国计民生、公共利益的“关键信息基础设施”。

2020年国家互联网信息办公室等十二部门联合制定的《网络安全审查办法》即旨在“确保关键信息基础设施供应链安全，维护国家安全”。

2021年7月某知名网络租车企业上市曾引发不小的风波，2021年11月《网络安全审查办法》修订，“联合出品方”增加了第十三家：证监会，以及“掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”等规定。

这意味着，对关键信息基础设施的规制，增添了新的维度。大型互联网企业境外上市以后需要接受网络安全审查。由于赴国外上市与赴香港上市的网络安全审查尺度不同，诸多企业的上市选择也有了根本性的变化。

也就是说，《网络安全法》实施五周年以来，对于企业安全运营也有了极大的改善。正是有了这一法律，让我国的互联网企业更加规范，更能持久健康地发展，对于促进我国经济高质量发展也有着非常大的促进意义。而这种影响，还将持续很久。

总顾问

叶绍琛

2022年 6 月1 日

CONTEN

目录



安全态势

P4 | 勒索软件攻击已造成国家危机！哥斯达黎加宣布进入紧急模式

P4 | “8220”挖矿团伙持续传播僵尸网络程序：重点攻击北上广等城市

P5 | 俄罗斯电视台在胜利阅兵日被黑，显示“恐吓式”反战信息

P5 | 农业机械巨头爱科遭勒索攻击，美国种植季拖拉机供应受影响

P6 | OpenSSL 命令注入漏洞安全风险通告

P6 | Active Directory Domain Services 权限提升漏洞风险通告

P7 | 国内攻防演习 4 月态势：哪些薄弱点最易被利用?

P10 | 国家药监局印发《药品监管网络安全与信息化建设“十四五”规划》

P10 | 2022 年将制定反电信网络诈骗法，预备审议网络犯罪防治法

P11 | 《政务网站系统安全指南》等 10 项网络安全国家标准获批发布

P11 | 美国司法部发布司法解释，不再对白帽黑客行为追究责任

P11 | 美国 NIST 发布《网络安全供应链风险管理框架指南》



政策解读

P12
工信部《APP 收集使用个人信息最小必要评估规范》征集意见，检测清单需进一步更新

ONTENTS



专题报道

P21
上千亿条冬奥相关日志，赛博威不仅仅是“已阅”

P25
要快、要好、还要省？小孩子才做选择，成年人全都要！



第 1 1 期

《网安观察》编辑部

主办　极牛网

总　　编　　辑：陈鑫杰
总　　顾　　问：叶绍琛
副　　总　　编：王文彦
威胁情报主编：乔跃春
移动安全主编：蔡国兆
网安人才主编：林俊濠
网安产业主编：张　程
网安赛事主编：余　浩
网安态势主编：王　震

公众号　小程序　网站

电子版请访问　www.geeknb.com　阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

版权所有 ©2021 极牛网，保留一切权利。
非经极牛网书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

无担保声明
本资料内容仅供参考，均“如是”提供，除非适用法要求，极牛网对本资料所有内容不提供任何明示或暗示的保证，包括但不限于适销性或者适用于某一特定目的的保证。在法律允许的范围内，极牛网在任何情况下都不对因使用本资料任何内容而产生的任何特殊的、附带的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。

事件篇

勒索软件持续肆掠，对政务民生、国防、能源、民航等多个关键行业造成重大伤害，特别是针对哥斯达黎加政府的攻击，已经影响到国家稳定；俄乌冲突引发的网空风险外溢至全球，黑客组织高调活动，欧洲多国政府受到较大影响。



勒索软件攻击已造成国家危机！哥斯达黎加宣布进入紧急模式

综合消息，自 4 月 17 日 Conti 勒索软件攻击爆发以来，北美国家哥斯达黎加至少有 27 个政府机构受到影响，其中财政部等 9 个机构受到严重影响，如征税工作受阻碍、公务员工资发放金额错乱等。哥斯达黎加新任总统 Rodrigo Chaves 在 5 月 8 日上任后，马上宣布进入全国紧急状态。Chaves 称，有证据显示，国内有内鬼配合勒索软件团伙敲诈政府，这场危机是政府多年未投资网络安全的苦果。

“8220”挖矿团伙持续传播僵尸网络程序：重点攻击北上广等城市

据 CNCERT 5 月 19 日消息，CNCERT 近期监测跟踪发现，“8220”挖矿团伙近期持续传播 Tsunami 僵尸网络程序。抽样监测发现，近期该团伙单日对上千台主机成功实施漏洞攻击，并下载挖矿、僵尸网络程序等恶意样本。上述团伙传播目标 IP 所在地域主要集中在北京、广东、上海等省份城市。目前捕获的“8220”攻击团伙的 IP 类型的攻击资源，主要分布于美国、乌克兰等国家。CNCERT 建议，对暴露在公网上的应用服务使用高强度口令及认证机制，定期对服务器进行加固，修复相关高危漏洞。

俄黑客组织宣布对美欧十国政府发动网络战，意大利政府网站已瘫痪

据观察者网 5 月 17 日消息，俄罗斯黑客组织“Killnet”在社交软件 Telegram 上发布视频，宣布向美、英、德等十国政府发起网络战。“Killnet”称，普通民众在这次网络战中不会有危险，而这些“支持纳粹和恐俄症”国家的政府会被清算。此外，“Killnet”还否认了意大利警方对该组织攻击欧洲歌唱大赛投票系统的指控，并且宣称已经攻陷意大利国家警察官网长达 30 个小时。

加拿大空军关键供应商遭勒索攻击，疑泄露 44GB 内部数据

据 The Record 5 月 11 日消息，加拿大、德国军方的独家战机培训供应商顶级王牌（Top Aces）披露，已遭到 LockBit 勒索软件攻击。LockBit 团伙的官方网站放出了要求，如不支付赎金将公布窃取的 44GB 内部数据。安全专家称，针对国防相关企业的攻击令人担忧，因为无从得知被盗数据最终会落入哪里，很有可能流入对手国家。LockBit 是目前最流行的勒索软件即服务平台之一，据统计今年已攻击了至少 650 个目标组织。

俄罗斯电视台在胜利阅兵日被黑，显示“恐吓式”反战信息

据华盛顿邮报 5 月 9 日消息，在俄罗斯举行胜利日阅兵的重要时刻，该国用户的智能电视显示画面遭到篡改，展示了许多血淋淋的反战标语信息。俄罗斯多个主要电视频道、最大搜索网站 Yandex、最大视频网站 RuTube 均受到网络攻击的影响。俄罗斯政府近期通过一项法律，任何抹黑俄罗斯军队及其在乌克兰作战行动的企图都是违法的，上述信息在俄罗斯国内会遭到禁止。

农业机械巨头爱科遭勒索攻击，美国种植季拖拉机供应受影响

据路透社 5 月 6 日消息，美国农业机械巨头爱科（AGCO）遭到勒索软件攻击，部分生产设施运营受到影响，官方网站无法访问，影响可能持续了多天。有经销商表示，这导致拖拉机销售在美国最重要的种植季节停滞不前。近一年来，多家农业供应链企业遭到攻击，农业逐渐成为勒索攻击重点目标，美国联邦调查局近一年已发布过两次行业预警。

汽车租赁巨头 Sixt 遭网络攻击，全球系统中断致使业务陷入混乱

据 SecurityWeek 5 月 3 日消息，国际汽车租赁巨头 Sixt 遭到网络攻击，部分业务系统被迫中断，运营出现大量技术问题。公司的客户服务中心和部分分支机构受影响较大，大多数汽车预定都是通过笔和纸进行的，服务热线短时离线后恢复，业务陷入混乱。据猜测，此次攻击可能属于勒索软件攻击，目前暂时没有相关组织表示负责。

北京健康宝遭受境外网络攻击：源头来自境外 已有效处置

据北京青年报 4 月 28 日消息，北京市第 318 场新冠病毒肺炎疫情防控工作新闻发布会召开。北京市委宣传部对外新闻处副处长隗斌在会上表示，当天北京健康宝使用高峰期遭受网络攻击。经初步分析，网络攻击源头来自境外。北京健康宝保障团队进行了及时有效的应对，受攻击期间，北京健康宝相关服务未受影响。在北京冬奥会冬残奥会期间，北京健康宝也遭受过类似网络攻击，均得到有效处置。

地缘政治引发欧洲风电安全危机！已有三家公司遭遇网络袭击

据华尔街日报 4 月 25 日消息，4 月中旬，德国风力涡轮机维护公司 Deutsche Windtechnik AG 遭遇勒索软件攻击，约 2000 台风力涡轮机的远程控制系统瘫痪了一天左右。这是自俄乌冲突全面爆发以来，欧洲第三家风能公司遭到网络攻击。此前涡轮机制造商 Enercon GmbH、Nordex SE 先后沦为网络攻击的受害者。有专家认为，欧美制裁俄罗斯能源入口使得风电行业受益，站队俄罗斯的黑客组织试图在这一行业制造混乱。

加拿大老牌航司遭网络攻击，导致航班严重延误近一周

据 CityNews 4 月 21 日消息，因供应商系统遭受网络攻击，加拿大老牌航空公司阳翼航空（Sunwing Airlines）的重要系统中断服务，致使航班严重延误近一周时间。此次事件导致至少 188 个航班发生延误，许多乘客因此被困在机场，有乘客表示已经滞留在机场超过 3 天。为减少服务中断，阳翼航空表示会尽量以手动方式处理航班业务。

漏洞篇

5月初，F5发布旗下BIG-IP严重漏洞的修复补丁，漏洞披露不久便遭到积极利用，攻击者试图实施数据擦除攻击。中国等多国CERT机构纷纷发布安全预警。



OpenSSL 命令注入漏洞安全风险通告

5月19日，奇安信CERT监测到OpenSSL官方发布OpenSSL命令注入漏洞（CVE-2022-1292）通告。该漏洞是由于c_rehash脚本未对外部可控数据进行有效过滤，导致可操作/etc/ssl/certs/目录的攻击者注入恶意命令，从而以该脚本的权限执行任意命令。OpenSSL 1.0.2、1.1.1、3.x版本均受到影响。目前，官方已发布更新版本，建议客户尽快做好自查，及时更新至最新版本。

Active Directory Domain Services 权限提升漏洞风险通告

5月13日，奇安信CERT监测到Active Directory Domain Services权限提升漏洞（CVE-2022-26963）细节及PoC已在互联网公开。当Active Directory证书服务在域上运行时，经过身份验证的攻击者可以在证书请求中包含特制的数据，然后从Active Directory证书服务中获取允许提升权限的证书，并将域中普通用户权限提升为域管理员权限。经研判，此漏洞PoC有效，漏洞现实威胁进一步上升。鉴于此漏洞影响较大，建议客户尽快自查修复，升级至安全版本。

Netatalk 远程命令执行漏洞安全风险通告

5月12日，奇安信CERT监测到开源文件服务器软件Netatalk的远程命令执行漏洞（CVE-2022-23121）细节及部分PoC公开。未经身份验证的远程攻击者利用此漏洞，可在受影响的Netatalk服务上以root权限执行任意命令。奇安信CERT已复现此漏洞，鉴于已有细节及部分PoC公开，攻击者可通过已有信息开发出利用代码，漏洞现实威胁上升，建议客户尽快做好自查，及时更新至最新版本。

F5 BIG-IP iControl REST 身份认证绕过漏洞安全公告

5月7日，国家信息安全漏洞共享平台（CNVD）收录了F5 BIG-IP iControl REST身份认证绕过漏洞（CVE-2022-1388）。F5 BIG-IP是美国F5公司一款集成网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。攻击者利用该漏洞，可在未授权的情况下执行任意系统命令，创建或删除文件及禁用服务。目前，漏洞利用细节已公开，厂商已发布补丁完成修复。



对抗篇

国内攻防演习 4 月态势：哪些薄弱点最易被利用?

一、本月演习整体情况

2022 年 4 月，奇安信 Z-TEAM 团队共承接攻防演习服务 31 场，其中行业级攻防演习 2 场，省级攻防演习 2 场，省级行业攻防演习 1 场，地市级攻防演习 4 场，客户自主攻防演习 22 场。

本月攻防演习成果如下。

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
数量	48	43	57	72	41	67	186	1221

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较集中，以专项任务、政务和金融为主，客户存在的安全问题主要涉及互联网侧应用组件存在漏洞缺陷、内部人员对钓鱼攻击防范意识不足、内网功能区域缺乏安全隔离、内网访问权限策略设置不严格、内网口令复用及弱口令普遍等。具体情况如下：

1、漏洞利用依旧是外网成功突破的主要手段

本月任务数据显示漏洞利用依旧是外网成功突破的主要手段。利用漏洞以平台组件历史漏洞为主，如未授权访问、Spring 组件漏洞、Shiro 反序列化、任意文件上传漏洞等，多因外部应用及系统组件缺乏日常安全巡检机制、对爆出的漏洞组件未及时升级更新造成的，这些漏洞的存在使得目标网络有随时被入侵的严重安全风险。

2、弱口令和口令复用问题在内网比较突出

本月任务中目标内网弱口令和口令复用问题依旧比较突出。在互联网应用系统，内网应用系统、服务器、数据库等信息设备中普遍存在弱口令，这导致信息设备可被攻击者轻易攻陷。同时多台设备使用相同密码、密码长期未修改等问题也比较常见，这些问题致使信息系统面临严重安全风险。

3、钓鱼攻击是实现外部突破的有力辅助

本月任务中针对特殊行业目标系统网络，钓鱼攻击成为外部突破的主要使用手段，由于金融、航空、电力这类目标业务具有较大的开放性，并且内部客服人员网络安全意识不强，因此具有较高的成功率。钓鱼攻击已成为攻击者实现外部突破的高效手段之一。

4、安全意识薄弱导致敏感信息泄露

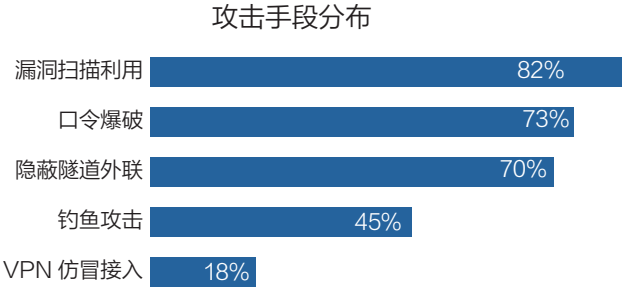
本月任务中目标网络敏感信息泄露较为严重，包括目录文件信息、业务系统、应用开发平台及后台登录地址、内网 IP 地址、接口、安全认证信息在内的敏感源码泄露等，这些敏感信息泄露原因多为安全配置疏漏、平台审核不严，此类敏感信息常常被用来实现针对性的快速突破及渗透。

5、内部网络纵深防护机制不够健全

本月任务中发现目标网络缺乏纵深防护机制。较多客户网络边界隔离不够清晰，一旦突破外网进入内网后，即可横向攻击大量系统、服务器、数据库等内网资产。部分客户在互联网边界安全防护、网络区域边界安全隔离、服务器安全纵深防护等方面未形成纵深防御体系。

三、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，多通过互联网侧业务系统漏洞利用和钓鱼攻击手段实现，内网横向拓展以弱口令、口令复用和内部应用漏洞利用等手段为主。使用的主要技术手段分布如下：



1、漏洞扫描利用

本月任务中漏洞扫描利用主要集中在互联网侧业务系统和门户网站，主要以 SQL 注入、未授权访问、组件反序列化、文件上传执行等漏洞为主。这些漏洞主要是由于系统组件更新不及时、安全策略设置缺陷引起的，直接反映出客户网络运维人员对下辖网络资产动态跟踪不及时、网络运维缺乏常态巡检机制、对存在的漏洞及安全威胁应对不够高效等问题。

2、口令爆破

本月任务中内网口令爆破主要通过弱口令和口令复用方式实现，是内网横向拓展的主要手段。常见问题为

未修改安全应用默认口令、管理员为多台网络节点设置同一口令等，直接反映出目标网络对弱口令和通用口令缺乏统一监管，尤其是对账号口令复杂度设置和安全使用缺乏严格要求。

3、隐蔽隧道外联

本月任务中因大部分目标内网无法通过外网直接访问，需要借助端口转发、隐蔽隧道技术等手段实现转发通信。尤其是对于网络功能区域划分严格、核心业务内网隔离措施完善的攻击目标单位，甚至需要两到三层以上通道转发才能实现对目标核心内网的稳定控制。

4、钓鱼攻击

本月任务中针对网络安全防护相对严密，外网系统难以直接突破的目标，钓鱼攻击成为实现外部突破的高效手段。外网钓鱼攻击主要针对安全意识相对薄弱的客服、人事等人员进行，内网则通过水坑攻击对网络运维、平台研发及核心业务人员等目标进行钓鱼攻击，实现重点突破。

5、VPN 仿冒接入

本月任务中VPN仿冒接入主要针对金融行业目标，因为金融业务性质特殊，分散机构多采用远程 VPN 接入业务网络，测试任务也充分利用目标网络的VPN资源，实现对目标业务内网的隐蔽接入渗透。VPN 仿冒接入认证信息主要通过 VPN 网关服务器漏洞利用、口令复用手段获取。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某金融目标在线点播系统存在 Struts2 漏洞，利用此漏洞可获取目标广播网服务器控制权限，直接突破逻辑内网隔离。

（2）某目标电子文档系统存在 CNVD-2021-26058 漏洞，通过此漏洞利用获取该系统后台服务器控制权限。

（3）某目标外网 OA 系统存在 0day 漏洞，可通过远程命令执行控制 OA 服务器。

（4）某目标管理平台系统存在 Weblogic 反序列化漏洞，可通过漏洞利用获取该管理系统权限，实现网络隔离突破。

（5）某目标互联网业务管理系统存在 Apache Struts2 远程代码执行（s2-005）漏洞，通过漏洞利用获取该管理系统权限。

2、钓鱼攻击

（1）某目标内网对管理员进行钓鱼攻击，在控制目标 ideal 系统后，通过 ideal 注册账号找到管理员邮箱，对该邮箱发送钓鱼邮件并成功上线。

（2）某目标通过电话客服获得某系统运维经理电话，对运维经理进行钓鱼攻击，并成功获取其所运维系统得控制权限。

（3）以招聘内推为由，添加某目标招聘业务人员为好友，对其进行钓鱼攻击，获取内网系统服务器权限。

（4）向某目标官网邮箱投稿钓鱼邮件，通过钓鱼攻击获取主机终端权限。

3、口令爆破

（1）某目标业务系统存在弱口令，可通过口令爆破直接登录该系统管理后台，对系统进行任意操作，获取系统后台中的敏感信息。

（2）某目标外网业务工作培训平台存在弱口令，可通过口令爆破登录业务后台，并进一步拓展控制平台服务器。

（3）某目标 OA 系统存在弱口令，可通过口令爆破直接登录 OA，并进一步获取内网办公业务人员电话、地址等敏感信息。

（4）某目标堡垒机存在弱口令漏洞，通过该漏洞获得内网系统后台管理员权限两个，内网可管控主机 732 台。

4、VPN 仿冒接入

（1）某目标业务网络 VPN 网关存在注入漏洞，通过漏洞利用获取接入目标业务内网的接入口令，最终实现仿冒接入及渗透。

政策篇

国内，全国人大常委会发布《2022 年度立法工作计划》，《反电信网络诈骗法》有望在年内制定推出；

国际上，美国司法部发布司法解释，不再对白帽黑客行为追究责任。司法部副部长称：“计算机安全研究是提升网络安全的关键驱动力。”



国内

国家药监局印发《药品监管网络安全与信息化建设“十四五”规划》

5 月 11 日，国家药监局印发《药品监管网络安全与信息化建设“十四五”规划》。《规划》要求健全和完善网络安全体系，夯实网络安全综合保障能力。具体包括加强网络安全保障管理、推进数据安全保障建设、升级安全管理运维平台。《规划》还提出了两项网络安全任务，完善药监云网络安全信任体系，完善国家局安全管理运维中心。

2022 年将制定反电信网络诈骗法，预备审议网络犯罪防治法

5 月 6 日，全国人大常委会发布《2022 年度立法工作计划》。《工作计划》提出，围绕维护国家安全，促进社会和谐稳定，将制定反电信网络诈骗法（6 月继续审议）等。预备审议电信法、网络犯罪防治法等项目，开展调研和起草工作，视情安排审议。另据《工业和信息化部 2022 年规章制定工作计划》，今年将起草《电信和互联网用户个人信息保护规定（修订）》。

证监会就《证券期货业网络安全管理办法（征求意见稿）》公开征求意见

4 月 29 日，证监会发布《证券期货业网络安全管理办法（征求意见稿）》公开征求意见。《征求意见》稿对证券期货业网络安全监督管理体系、网络安全运行、数据安全统筹管理、网络安全应急处置、关键信息基础设施网络安全、网络安全促进与发展、监督管理与法律责任等方面提出了要求。《征求意见》稿规定，核心机构和经营机构应当依法履行网络安全保护义务，对本机构网络安全负责，相关责任不因其他机构提供产品或者服务进行转移或者减轻。

国家发展改革委发布《电力可靠性管理办法（暂行）》

4 月 25 日，国家发展和改革委员会发布《电力可靠性管理办法（暂行）》。《办法》共十一章，其中第七章为网络安全。《办法》规定，电力网络安全坚持积极防御、综合防范的方针，坚持安全分区、网络专用、横向隔离、纵向认证的原则。《办法》提出，加强网络安

全审查、容灾备份、监测审计、态势感知、纵深防御、信任体系建设、供应链管理等工作，开展网络安全监测、风险评估和隐患排查治理，提高网络安全监测分析与应急处置能力。

《政务网站系统安全指南》等 10 项网络安全国家标准获批发布

4 月 24 日，全国信息安全标准化技术委员会归口的 10 项国家标准正式发布。具体包括智能家居通用安全规范、可信执行环境 基本安全规范、SM9 密码算法使用规范、移动互联网应用程序（App）收集个人信息基本要求、工业控制系统信息安全防护能力成熟度模型、网络数据处理安全要求、信息安全风险评估方法、可信计算密码支撑平台功能与接口规范、信息安全服务 分类与代码、政务网站系统安全指南。



美国司法部发布司法解释，不再对白帽黑客行为追究责任

5 月 19 日，美国司法部发布针对《计算机欺诈与滥用法》（CFAA）的政策执行修订（类似司法解释），首次提出不应对善意网络安全研究追究责任。善意研究是指：仅出于善意测试、调查和 / 或修正安全缺陷或漏洞的目的访问目标计算机。这类活动是以旨在避免对个人或公众造成任何伤害的方式进行的，并且从该活动中获得的信息主要用于促进被访问设备 / 机器 / 在线服务 / 人员的安全或保障。美国司法部副部长 Lisa O. Monaco 表示，“计算机安全研究是提升网络安全的关键驱动力，此举旨在为善意研究人员提供明确规定。”

欧盟商定 NIS2 指令，加强关键领域安全保护

5 月 13 日，欧洲理事会和欧洲议会就 NIS2 指令达成临时协议，商定了在整个欧盟范围实现高水平网络安全的措施，以进一步提高公私部门及整个欧盟的网络弹性和事件响应能力。NIS2 指令为涵盖的关键领域制定了网络安全风险管理措施和事件报告义务的基线，旨在消除不同成员国的要求和实践差异，并要求成立欧洲网络危机联络组织 EU-CyCLONe，执行大规模网络安全事件的协调管理。

美国众议院通过《促进数字隐私技术法案》：大力发展隐私增强技术

5 月 11 日，美国众议院正式通过《促进数字隐私技术法案》，将由参议院进行下一步审议。《法案》是一项支持隐私增强技术研究和促进负责任数据使用的拟议法案。《法案》围绕隐私增强技术的基础研究、劳动力、市场发展、联邦政府采用、最佳实践等方面进行布局。隐私增强技术作为一种广泛的技术，允许组织收集、共享和使用数据，同时减轻这些活动产生的隐私风险。

美国 NIST 发布《网络安全供应链风险管理框架指南》

5 月 5 日，美国国家标准技术研究院（NIST）发布《网络安全供应链风险管理框架指南》项目，这一指南遵循拜登于 2021 年 5 月发布的“改善国家网络安全”行政命令（EO 14028），要求政府机构采取措施“提高软件供应链的安全性和完整性，优先解决关键软件问题。”该指南概述了组织在识别、评估和响应供应链不同阶段的风险时，应采用的主要安全控制措施和做法，以帮助组织识别、评估和响应整个供应链中的网络安全风险，同时还分享了与供应链攻击相关的趋势和最佳实践。



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

极牛众星计划

下一代网络安全新形态教材



政策解读

工信部《APP收集使用个人信息最小必要评估规范》征集意见，检测清单需进一步更新

2022年5月7日，工信部发布《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范 第1部分：总则》等4项行业标准（详见第4节）报批公示稿。公示截止时间为2022年6月7日。该标准适用于APP提供者遵循最小必要原则规范其对用户个人信息的处理活动，对于企业有较强的参考价值。

（一）体系定位

本次公示的4项行业标准（**总则、位置信息、图片信息、短信信息**）为《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》系列行业标准的组成部分。该系列标准旨在对移动互联网行业收集使用人脸、通讯录、短信、位置、图片等敏感个人信息进行规范，落实最小、必要的原则。

该系列行业标准共由16个部分构成：**总则、位置信息、图片信息、终端通讯录、设备信息、软件列表、人脸信息、录像信息、录音信息、通话记录、短信信息、好友列表、传感器信息、应用日志信息、身份信息、剪切板信息。**

（二）与《APP收集使用个人信息最小必要评估规范》团体标准的关系

本次由工信部发布的评估规范属于行业标准，其与电信终端产业协会于2020年起陆续发布的17项《APP收集使用个人信息最小必要评估规范》团体标准密切相关。根据《中华人民共和国标准化法》的规定，标准包括国家标准、行业标准、地方标准和团体标准、企业标准。（T/TAF 077.X-2020）《APP收集使用个人信息最小必要评估规范》团体标准是在缺少相关行业标准的情况下，由电信终端产业协会相关团体于2020年起自主发布，并由社会自愿采用的标准。而（YD/T 4177.X-2022）《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》行业标准是由工信部主导制定的。区别于上述团体标准，该行业标准是对国家标准的补充，**适用于整个通信行业，且指标低于该行业标准的团体标准为无效标准。因此，通常情况下应优先选用该行业标准，并在本系列其他行业标准文件未颁布之前参照相应团体标准。**

此外，虽然无论行业标准还是团体标准都不具备法律强制力，但《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》作为《个人信息保护法》所明确“最小必要原则”的细化落实，及其“主管监管部门、第三方评估机构等组织对移动互联网应用程序收集图片信息行为进行监督、管理和评估”的适用范围，企业仍应将该系列行业标准作为APP合规的重要参考，并在其他部分行业标准出台之前了解既有团体标准内容，从严落实标准要求。



（三）适用范围

移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》系列行业标准适用于移动互联网应用程序（APP）提供者规范用户个人信息的处理活动，也适用于第三方评估机构等组织对移动应用软件收集使用个人信息行为进行监督、管理和评估。个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

· 移动智能终端

能够接入移动通信网，具有能够提供应用程序开发接口的操作系统，并且具有安装、加载和运行应用软件能力的终端。

· 移动互联网应用程序

可安装在移动智能终端内，能够利用移动智能终端操作系统提供的公开开发接口，实现某项或某几项特定任务的计算机软件，包含移动**智能终端预置应用软件，小程序、快应用及互联网信息服务提供者**提供的可以通过**网站、应用商店**等移动应用分发平台**下载、安装、升级**的应用软件。

（四）主要内容

标准编号	标准名称	标准主要内容
YD/T 4177.1-2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 1 部分：总则	本文件规定了 APP 收集使用个人信息的最小必要基本原则、评估要求、评估方法及评估流程
YD/T 4177.2-2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 2 部分：位置信息	本文件规定了移动互联网应用程序（APP）在处理涉及用户个人信息（位置信息）的告知同意、收集、存储、使用、传输、删除等活动中的最小必要评估规范，并通过设备信息在处理活动中的典型应用场景来说明如何落实最小必要原则
YD/T 4177.3-2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 3 部分：图片信息	本文件规定了移动应用软件在处理涉及个人信息主体个人信息相关图片信息的收集、存储、使用、删除等活动中的最小必要信息规范和评估方法，并通过对在个人信息处理活动中的典型应用场景来说明如何落实最小必要原则
YD/T 4177.11—2022	移动互联网应用程序（APP）收集使用个人信息最小必要评估规范第 11 部分：短信信息	本文件是 APP 收集使用个人信息最小必要评估规范系列标准中的短信信息部分，旨在贯彻个人信息收集使用的最小必要的原则，针对 APP 访问、收集、存储、使用、删除用户手机短信（含彩信、5G 消息等多媒体方式）信息等各环节提出相应的最小必要性符合度评估项，并结合典型场景，对 APP 最小必要处理短信信息进行规定

（五）基本原则——最小必要

APP 个人信息的处理应遵循最小必要原则，即处理个人信息应当具有明确、合理的目的，应与处理目的直接相关，采取对个人权益影响最小的方式。**当 APP 提供的业务功能不在《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》系列标准内，同样应满足最小必要要求。**

（六）《总则》明确的最小必要评估基本要求

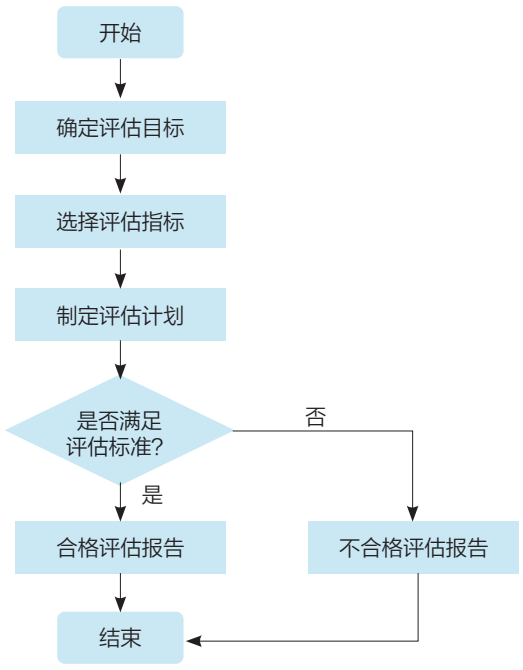
《APP 收集使用个人信息最小必要评估规范 第 1 部分：总则》规定了 APP 收集使用个人信息的最小必要原则的评估要求，其从权限、告知同意、收集、存储等维度全方位地对 APP 个人信息处理环节进行了规定，详见下表：

评估维度	要求
权限	权限申请和使用应遵循最小必要原则，要求如下： · 权限申请和使用的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · APP 应申请与业务功能相关的权限，**不应过度申请权限。**如 APP 的业务功能中，不包含录音相关场景，则不应申请录音权限。 · APP 申请敏感权限时，应**同步告知**权限使用的目的和用途。 · APP 宜优先**采用系统自身功能，代替调用相关敏感权限。**如 APP 需要拨打电话功能时，可优先选择调用系统的电话界面，而不是申请电话权限。 · 不得以改善服务质量、提升使用体验和实施风险控制等为由，**强迫**个人信息主体授予权限。 · APP 申请权限时需要在使用对应业务功能时申请，不应一揽子申请多个权限，不得默认、捆绑或使用其他手段变相欺骗、误导、强迫个人信息主体授予权限。 · 对于**第三方 SDK** 等外部代码的引用，APP 应要求 SDK 其相关权限的申请同样满足最小必要原则，不得过度申请权限。
告知同意	告知同意应遵循最小必要原则，要求如下： · 告知同意应遵循最小必要原则，即 APP 所提供产品或服务涉及多项业务功能的，处理个人信息时，宜按业务功能**单项或分项**获得个人信息主体同意，不应采用捆绑方式强迫个人信息主体一次性同意多种业务功能收集的个人信息。个人信息主体拒绝同意时，仅影响与所拒绝个人信息相关的业务功能的正常使用。 · 告知同意的时机及频率，宜在收集使用之前或收集使用之时的**适当时机**告知，增进个人信息主体对告知与所处理收集的个人信息之间关联性的理解。
收集	收集个人信息应遵循最小必要原则，要求如下： · 收集个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · APP 被授予权限后，权限使用应遵循最小必要原则，即应合理使用申请的权限，不应滥用权限，超频次、超范围、超精度收集个人信息。
存储	个人信息的存储包含本地存储和服务器远端存储，均应遵循最小必要原则，要求如下： · 存储个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · 存储个人信息的类型及数量应遵循最小必要原则，不应超出业务功能的实际需要。 · 存储个人信息的时间应遵循最小必要原则，即存储个人信息的时间，**应当为实现处理目的所必要的最短时间，**在超出上述期限后，应对个人信息进行**删除或匿名化处理。**（注：对于保存在端侧的个人信息，只需对业务运行过程中产生的包含个人信息的临时文件，或过程文件指定删除时间，其他个人信息由用户自己管理和控制） · 收集个人信息后，宜**立即进行去标识化处理，**并将可用于恢复识别个人的信息与去标识化后的信息**分开存储。** · APP 如需在终端本地存储个人信息，则应将个人信息存储在**受保护的文件区域，**防止其他 APP 非授权访问。 · 个人生物识别信息应在本地进行加密存储。如因业务需要确需传出终端的，应使用**单向不可逆摘要算法**进行摘要处理或使用高强度加密算法进行加密处理，且**单独明确告知，用户选择同意**后，方能传出终端。

使用	使用个人信息应遵循最小必要原则，要求如下： · 使用个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要，法律法规另有规定的除外。 · 使用个人信息时，除目的所必需外，应**消除明确身份指向性**，避免精确定位到特定个人。 · 使用个人信息进行定向推送应遵循最小必要原则，不应超出业务功能的实际需要。 · 若 APP 定向推送功能使用了第三方的个人信息来源，应以**个人信息处理规则**等形式向个人信息主体**明示业务功能使用第三方的个人信息进行定向推送**，并向个人信息主体明示第三方的个人信息来源。 · 使用个人信息进行定向推送应显著**区分个性化展示和非个性化展示**，显著区分的方式包括但不限于：标明“推荐”、“猜你喜欢”等字样，或通过不同的栏目、版块、页面分别展示等。 · 使用个人信息进行定向推送应当同时提供**关闭个性化展示**的选项。此外，APP 宜建立个性化展示所依赖的个人信息（如标签、画像维度等）的**自主控制机制**，保障个人信息主体调控定向推送展示相关性程度的能力。
加工	加工个人信息应遵循最小必要原则，要求如下： · 加工个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。 · 间接获取个人信息后，进行加工处理形成新的个人信息并用于其他目的，需要告知，并**再次征得个人信息主体的同意**。
传输	传输个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。
提供	提供个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。
公开	公开个人信息的目的、方式、范围应遵循最小必要原则，不应超出业务功能的实际需要或合理关联，法律法规另有规定的除外。
删除	删除个人信息应遵循最小必要原则，超出存储期限后，应对个人信息进行删除或匿名化处理。

（七）《总则》确认的基本评估流程

APP 收集使用个人信息最小必要评估流程应包括确定评估目标、选择评估指标、制定评估计划、实施评估及得出评估结论五个活动。



1. 确定评估目标

被评估方可为 APP 或者 APP 中某项某类功能。

评估方可为 APP 提供者、开发者和运营者，也可为第三方实验室。

2. 选择评估指标

评估方根据被评估方提供的技术说明文档、被评估 APP 样品等材料：确定初步的方案审核，发现涉及的个人信息类型，选择对应的评估规范标准，并由此定义后续的评估的计划和评估项例。

3. 制定评估计划

评估方应根据评估目标，本着公平、公正、公开原

则开展评估工作。

评估准则内容应至少包括评估对象和范围、评估依据、评估环境、评估工具。

评估准则中应明确评估通过 / 不通过准则。

4. 实施评估

依据对应的评估规范标准开展实施评估活动。

通过各部分实施评估工作可顺序开展也可并行开展，无完整的顺序关系。

各部分最小必要评估结果均应以评估报告的形式进行输出，其内容至少应包括开展最小必要信息类型、评估所选择的评估指标及针对评估指标的评估结果。

5. 得出评估结论

针对开展评估的个人信息类别进行评估，APP 收集使用最小必要未见异常并通过评估，否则未通过评估。

在最小必要评估报告中，应包含评估的环境、评估基本要素和每一项评估的结果，同时还应具体描述评估过程中的步骤，如包含未通过项则评估报告中应包含未通过原因的具体描述。

（八）本次公布的其他评估规范中的重点要求

《APP 收集使用个人信息最小必要评估规范》系列行业标准除总则外，此次公开的其他三份标准文件针对**位置信息、图片信息、短信信息三类敏感个人信息处理活动，就其最小必要性符合度评估项进行了特别规定。**针对每一类数据，相应评估规范均针对不同的处理活动期间，如收集、存储、使用等阶段给出了相应的是否满足“最小化”的评估要求。**由于规范规定的颗粒度非常细，且具有很强的实践操作性，为避免遗漏，本文不再做提炼总结，建议直接阅读相应评估规范。**

值得一提的是，针对每一类数据，各评估规范都对相关信息进行了分类，并列明了典型应用场景，对于受众准确和深入理解工信部监管思路具有很大帮助。有关三类信息的具体分类和典型应用场景我们试总结如下：

信息类型	信息分类	典型应用场景
位置信息	根据 APP 业务场景，APP 可收集的位置信息数据分类包括： · 终端定位信息（卫星定位信息、无线网络信息、移动通信基站定位、传感器、IP 地址等）； · 用户填写的位置信息； · 图片、录像数据中的位置信息	· 地图服务 · 广告服务 · 调度服务 · 资产管理服务 · 搜索服务 · 推荐服务 · 画像服务 · 风控服务
图片信息	图片可以通过拍照、屏幕截图及对图片的再加工的方式生成。**根据图片信息中包含的内容，**可将图片信息分为以下三类。 · 图片基本信息：指图片的基本特征信息，包括图片内容信息（原始的和编码后的二进制码）、图片格式、大小、分辨率； · 图片附加信息：拍照时间、拍照设备、拍照参数、图片名称等可关联出个人的图片信息； · 图片位置信息：指拍摄图片时的精准定位信息。如安卓系统可通过 GpsLocationProvider 来获取精确位置信息	· **社交类：**个人信息主体通过 APP 发送固定数量的图片到明确的一个或多个好友或朋友圈限定范围的场景。 · **媒体发布类：**个人信息主体出于图片公开的目的将图片通过 APP 发布到媒体平台的场景。 · **图片加工类：**个人信息主体通过 APP 对图片进行编辑生成新的图片的场景。 · **图像识别类：**个人信息主体通过 APP 对图片或扫一扫生成的缓存图片进行识别的场景。 · **云盘备份类：**通过 APP 将本地图片备份到云盘的场景。 · **客服 / 售后类：**个人信息主体在 APP 中因某种诉求发送图片到客服或售后的场景

短信信息	文件将短信信息包含的信息类型划分为如下类型。 · **本机用户标识：**用于识别或区分短信、彩信信息所在移动终端设备用户的标识信息，可包括发送者的手机号等；依据短信信息的发送方，本机用户标识可以是短信信息的发送者标识，也可以是短信信息的接收者标识。 · **对端标识：**用于识别或区分短信、彩信信息所在移动终端设备用户的短信通信对端标识信息，包括接收者的手机号等。 · **短信内容：**为短信发送者编辑并发送给接收者的各种格式的内容。单一的短信内容是否包含个人信息、包含的个人信息的类目数量及包含的具体个人信息类型取决于每个短信内容的本身。 · **时间：**移动终端设备用户接收或发送该条短信的时间	· **短信云备份：**以数据备份为目的，APP 将用户终端上的短信信息传输至远端服务器上存储的场景。 · **验证码便捷获取：**以协助用户完成登录或支付等操作为目的，APP 识别短信中的验证码并提示用户的场景。 · **便捷短信查询与服务订阅：**以方便用户操作为目的，APP 帮助用户发送特定短信指令至特定号码，查询相关信息或订阅服务的场景，如流量余额查询。 · **短信优化编辑与发送：**以协助用户编辑并发送短信为目的，APP 提供短信编辑功能并发送短信至用户指定号码的场景。 · **短信功能体验增强：**以增强用户短信功能体验为目的，APP 为用户提供如短信发送商户识别和图形化展示等增强短信功能的场景。 · **手机间数据互传：**以在用户不同手机间传输数据为目的，将用户一部手机中的短信信息传输至用户另一部手机的场景，如换机。 · **骚扰拦截：**以帮助用户拦截、屏蔽诈骗、广告等用户不期望接收的短信信息为目的，APP 识别、展示并处置相关短信信息的场景。 · **服务智能化：**以改善服务智能化程度或用户体验为目的，APP 访问用户短信信息的场景。 · **已关联设备的配套应用：**通过此类应用用户可将移动设备与已关联设备（如智能手表、汽车、智能家居设备等）连接起来，还能够收发短信。 · **跨设备同步或转移短信：**在多个设备上（如手机和笔记本电脑之间）同步短信信息。 · **设备自动化：**用户可让设备根据其设置的一个或多个条件（触发条件），在操作系统的多个区域自动执行重复性操作。 · **企业存档及设备管理：**企业存档、客户关系管理 CRM 和 / 或设备管理，如运营商通过短信上报设备信息与驻网状态。 · **车载免提使用和投影显示：**与驾驶 / 出行的核心功能（如导航）直接相关的 APPs，尤其是在用户与设备的物理互动受到限制的情况下。 · **呼救短信：**可在发生人身安全或紧急状况时发送报警短信。 · **用户数据本地备份与还原：**用户的事务性备份和还原及企业的归档（限时 / 非连续）

（九）合规建议

我们理解，**企业应当重点关注、优先适用新发布的行业标准，从数据全生命周期出发规范 APP 的个人信息处理活动以此落实最小必要原则，并持续监测该系列其他行业标准的发布。**同时，考虑到该系列行业标准整体为团体标准的优化、提升，我们也建议企业了解既有团体标准内容，提前做好部署。

目前阶段可供采取的具体行动包括：

（1） 梳理现有 APP 位置信息、图片信息和短信信息，并将其根据《评估规范》进行基本分类。

（2） 根据《评估规范》要求，按照信息类别排查其数据处理活动是否符合最小必要原则，并作出必要整改，对于无法整改的（如定推服务中对与第三方来源信息的披露），应当考虑适当的风险规避措施。

（3） 修订相应的《隐私政策》。

极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

极牛网旗下面向网络安全工程师的社群平台，汇聚行业中网安工程师的知识和社交平台，围绕『技术』『管理』和『圈子』三个核心能力，将前沿的技术内容、技术管理成长感悟、技术圈子社群平台等向优质的网安工程师开放，每月定期组织社群会员线下活动，强调内容分享的体系化和活动内容的多样性，为中国网络安全工程师打造专属的全方位综合赋能的社群平台。

技术

聚焦前沿技术、热点技术、难点技术，提升网安在企业架构中的决策能力和迭代能力。

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

建立精准的技术方向圈子，针对不同的职业发展阶段，组成技术成长小组一起结伴同行。

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

极牛·产业生态

网络安全产业生态平台

极牛网络安全产业生态平台，通过产服、产孵、产投、产研四大引擎，打通技术、产品、平台能力以及B端G端场景和服务体系，构建产业核心生态圈，与合作伙伴共生共赢，助力网安产业智慧升级。



四大引擎

产服

以产业基地为载体
提供产业生态服务
助力产业发展

产孵

以产业加速器为载体
孵化优质企业
与ToB业务的合作

产投

以产业生态投资
为重要抓手
构建产业生态体系

产研

构建产学研体系
聚焦底层技术创新
全面赋能网安产业

产业生态架构

与生态伙伴一起持续加大资本 、资源 、 技术 、 能力和商机投入，助力科技创新驱动网络安全产业升级，为社会创造更大价值



解构

网络安全研发

面对安全设施日益复杂、安全响应压力不断增大的挑战，平台化正成为安全的未来发展方向。



平台化成为共同选择

4月19日，奇安信集团举办的研发平台战略发布会，奇安信董事长齐向东发表“研发平台化 网络安全的未来之路”的主题演讲，首度阐释集团的平台化战略。数日后，趋势科技发布统一网络安全平台 Trend Micro One。Gartner 的最新研究称，安全产品整合是未来的潮流。

网络安全平台以降低网络安全的成本和复杂性，提高响应能力和效率为目标，正在成为头部网络安全企业的共同选择。

网络安全世界正发生巨变

网络安全世界正在发生巨大变化，变化之快之大，使其面临与过去的情况完全不同的网络安全格局。

数字转型逐步深入，企业越来越多普遍地部署数字平台、云计算、物联网 (IoT) 和移动技术，由此产生了更多需要管理的端点、更多需要保护的网络和更多需要保护的数据。作为连接企业所有网络资产的攻击面正在迅速扩大。

与不断采用的新技术相比，网络安全则是另一回事：实际上，近 80% 的机构引入创新技术速度超过了保护自身免受网络攻击的能力。安全多是事后考虑并临时部署，由此部署的解决方案会带来更多的复杂性。

长期以来，企业习惯于头痛医头的安全策略，习惯于添加孤立的安全工具来应对单一的安全问题。根据 ESG 研究集团的调查，近 2/3 的大型企业（ 5000 名以上员工的机构 ）至少有 25 种网络安全产品在使用中。波耐蒙研究所(Ponemon Institute)在全球的调查则显示，企业在其网络上部署了 45 种网络安全相关工具。

企业部署的网络安全工具越多，其防御的效率却并没有提高。管理成本高昂的零散工具拼凑在一起，给有效和快速的威胁检测造成阻碍。

过多网络安全工具导致机构无法及时检测和打击网络攻击：根据 IBM 的网络弹性报告，部署超过 50 多种网络安全工具的企业，其检测威胁的能力降低了 8%，防御能力降低了 7%。同时，大多数机构无法配备足够多的安全运营人员来管理增多的工具和处理频出的告警。

与此形成对照的是，攻击者的网络攻击技术与手段却不断精进，频繁利用各种攻击面的安全漏洞，实施勒索与数据窃取活动。

彼此孤立、随意增长的安全工具与危险的威胁形势、不断增长的攻击面越来越不能匹配。

平台化成为共同选择

ESG 在 2019 年的研究表明，许多机构已经受够了这种日益复杂、数量众多的安全设施：大量的安全工具令企业“不堪重负”。ESG 的网络风险管理研究项目显示，从多家安全厂商购买产品与技术会增加复杂性和成本。Gartner 在 2021 年底的研究也显示，目前用户对于集成与整合安全系统的需求不断增长。

研究人员建议，企业应与经验丰富的网络安全专家合作，构建能够动态扩展的网络安全平台，以最大限度地减少不断增长的攻击面，从而可以保障数据安全和业务稳定。

因此，为了提高安全效率、降低复杂性，企业需要从使用多个不同且孤立的安全工具转为使用高性能的网络安全平台，以保护分布在边缘环境、用户、系统、设备和关键应用中的数据。

作为单点工具的替代品，紧密耦合的安全平台将安

全能力整合到单一集成平台中，可以覆盖端点、网络和云，提供高级威胁防护与集中管理，无疑成为应对当前安全挑战的最优选择。

正如 20 世纪 90 年代，许多组织放弃了部门应用，转而采用为企业业务流程和规模设计的集成 ERP 软件。尽管转变并不容易，但将应用和数据整合到统一平台，带来了新的业务流程、改善了决策制定，实现了更高的收入和更低的成本。



在网络安全背景下，通过集成和整合实现的平台化，可以实现从整个基础设施——端点、电子邮件、云工作负载和应用、网络，收集和管理数据，无疑会改进威胁预防，加速威胁检测和事件响应。

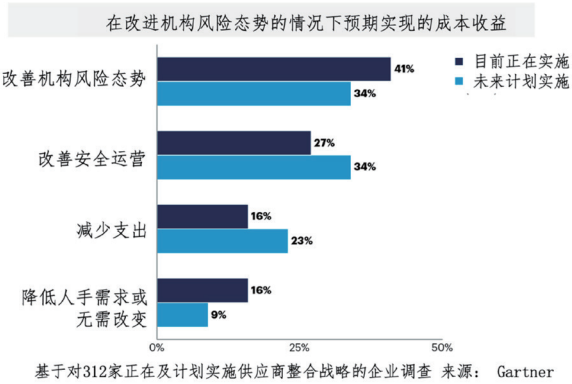
从产品集成到供应商整合

与建设安全平台相对应，越来越多的机构在推进安全供应商整合战略——寻找具有集成技术平台的网络安全战略合作伙伴，在简化安全运营的同时提升安全能力。

Gartner 预计，到 2025 年，3/4 的大型机构将积极推行供应商整合战略，目前这一比例约为 1/4。ESG 的研究则显示，有高达 91% 的企业正积极整合或考虑整合网络安全供应商。

整合网络安全供应商可以带来诸多收益。根据 Gartner 的调查，供应商整合可以改善风险态势、改进安全运营，以及降低成本等收益。

供应商整合战略的主要收益



基于对312家正在及计划实施供应商整合战略的企业调查 来源： Gartner

因此，研究人员建议，为了保护安全投资和提升灵活性，企业安全负责人应部署具有开放架构、开发人员支持和合作伙伴生态系统的平台，可以实现现有的第三方系统的集成。

目前，国内外的安全厂商正逐步分为集成平台厂商和产品组合厂商，前者集成安全工具，实现1+1>2的效果；后者几乎没有集成。

据奇安信集团董事长齐向东介绍，平台化一直是奇安信长期的战略。从 2020 年启动平台化战略，到目前已经完成了第一步，即研发平台化。研发平台化可以提升人效比，帮助公司盈利。未来要实现第二步，即产品平台化，真正地实现安全产品协同与数据统一管理。最终实现第三步，即到 2025 年实现能力平台化。未来，齐安信将在合适的时间向生态伙伴开放其研发平台。

华云信安·产业教育中心

网安人才培养新模式
打造产业人才成长圈

产教融合

INTEGRATION OF PRODUCTION AND EDUCATION

- 共建产业学院
- 共建合作专业
- 共建联合实验室
- 共建人才/师资培养基地
- 1+X证书合作
- 教育部协同育人项目合作

上千亿条冬奥相关日志，赛博威不仅仅是“已阅”

作为世界上规模最大、影响最广、竞技水平最高的冬季综合性体育赛事，冬奥会的吸引力似乎已不再局限于冰雪运动员及爱好者。随着数字化技术的日益普及，无论是组织严密的黑客团伙还是民间网络犯罪分子，都试图寻求对奥运会进行网络攻击。比如在平昌冬奥会在开幕式当天，包括冬奥会网站、电视服务在内均遭到黑客攻击，导致部分业务中断。

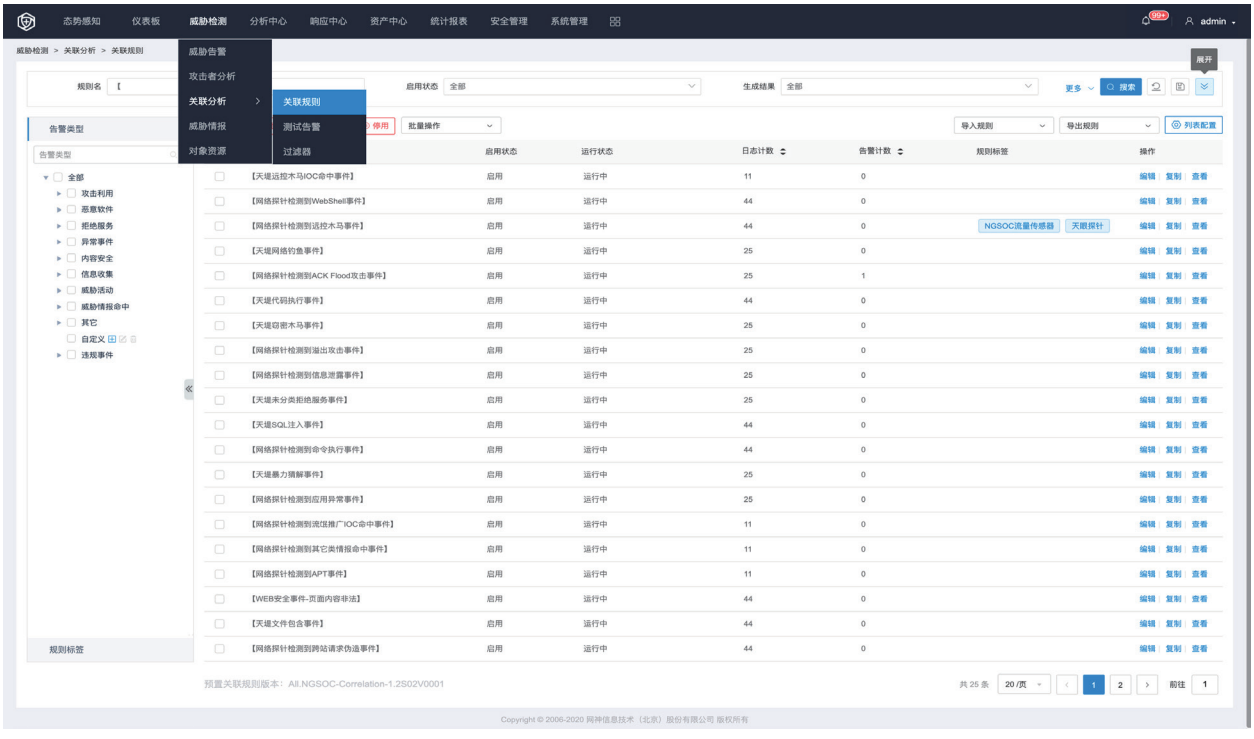
面对网络攻击的压力，在北京冬奥会，奇安信首创了冬奥会系统安全体系，实现了网络安全的“零事故”。而在零事故的背后，其中一项关键性技术就是奇安信集团自研的大数据实时关联分析技术 -Sabre（赛博威）引擎，它支撑起对冬奥 26 个场馆、上千亿条日志的实时监控与安全分析，累计监测数亿次网络攻击，跟踪和研判上百起涉奥威胁事件。

冬奥是一个实时关联分析技术的非常典型的应用场景，具备完整要素。

多源异构数据的采集

毋庸置疑的是，安全运营是落实网络安全防护的最重要手段之一，而安全运营的核心是安全分析，安全分析的核心目标是找出异常事件，并判断这些异常事件是不是由网络攻击造成的。

在这里，事件是 IT 系统中某一活动产生的一组数据，体现的是一个对象，它是有特定的属性和对应的属性值组成。比如一个防火墙事件可能包括源 IP 、包括



目的 IP、目的端口等信息，而这些数据都被以日志的形式记录了下来。

所以想要找出异常事件，安全分析的第一步，就是把日志数据都采集起来，并以事件流的方式输入到安全分析引擎中。

“冬奥期间的日志数据来自于 18 类、共计 1000+ 数据源。”奇安信实时安全分析引擎负责人覃永靖介绍，冬奥期间，所有 IT 系统和网络设备的日志都要汇聚在实时数据平台，不仅仅包括奇安信部署的自有防火墙、SD-WAN、天擎等 55 款 813 台各类安全设备，还包括终端、服务器、网络设备、应用系统、业务系统等所有各类 IT 资产。

这些数据源分布在各个场馆、网络中心、数据中心以及云上系统，它们所产生的日志会被源源不断地送到实时安全分析引擎中进行关联分析。

这其中就产生了三个要特别注意的问题。

第一是尽可能采集所有安全相关日志，不遗漏相关数据。全量日志数据是不发生漏报的最基本条件。网络攻击尤其是 APT 攻击的发现往往取决于看到细节的能力，部分数据漏掉后就很容易产生“漏网之鱼”。比如一次突然的异地登录或者一个未知域名的访问，这些都有可能是已经被入侵的信号。如果采集的数据不全，这些信号就可能会被错过了。

第二是需要将采集的数据尽可能快的发送到安全分析平台，日志在源源不断的生产，后面分析引擎处于一刻不停的自动分析过程中，采集到的数据需要确保一定的时间线，即前后的时间差需要在一个窗口之内，时间相差太大的日志会影响分析的资源和结果产生影响，因此在整条数据流水线上需要保证一定的实时性。

第三是要能够对各类不同的安全日志进行标准化采集、传输解析和处理。数据源不只有奇安信自有的安全设备，还有多个不同供应商的各类应用，这其中不只有网络安全厂商，还包括网络设备提供商、云计算提供商、应用软件提供商甚至包括大大小小的开源组件等等，所以对于多源异构数据的支持也非常重要。这个过程叫做归一化，不同类型但相同含义的字段需要统一类型和名称，为后面的实时安全分析做好准备。

实时安全分析

日志收集起来后，仅仅是“已阅”是不行的，实时分析引擎的核心应该是“判”。

安全分析方法主要包括两种；第一种是延迟计算，即数据收集和安全分析分离；第二种是实时计算，也就是数据收集和安全分析同步进行。

显而易见的是，在每天能够产生超过 40 亿条日志、峰值可以达到近 10 万条每秒的冬奥网络环境下，实时计算更加合适。

否则安全事故没准已经发生了，计算还没开始，这还谈何零事故。

奇安信的实时安全分析引擎分为三层。底层是大数据集群，主要用于日志数据的采集、存储和预处理。大数据集群为实时安全分析提供了强大的算力支持，否则面对如此海量的多源异构数据就该“罢工”了。

中间层主要进行安全分析，它基于目前最流行的开源实时计算框架 Flink 构建，负责利用各种技术手段，同时结合威胁情报、漏洞情报、资产等知识数据，对日志进行安全分析。

最上层则是应用层，负责与用户进行交互，输出分析结果和向安全分析引擎传输用户指令。

众所周知，安全分析的关键要素就是时间，即要求能在最短的时间内发现网络攻击行为、响应安全事件，并且在发现新型攻击行为之后，能够第一时间上线针对性的安全检测方法。

显然，快速完成安全分析是零事故的另一个关键保证，它能够将网络攻击控制在最小范围内。

好在 Flink 最重要的特点是允许以数据并行和流水线方式执行任意流数据程序，并且具备高吞吐低延迟的能力。这就意味着，在充足算力的支持下，即便冬奥期间的日志量再大一些，奇安信安全分析引擎依然能够平稳运行，保证日志分析的速度和准确度。

但安全分析的目的是要找出异常事件，因此用户需

要快速实现威胁建模，并在特定模型下将计算结果与外部输入的检测规则、威胁情报、漏洞情报等知识库进行匹配。

所以，安全分析引擎不仅仅要求极快的计算速度，还要使用起来非常便捷，这样才能最大化提升安全分析的效率。

对于后者，原生 Flink 框架的支持力度是远远不够的。

“所以我们提供了一种针对安全分析场景进行特定优化的安全分析语言。”覃永靖说，它满足了以下几个特点：

第一，简单易用，学习成本低，易上手，能够满足一个没有研发背景的人，也能经过简单学习之后就能上手使用。

第二，支持丰富的数据类型，这些数据不仅要包含文件读写、网络访问等基础数据类型，还要包含大量的安全数据比如 IP，各类时间、资产、漏洞、威胁情报、地理位置等，用户可以不做任何定制就能直接对这些数据进行关联分析，因为这些数据能够为安全分析提供大量的直接证据。比如恶意软件感染发生的时间，感染的主机类型、数量、与外部发生通信的 IP 地址、使用的漏洞、攻击载荷等等。

第三，提供丰富的语义，尤其对安全分析语义进行增强和定制以及扩展。安全分析的场景是复杂、多变的，没有丰富的语义很难满足所有安全分析的需求。但即便是这样，不同的网络环境依然会面临无对应语义的情况，这就需要有经验的分析师进行个性化扩展。攻击手法的变化非常频繁，对于安全分析来说，总会遇到一些安全语义无法判断和解释的行为，尤其是冬奥场景，这对于国内安全厂商来说都是头一回，很难保证不出现什么意料之外的局面。

行为分析与复杂事件关联

如果分析结果能够与已知的规则、威胁情报进行匹配，比如 URL、IP 地址、文件 MD5 等，那自然是网络安全问题无疑，但还有一些时候并不是这样。

举个典型的例子，比如内网某主机的流量经常会明显高于其他同类型主机。

这当然有可能是该主机已经被攻陷，被植入了一些特殊的木马导致流量异常增高。攻击者使用了全新的特种木马和基础设施，导致终端安全软件并没有检测出来。

但如果是仅凭流量偏高这个条件，分析人员很难判定它是异常，因为分析工具并没有一个基线标准能够进行比对，有可能就是有一些特殊业务或者特殊时间段，导致流量偏高。

针对这种事件，行为分析是一个非常有用的安全分析方法，它通过学习待分析对象的历史数据生成安全基线，来检测异常行为。比如今天这个主机的流量不仅比同类型其他主机高，也比历史平均水平和流量峰值高出许多，那基本可以判定是异常行为，需要进一步检查。

从中能够看出，安全基线是判定异常行为的核心。

安全基线分为三类，第一类是统计类安全基线，包含常见的时长、大小、频率、空间、范围等多种形式；第二是序列类，比如指数平滑类和周期类安全基线，具备明显的时间先后顺序或者周期规律；第三是机器学习类的安全基线。（基线详情可参考《当你不知道孰是孰非的时候，总有一个引擎在默默制定判断标准》）

在冬奥场景中，基线检测的应用范围会更加广泛。作为一个全新搭建起来的复杂信息系统，不论是人还是安全设备，都会感到非常“陌生”。因此，历史数据的学习，对于检测异常行为而言十分必要。

除了行为分析以为，关联分析也是必不可少的一项手段，它主要适用于两个场景：第一，单一事件无明显异常，但多个相关事件进行关联则表现出明显异常；其二，单一数据源无法反应攻击全貌，需要综合终端、流量、服务器等多个数据源进行全局关联分析，还原完整攻击链条。

再举两个例子。日志显示，多个高危端口短时间内被多次扫描并尝试登录；内网某服务器发现非法访问行为。

这些事件可能独立发生，也可能会同时发生，之间可能有关联也可能没有关联。如果结合前文中的例子，那么完整的事件就有可能是攻击者攻陷了某内网终端，并利用该终端通过高危端口访问某服务器。

这就是关联分析的重要意义。

“关联分析是一个常用的安全分析方法，比如当发现某个安全事件后需要将攻击者信息进行全局关联，来发现是否还有其它攻击行为。”覃永靖说，这就像拼图游戏，缺少一块是永远拼不完整的。

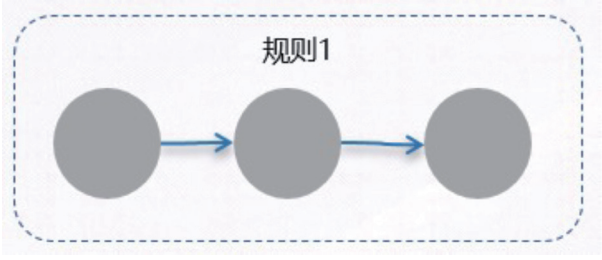
性能优化与状态监控

需要注意的是，对于冬奥这种全球瞩目的大型体育赛事，对于业务的连续性要求是近乎严苛的。大到全球的电视转播，小到一个记分牌或者计时牌，都不能中断。

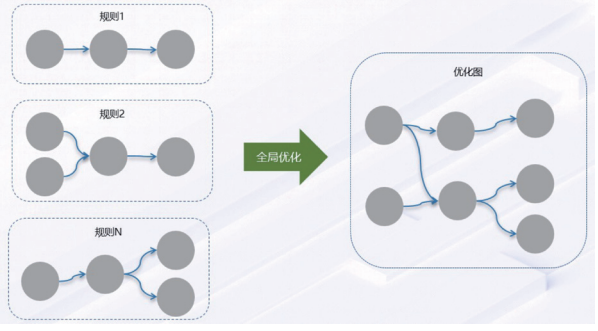
这也就是说，网络安全事故是决不能出现的，但同时也绝对不能出现“网络攻击没把网络搞瘫，‘安检’却把它搞瘫了”的现象。

这就需要对性能和资源使用进行优化，防止占用过多硬件资源。

对于实时分析引擎而言，每条检测规则可抽象为一个逻辑子图，用于表达检测流程，就像下图这样：



然而一个安全检测集通常包含上千条规则，如果同时运行这么多规则，必定会消耗大量的资源，因此需要在全局层面进行优化，将分散的子图转换为一个执行图，以此大幅降低计算复杂度，大致过程如下图：



另外一个需要重点优化的就是外部数据的匹配。在冬奥期间，奇安信累计投入生产了超过 25000 条高质量的威胁情报，如果再加上 10000+ 台终端信息、漏洞情报信息以及各种黑名单、白名单，这个数据量是相当大的。如果每次事件都进行一一匹配，就相当于挨个“打招呼”，不仅需要大量时间，还会造成性能损耗。因此分析引擎需要支持一些数据匹配和存储的优化计数，包含精确、范围和模糊匹配的方法，来提升匹配速度。

比如威胁情报、资产、漏洞、各种白黑名单等，对于超大规模数据表的匹配会带来一些很大的挑战，比如大规模串正则匹配问题等，比如超大规模串正则匹配引擎（100w+），hash 匹配、大规模 IP 匹配计数，包含精确、范围和模糊匹配，以及大规模知识库存储和匹配的优化方法。

万事俱备，然而当引擎真正运转起来之后，作为使用者，还得关心它运行的好不好，如果某些组件资源占用过多，就得对其采取下线、隔离或者限制资源使用等措施了，防止影响其他规则甚至业务的正常运行。

当然，有时候也不能过快了。

实时分析引擎的下游业务可能是一些处理能力比较慢的流程，这时候就需流量控制，防止较快的处理流程向较慢的处理流程输入过多的数据而引起资源过度消耗和卡顿。流量控制需要支持主动流量控制、被动流量控制以及时间窗口相关的流量控制，通过用户配置或自动处理来解决前后处理性能不一引起的数据丢失和系统不稳定问题。

粗算起来，冬奥期间经过实时分析引擎的日志数量就超过了 1000 亿条，产生的告警数量也是极为庞大的。这样的爆肝能力搭载在奇安信 NGSOC 上，难怪会让奇安信冬奥重保奇安信冬奥保障总架构师尹智清直呼“爱了爱了”。

不过，保证冬奥零事故也不是就靠一个实时分析引擎就能完成的，而是人 + 工具 + 流程 + 数据的交互结合，并且不断完善的动态体系。

而奇安信冬奥期间实时安全分析所累积的经验，也将为整个中国乃至全球的网络安全服务。

要快、要好、还要省？小孩子才做选择，成年人全都要！

产品经理：“开发的兄弟们，咱们这个新版发布时间，能不能再提前几周？”

交付主管：“客户希望这版性能要好、bug 要少，还要稳定可靠……”

HR：“对不起，HC 已经锁了，其他部门也抽不来人了。”

……

“少小不努力，长大敲代码”。话说每一位程序猿、攻城狮，上辈子都是折翼的天使。他们经常要加班加点，没完没了的写代码，满足各种需求变更，争抢工期，保障质量。尤其是，他们经常要同时满足三个不同的愿望：

愿望 1：产品经理希望开发更快

愿望 2：销售、交付们希望质量更好

愿望 3：HR 需要更高的人效比，即控制好人力成本

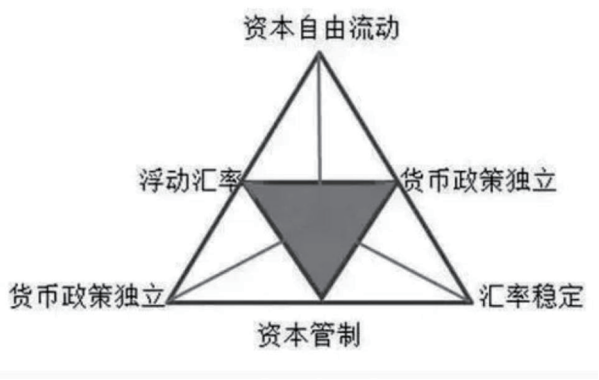
说实话，满足其中两个需求，通常就需要使出洪荒之力了，如果要实现三个，即便是将阿拉丁神灯召唤出来，也未必能够得偿所愿。

引用奇安信川陀平台技术负责人刘浏（人称：刘大爷）的话，对于每一位具有匠心的产品经理来说，都期望每款新产品能又快、又好、又低成本的开发出来，但真正在做一款产品时，必定会在“不可能三角”中艰难取舍。

为什么同时满足三个需求，就非常难呢？这里要普及一下“不可能三角”的概念。

不可能三角（Impossible trinity），原本出自于经济学领域，主要指经济社会和财政金融政策目标选择面临诸多困境，难以同时获得三个方面的目标。在金融政策方面，资本自由流动、固定汇率和货币政策独立性三者也不可能兼得。





“不可能三角”虽然起源于经济学领域，但实际上在我们生活中，可以说是无处不在。比如说找工作，“钱多、事少、离家近”，就是常见的不可能三角。爱情中也存在“不可能三角”，女生选择男生的标准，则不可能同时高帅、专一、有钱；男生选择女生，“不可能三角”就变成了漂亮、温柔、独立。还有选择餐馆的“不可能三角”：好吃、便宜、人少。

这个三者难以兼得、最多选二的规律，就叫“不可能三角”。

那么，传说中的“不可能三角”真的无法打破么？是否有一种钥匙，能让我们放弃取舍，实现三者兼得呢？



答案是肯定的。

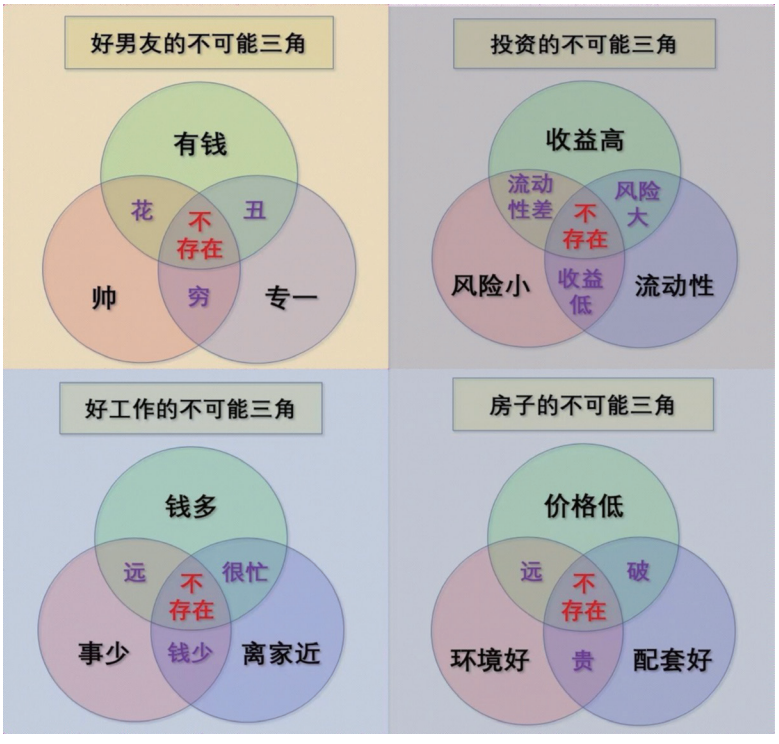
有句话说的好：小孩子才做选择，成年人全都要。

对于一个优秀的研发团队来说，就是需要解锁出“三头六臂”的必杀技，同时满足“快”“好”“省”的各种需求。

奇安信推出的研发平台，就是在探索能实现“高效率、高品质、节省成本”的三全之道。

奇安信集团董事长齐向东曾说过：数字化产业中，经常会遇到两个魔咒：第一个是人员增速超过营收增速的“人效比魔咒”，就是服务客户越多，工作量越大、开发周期越长，相匹配的人员就越多，导致人力成本也越多。

第二个是标准化产品无法满足个性化需求的“标品化魔咒”。数字化产业中企业客户业务复杂，个性化强，很难实现“标品化”。为满足不同企业的不同功能需求，服务提供商要对产品进行定制开发，研发周期一般是 9 个月，这就造成一款产品的定制难、复用难。



研发平台是如何解决的呢?

首先拿“快”这一维度来说。奇安信集团副总裁、大禹平台负责人左文建给出的钥匙是：“依托大禹平台，奇安信在监管态势感知、SASE、TSOC、工业安全等多个领域的首版本发布时间，从同类产品 9 个月缩短至 3 个月，研发效率提升了 300%。冬奥研判分析体系的开发周期，在冬奥组委的极限需求下，更从传统的 100 天缩短至 10 天，堪称定制开发的‘新基建狂魔’。” 刘浏也以“云安全管理平台”这款产品为例，“基于川陀平台，该产品仅用三周时间就重构完成了旧版本耗时一年开发的功能点。”



再拿“好”来说。性能好，是提高产品竞争力的核心武器。奇安信集团副总裁、首席架构师兼鲲鹏平台负责人吴亚东表示，鲲鹏平台作为电信级网络操作系统，堪称网络和安全完美融合的用户态协议栈，它具备全功能、高性能、高可靠三大优势，从而助力产品连续 2 年中标中国移动防火墙集采及中标中国联通防火墙集采等项目。最终实现 2021 年鲲鹏平台产研人员人均创收超过 410 万元，同比激增约 40%，达到网络安全行业头部厂商的 2~3 倍，同时人均创造毛利 266 万元，同比增速更达 43.5%。

第三是“省”的维度。困扰网络安全行业最大的痼疾，就是“增收不增利”，而研发平台在降本增效方面效果明显。奇安信拥有多达 30 余款产品的庞大终端舰队，在业内遥遥领先，通过基于川陀平台的统一式量产，在保障高质量、低 bug 的前提下，成本下降达 2/3，“省”优势不言而喻。同样，通过鲲鹏平台的量产应用，同等规格性能下成本降低一半，让边界安全系列产品的性价比实现了倍增。使得边界安全产线 2021 年营收同比增长 47.4%，三倍于 15.8% 的网络安全行业平均增速（中国信通院数据）。而毛利同比增长 51.2%，实现了“增收更增利”。

面对“快”“好”“省”的“不可能三角”，奇安信以大禹、鲲鹏、川陀等代表的研发平台，努力实现三者兼顾。其最终目标，就是将研发工程师从重复造轮子的投入中解放出来，用更高效的乐高模式，开发出更优秀的产品，进而推动行业的发展和进步。



华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称 华云信安™ ）成立于2016年，是一家深耕于网络空间安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安™总部位于深圳，在广州、上海、武汉设有分支机构，公司核心团队来自奇安信、网易、华为、绿盟、思科等国际知名科技企业，具有深厚的网络安全技术实力和管理经验。

华云信安™目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安™凭借创新的网络安全产品体系、深厚的网络安全服务能力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、政务等领域的广大客户，提供专业优质的网络安全产品、网络安全解决方案和网络安全技术服务。

网络犯罪研究中心

华云信安·网络犯罪研究中心，是专注于打击网络犯罪的安全服务部门，致力于打击涉网新型犯罪领域的安全技术研究与产品研发，包括涉网犯罪案件技术支撑、网络诈骗案件技术支撑、涉众型经济犯罪案件技术支撑等，以攻防实验室和极牛技术社群组成创新型的安全研究团队，为国家及各省市公安机关提供高效专业的打击涉网犯罪情报分析服务和实战解决方案。

极牛攻防实验室

华云信安·极牛攻防实验室，由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028