内部发行 免费赠阅
出版物准印证号：京内资准字 2021- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

RSAC2022 安全的转型与未来 P12

P28
瑞兽白泽：一场持续和攻击者斗智斗勇的四年往事

P34
1 年走完 3 年路 汽车行业网络安全如何“ 弯道超车”？ 广汽乘用车交出一份答卷

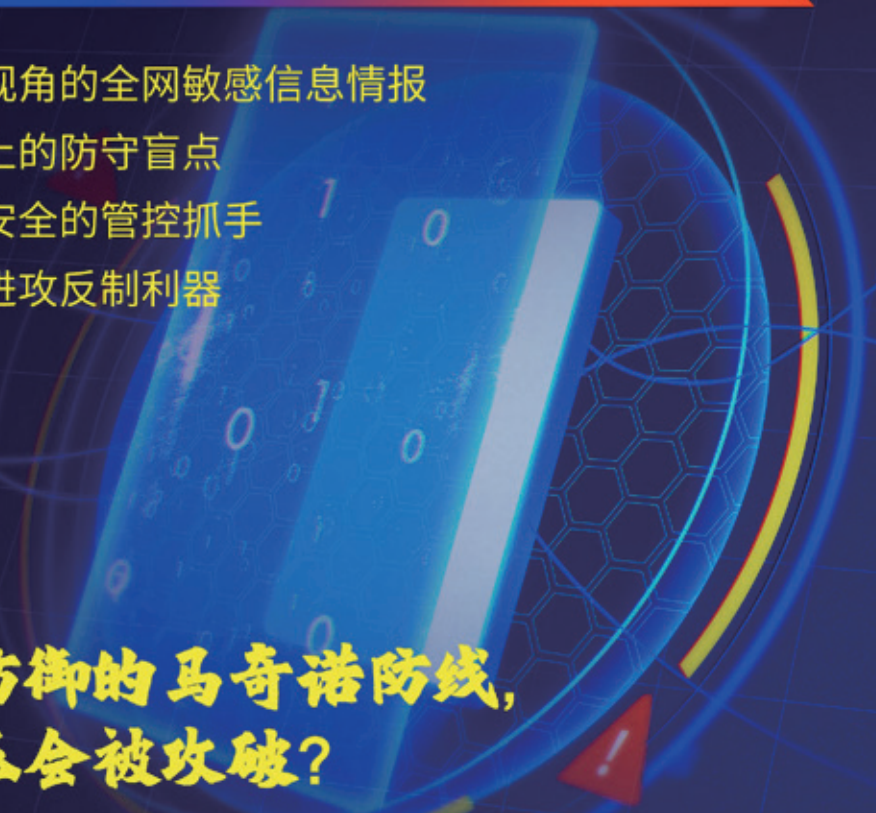
P38
你不是一个人在战斗

第18期
2022 年 6 月

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器



纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

安全的钟摆

疫情爆发以后，RSAC 会议首次开启线下模式，与高峰年份的 4 万人相比，今年 26,000 人的规模似乎略显缩水，但来自全球的创新技术和产品还是让与会者振奋。

与会议的缩水规模相比，网络安全行业实际上却正在迎来有史以来最高光的时刻：网络攻击处于历史最高水平，攻击者针对所有关键部门进行攻击。网络安全不再是竞争优势，而成为生存的必需品。过去数年中，安全解决支出的增长已超过其他 IT 细分领域。2021 年网络安全投资达创纪录的 264 亿美元，与比 2020 年相比，增长 2.4 倍。2022 年，全球网络安全预算预计同比增长 10 ~ 13%，而 IT 总预算同比增长 4 ~ 5%。

对 RSAC 与会安全主管的访谈显示，企业的安全预算没有减少。不过面对超强的攻击对手，组织除了采用创新技术防护供应链生态安全，以及不断变化的网络环境，加强公共机构与私营部门的紧密合作成为各方共识。

对于行业安全主管来说，安全自动化，提升风险洞察，以及量化安全风险是最迫切的需求。

因此，如同人类社会的钟摆定律一样，网络安全投资重点在经历了“预防”向“检测和响应”的转移后，再次出现转移：攻击面管理成为参观者最关心的问题。充分了解网络环境及安全态势，才能降低网络风险。

在某种程度上，网络安全行业处于军备竞赛中。对供应链、云基础设施和物联网网络的攻击持续增长，推动行业持续创新。让持续技术创新跟上攻击者的步伐，对于网络安全至关重要。

安全创新在重视技术的同时，显然不能将技术作为所有安全问题的解决方案，而不考虑人为因素。

美国国家标准与技术研究院 (NIST) 的计算机科学家 Julie Haney 认为，组织可以而且应该避免“给用户带来太多负担、不以以用户为中心”等网络安全陷阱。

她认为，可用性是实现有效网络安全的关键问题。有效性、效率和满意度则是可用性的三个核心原则，也即实现目标、支出合理、满足用户期望。这或许可以成为安全技术创新的尺度。

总编辑

2022 年 6 月 1 日

CONTEN

目录

安全态势

P4 | 非洲最大连锁超市遭勒索团伙敲诈，600GB 数据被窃取

P4 | Mirai 变种 Miori 僵尸网络在国内大规模传播，浙江受影响最严重

P4 | 数万个开源项目开发账户遭大规模泄露：超 7.7 亿条日志暴露

P5 | 意大利第五大城市遭勒索软件攻击，导致全城断网近一周

P5 | 富士康墨西哥工厂遭勒索软件攻击，业务运营受干扰

P5 | 南非总统的个人信贷数据泄露：该国已沦为“黑客乐园”

P6 | Windows SMB 拒绝服务漏洞安全风险通告

P6 | Linux Kernel eBPF 权限提升漏洞风险通告

P6 | Confluence 远程代码执行漏洞安全公告

P7 | 国内攻防演习 5 月态势：哪些薄弱点最易被利用?

P10 | 国家能源局修订两项电力行业网络安全政策公开征求意见

P10 | 网信办修订《移动互联网应用程序信息服务管理规定》发布施行

P10 | 市场监管总局、网信办发布《数据安全管理认证实施规则》

P11 | 《零信任参考体系架构》等 4 项国家标准公开征求意见

P11 | 美国参议员提出《健康和位置数据保护法》，治理数据交易乱象

月度专题

RSAC2022：安全的转型与未来

P12

数字化转型加速，网络安全成生存必需。网络安全行业面临持续创新需求，RSAC 有哪些明确的方向?

TS

攻防一线

P28

瑞兽白泽：一场持续和攻击者斗智斗勇的四年往事

安全之道

P34

1 年走完 3 年路 汽车行业网络安全如何“ 弯道超车”？ 广汽乘用车交出一份答卷

奇安信人

P38

你不是一个人在战斗

安全叨客

P44

数据安全大考
四大丢分细节，你都踩坑了吗?

研究报告

P54

APP 违规收集个人信息风险分析报告（2022 年第一季度）

奇安资讯

P48 | 齐向东出席 2022 数博会：数据安全是“东数西算”的底板工程
P48 | 奇安信举行百余场冬奥网络安全“零事故”经验分享会
P48 | 扩展云安全运营之路 奇安信云安全再获信通院认可
P49 | 奇安信与吐鲁番市合作共建吐鲁番市网络安全教育基地正式揭牌
P49 | 共筑发电行业网络安全“护城河” 奇安信与国电南自达成战略合作
P49 | 奇安信集团受邀亮相 RSAC2022 展示冬奥网络安全“零事故”创新
P50 | 奇安信公益基金会“眼明心安”项目启动 为西藏眼疾患儿点亮未来
P50 | 奇安信与达梦数据达成战略合作 打造国产数据库一体化产品
P50 | 2021 中国网站安全报告：11.5 万个网站被报告安全漏洞 14.6 万个
P51 | 奇安信集团与南京航空航天大学达成战略合作 打造安全协同创新中心
P51 | 圆满完成网络安全专项行动任务 奇安信获公安部感谢信
P52 | 奇安信获冬奥网络安全保障“表现突出单位”荣誉称号
P52 | 连续多年位居前列 奇安信安全隔离与信息交换系统市场份额持续扩大
P52 | 奇安信开源软件供应链安全技术应用方案获 2022 数博会“新技术”奖
P53 | 奇安信“95015”获数博会领先科技成果奖
P53 | 2022IT 市场权威榜单：奇安信获九项荣誉

《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
安全叨客主编：王梦琪
奇安资讯主编：陈　冲
研究报告主编：包世玉

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2021-L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2022 年 6 月 26 日
发行对象：奇安信集团内部

内部发行　免费赠阅

事件篇

非洲地区网络威胁形势日益严峻。最大连锁超市遭遇数据勒索攻击，多国受影响。南非总统个人信息泄露，有黑客团伙指责该国已经成为黑客乐园，任何人都能轻松绘制出南非数字基础设施分布。

非洲最大连锁超市遭勒索团伙敲诈，600GB 数据被窃取

据 BleepingComputer 6 月 15 日消息，非洲最大连锁超市 Shoprite 披露，近期遭遇了一起安全事件，部分国家的客户可能受影响，姓名、身份证号等信息泄露。勒索软件团伙 RansomHouse 声称对此负责，称已窃取 600GB 数据，要求支付赎金。RansomHouse 还毒舌“点评”了 Shoprite 差劲的安全意识，如用明文文本和原始图片保存大量个人数据。Shoprite 在非洲 12 个国家经营近 3000 家门店。

Mirai 变种 Miori 僵尸网络在国内大规模传播，浙江受影响最严重

据 CNCERT 6 月 14 日消息，国家互联网应急中心（CNCERT）和奇安信近期监测发现一个新的且在互联网上快速传播的 DDoS 僵尸网络 Mirai_miori，传播方式主要为弱口令爆破及 1 day 和 N day 漏洞。监测分析发现，今年 4 月 6 日至 6 月 6 日 Mirai_miori 僵尸网络日上线境内肉鸡数最高达到 1.1 万台，累计感染肉鸡数达到 4.4 万。肉鸡排名前三位的省份为浙江省（37.2%）、云南省（10.9%）和河南省（6.2%）。

数万个开源项目开发账户遭大规模泄露：超 7.7 亿条日志暴露

据 TheHackerNews 6 月 14 日消息，安全研究人员发现，流行的持续集成开发工具 Travis CI 存在 API 漏洞，导致大量开发账户敏感数据暴露，超过 7.7 亿条 Travis CI 免费版用户日志数据以明文方式泄露，其中包含大量敏感机密信息（开发令牌、云服务凭证等），包括 Github、Docker 的数以万计的开源项目开发账户受到影响。Travis CI 是一种被称为持续集成的越来越流行的敏捷开发工具，通常缩写为 CI，它使开发和测试代码变更的过程自动化，已经成为现代开发和云原生应用程序管道的重要组成部分。

俄罗斯知名媒体电台遭黑客攻击：奏响乌克兰国歌

据 HackRead 6 月 9 日消息，俄罗斯生意人报电台（Kommersant FM）的播报在 8 日出现中断，转而

播放乌克兰国歌和其他反战歌曲。之后，广播很快中止。官方发布声明称，遭到黑客攻击，将尽快恢复播报。被黑客篡改的是生意人报电台的午间播报节目，该电台是俄罗斯知名私营媒体生意人报的广播版。英媒 BBC 记者 Francis Scarr 在推文中提到，当时生意人报电台播放了乌克兰著名爱国民歌、曾经的国歌《哦，草地上的红荚蒾》。

意大利第五大城市遭勒索软件攻击，导致全城断网近一周

据 BleepingComputer 6 月 9 日消息，意大利南部巴勒莫市 3 日（周五）遭受网络攻击，导致全城断网、IT 系统瘫痪近一周，给当地旅游业和城市运营带来灾难性影响。据当地媒体报道，受影响的系统包括公共视频监控管理、警务及市政府的所有（网络）服务。市民的出生证明、结婚证明及户籍和居住证明等文件都无法办理或变更，也无法使用网络进行交流或获取服务。Vice Society 勒索软件组织声称对此负责。巴勒莫拥有约 130 万人口，是意大利人口第五大城市。

富士康墨西哥工厂遭勒索软件攻击，业务运营受干扰

据 BleepingComputer 6 月 2 日消息，富士康公司确认其位于墨西哥的一家生产工厂在 5 月下旬受到勒索软件攻击的影响。富士康没有提供任何有关攻击者的信息，但勒索软件组织 LockBit 声称对此负责。被攻击的富士康工厂位于墨西哥蒂华纳，是美国加州消费电子产品的重要供应中心，被认为是一个战略设施。富士康在官方声明中表示，勒索软件攻击对其整体运营的影响较小，工厂正在逐步恢复。这不是富士康第一次被勒索攻击，此前 2020 年 12 月，公司另一处墨西哥工厂也遭遇过类似事件。

南非总统的个人信贷数据泄露：该国已沦为“黑客乐园”

据 MyBroadband 5 月 29 日消息，黑客团伙 SpiderLog$ 公开了南非总统 Cyril Ramaphosa 自 2000 年在国内四大银行之一的贷款详细记录，这批数据来自另一黑客团队，为其入侵征信机构 TransUnion 所窃取。SpiderLog$ 称，南非已经成为“黑客乐园”，任何人都能轻松绘制出南非数字基础设施分布，甚至包括国防 / 国安等敏感系统。此次曝光使得大众意识到了南非信息系统的显著漏洞，特别政府 / 国防 / 国安等部门的系统安全性。

印度第二大航司遭勒索软件攻击，大量乘客滞留在机场

据 BBC 5 月 25 日消息，印度第二大航司香料航空（SpiceJet）遭勒索软件攻击，内部系统受影响离线，导致多个航班延误数小时，大量乘客滞留在机场。此次针对香料航空运营体系的网络攻击，直接影响到飞往印度及海外各国的众多乘客，数小时的延误将转化为巨大的经济损失。这是近期又一起网络攻击影响航班运转事件，此前 4 月，加拿大老牌航空公司阳翼航空遭网络攻击，致使航班严重延误近一周时间，大量乘客在机场滞留多日。

俄最大银行遭到最严重 DDoS 攻击，普京称正经历“信息空间战争”

据 BleepingComputer 5 月 20 日消息，俄罗斯最大银行联邦储蓄银行（Sberbank）官网披露，在 5 月 6 日成功击退了有史以来规模最大的 DDoS 攻击，峰值流量高达 450 GB/ 秒。该行安全负责人表示，俄罗斯网络安全发生了结构性转变，过去 3 个月来企业遭受的网络攻击呈现爆炸性增长，攻击实力大幅提升。普京称俄罗斯正在遭受“信息空间战争”，他提出了三项关键任务，以确保俄关键信息基础设施安全。

漏洞篇

5 月末，多家安全公司披露，微软支持诊断工具远程（MSDT）的代码执行漏洞（代号 Follina，CVE-2022-30190）遭到多个攻击团伙在野滥用，微软在 6 月补丁日正式发布修复补丁。

Windows SMB 拒绝服务漏洞安全风险通告

6 月 16 日，奇安信 CERT 监测到 Windows SMB 拒绝服务漏洞细节及 PoC 在互联网公开，Windows SMB 在处理请求的过程中存在空指针引用缺陷，未经身份验证的远程攻击者可通过向 Windows 域控制器发送特制请求来利用此漏洞，从而导致目标系统拒绝服务。经验证，此漏洞公开的 PoC 稳定有效，未经身份验证的攻击者可利用此漏洞攻击默认配置的域控制器，攻击普通 Win10、Win11 主机用户需要经过身份认证。值得注意的是，微软已于 2022 年 4 月份修复了此漏洞，并于 6 月补丁日公开。

Linux Kernel eBPF 权限提升漏洞风险通告

6 月 13 日，奇安信 CERT 监测到 Linux Kernel eBPF 权限提升漏洞 (CVE-2022-23222) 的 PoC 在互联网上公开。由于内核在执行用户提供的 eBPF 程序前缺乏适当的验证，攻击者可利用这个漏洞提升权限并在内核上下文中执行代码。要利用此漏洞，攻击者首先需要获得在目标系统上执行低权限代码的能力。大多数 Linux 发行版本默认禁用非特权运行 BPF 程序。经验证，此漏洞 PoC 有效。鉴于此漏洞影响范围较大，危害较大，建议客户尽快做好自查及防护。

Confluence 远程代码执行漏洞安全公告

6 月 3 日，国家信息安全漏洞共享平台（CNVD）收录了 Confluence 远程代码执行漏洞（CVE-2022-26134）。未经身份验证的攻击者利用该漏洞可在目标服务器执行任意代码。目前，漏洞细节信息尚未公开，厂商已发布漏洞缓解建议，暂未发布修复补丁。Confluence 是一款专业的企业知识管理与协同软件，常用于企业 wiki 的构建。

微软支持诊断工具 MSDT 远程代码执行漏洞安全公告

5 月 31 日，国家信息安全漏洞共享平台（CNVD）收录了微软支持诊断工具远程（MSDT）代码执行漏洞（CVE-2022-30190）。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，漏洞利用代码已公开，且已出现在野利用的情况。微软公司已发布漏洞缓解指南，CNVD 建议受影响用户按照临时防范措施缓解漏洞攻击威胁。

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

一、本月演习整体情况

2022 年 5 月，奇安信 Z-TEAM 团队共承接攻防演习服务 36 场，其中行业级攻防演习 2 场，省级攻防演习 1 场，地市级攻防演习 10 场，客户自主攻防演习 23 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	44	58	67	92	21	112	237	2491

二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，覆盖目标面比较广，涵盖了政务、金融、电力、互联网、企业等目标，客户存在的安全问题主要涉及互联网侧业务系统组件存在历史漏洞、内部人员对钓鱼攻击防范意识不足、内网功能区缺乏安全隔离、内网口令复用及弱口令普遍等。具体情况如下：

1、历史漏洞仍是实现外部渗透的主要突破口

本月任务中针对多行业不同目标网络，漏洞利用仍是实现外部渗透的主要突破口。被攻陷目标互联网侧应用漏洞以平台组件历史漏洞为主，如外部应用中未授权访问、Shiro 反序列化、Weblogic 反序列化、SQL 注入、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、对爆出漏洞的组件未及时升级更新造成的，这些问题的存在致使目标网络防线有随时被攻破的风险。

2、钓鱼攻击具有较高成功率

本月任务中目标的核心业务网络安全防护相对严密，针对外部系统难以直接突破的情况，钓鱼攻击成为了另一种外部突破的主要实现手段，并且具有较高的成功率。钓鱼攻击主要选择目标内部网络安全意识相对薄弱的人员。通过冒充同事或客户身份，以内部业务交流或客服咨询为由发送木马打开突破口。

3、访问策略缺陷是重大安全隐患

本月任务中发现多个行业目标的外部业务系统存在未授权访问的问题，可以通过未授权访问，直接访问这些外部业务系统后台，进而可以利用访问权限执行后台命令及获取后台配置文件、数据库等敏感信息。未授权访问多因对外部接入的安全配置或权限认证相关策略设置存在缺陷，导致对外部用户的访问地址、访问权限缺乏限制，为网络安全埋下了重大安全隐患。

4、 弱口令是内网严重安全隐患

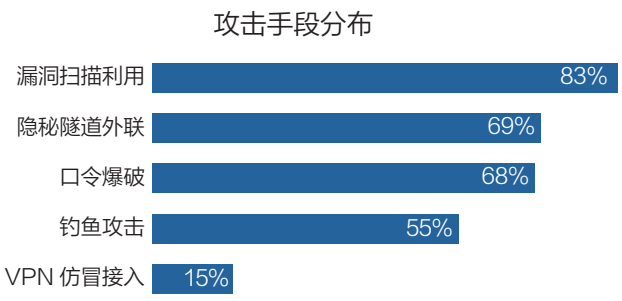
本月任务中口令爆破主要通过弱口令和口令复用实现，互联网侧口令爆破很少成功，在目标内网则成功率很高，是内网横向拓展的主要手段。通过搜集目标网络中各种设备的默认口令、弱口令来分析其密码组合规律，从而实现对目标内网相关网络应用、安全设备和服务器的快速爆破。

5、目标网络缺乏纵深防护机制

本月任务中目标网络普遍缺乏纵深防护机制，存在互联网侧服务器和核心内网未进行边界隔离的情况，内网的安全设备部署缺少功能域划分、vlan 隔离等措施。主要表现为突破互联网侧应用服务器后，可直接对内网业务进行扫描探测，很容易实现对内网核心业务的拓展渗透。

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，多采用互联网侧系统漏洞利用和钓鱼攻击等方式进行，内网横向拓展则以隐蔽隧道外连、内网漏洞利用、弱口令和口令复用等手段为主。使用的主要技术手段分布如下：



1、漏洞扫描利用

本月任务中漏洞利用集中在互联网侧业务系统和门户网站，以未授权访问、组件反序列化、任意文件上传

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缺乏应对等问题。

2、隐蔽隧道外联

本月任务中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、隧道技术等手段实现对内网的渗透拓展。以金融目标为代表的网络功能区划分严格、核心业务隔离措施完善的关键领域业务网络，则需要两到三层的通道转发实现对目标核心业务内网的渗透拓展。

3、口令爆破

本月任务中口令爆破主要体现在弱口令和口令复用，目标内网横向拓展过程中弱口令、口令复用则较为普遍，主要原因是目标网络缺乏对弱口令和通用口令的统一治理，没有对账号口令设置和使用进行安全规范要求，如对密码复杂度提出要求、禁止使用通用账号口令、账号口令定期更新等。

4、钓鱼攻击

本月任务中针对不同目标，根据其业务特点，在钓鱼目标选择、钓鱼木马素材及话术组织方面均做了针对性的准备工作。比如，针对客服人员和人事部门目标，采取业务咨询、第三方合作或网络应聘等方式；针对管理人员和职能部门目标，则采取业务申请或报告提交等方式进行钓鱼突破。

三、典型攻击手段实现案例

1、外部漏洞利用

（1）某电力目标招聘官网存在任意文件上传漏洞，通过任意文件上传漏洞获取该机器上的登录凭证，登录后控制 96 台主机、2 台数据库、5 个 Web 后台。

（2）某目标域控存在 CVE-2021-42287、CVE-2021-42278 漏洞，通过该漏洞获得主域控权限，并抓取域管密码获取到域控权限，可接管控域终端 1912 台。

（3）某目标管理平台系统存在 Shiro 远程命令执行漏洞，通过漏洞利用获取该系统后台服务器控制权限。

（4）某目标综合服务平台系统存在 CVE-2022-22947 漏洞，通过该漏洞获取到服务器权限。

2、口令爆破

（1）某目标动态仓储系统存在弱口令，可通过口令爆破直接登录该系统后台，获取后台管理权限。

（2）某目标数据库存在弱口令漏洞，通过漏洞利用获取到数据库权限，可查看某部门人员姓名、身份证、电话、地址等敏感信息。

（3）某目标内网域控服务器存在弱口令漏洞，通过弱口令获得域控权限后，可同时控制内网域控、域内主机和域内用户等。

（4）某目标 Web 控制台存在默认口令漏洞，通过该漏洞登录 Web 控制台后，可对监控主机下发脚本执行命令等。

3、钓鱼攻击

（1）通过浏览某目标政务外网 VPN 页面发现页面上可查询到 VPN 问题反馈人员的电话号码，通过微信搜索加为好友后，发送带有钓鱼木马的“VPN 申请单”，用户成功点击上线。

（2）通过搜索 QQ 群，申请加入某目标的 QQ 群后进行定点人员钓鱼，使用 QQ 临时会话发送木马文件，利用文件名诱导相关人员打开，进行钓鱼攻击，成功获取主机终端控制权限。

（3）以邮箱异常处理问题为由，对某目标的技术支持人员发送木马文件进行钓鱼攻击，成功上线并获取某系统服务器权限。

（4）通过对某目标内网投资系统运维人员进行水坑钓鱼，成功上线 4 台个人终端，并获取到内网 5 台数据库权限、2 台服务器权限、2 台 Web 后台权限。

政策篇

国内，国家能源局修订《电力行业网络安全管理办法》，首次要求设立首席网络安全官，网络安全预算不低于信息化总投入的5%；

国际上，美国商务部发布规定，要求向中国政府相关的最终用户进行漏洞披露等活动，需申请许可。

国内

国家能源局修订两项电力行业网络安全政策公开征求意见

6月15日，国家能源局公布了《电力行业网络安全管理办法（修订征求意见稿）》《电力行业网络安全等级保护管理办法（修订征求意见稿）》，公开征求意见。《电力行业网络安全管理办法（修订征求意见稿）》要求，电力行业关键信息基础设施运营者的主要负责人对关键信息基础设施安全保护负总责，要明确一名领导班子成员（非公有制经济组织运营者明确一名核心经营管理团队成员）作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作。

网信办修订《移动互联网应用程序信息服务管理规定》发布施行

6月14日，国家互联网信息办公室发布新修订的《移动互联网应用程序信息服务管理规定》。新《规定》要求，应用程序提供者和应用程序分发平台应当履行信息内容管理主体责任，建立健全信息内容安全管理、信息内容生态治理、数据安全和个人信息保护、未成年人保护等管理制度，确保网络安全，维护良好网络生态。新《规定》自2022年8月1日起施行。

市场监管总局、网信办发布《数据安全管理认证实施规则》

6月9日，市场监管总局、网信办宣布开展数据安全管理认证工作，并发布《数据安全管理认证实施规则》。《实施规则》以《信息安全技术 网络数据处理安全要求》及相关标准规范为认证依据，规定了对网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等处理活动进行认证的基本原则和要求。《实施规则》明确，认证模式为“技术验证+现场审核+获证后监督”。认证证书有效期为3年。

《“中国+中亚五国”数据安全合作倡议》发布

6月8日，“中国+中亚五国”外长第三次会晤举行，会晤通过了《“中国+中亚五国”数据安全合作倡议》。倡议提出，在遵守国内法和国际法基础上，各方建议各国及各主体：就防范全球信息安全所面临的挑战和威胁，保障数据安全，开展协调行动与合作；应以事实为依据，全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应链开放、安全、稳定；各国应尊重他国

主权、司法管辖权和对数据的安全管理权，未经他国法律允许，不得直接向企业或个人调取位于他国的数据。

《零信任参考体系架构》等 4 项国家标准公开征求意见

综合消息，近一个月来，信安标委发布了 4 项国家标准的征集意见稿文件。包括《信息安全技术 互联网平台及产品服务隐私协议要求》《信息安全技术 零信任参考体系架构》《信息安全技术 移动智能终端的移动互联网应用程序（APP）个人信息处理活动管理指南》《信息安全技术 应用商店的 APP 个人信息处理规范性审核与管理指南》。

美国参议员提出《健康和位置数据保护法》，治理数据交易乱象

6月15日，美国参议员Elizabeth Warren提出了《健康和位置数据保护法》法案要求，禁止数据经纪人出售或传输位置数据和健康数据，并要求联邦贸易委员会颁布规则，在 180 天内实施该法律。同时，对符合 HIPAA 的活动、受保护的第一修正案言论和有效授权的披露作出例外规定。通过授权联邦贸易委员会、州检察长和受害者提起诉讼以执行法律规定，确保该法案的规定得到强有力的执行。

美国商务部发布《信息安全控制：网络安全条目》，强化漏洞信息管控

5 月 26 日，美国商务部工业和安全局发布《信息安全控制：网络安全条目》细则最终版，并生效执行。该文件要求，美国实体进行漏洞披露等跨境网络安全活动时，如最终用户与 D 组国家（包括中国）的政府有关，须申请许可才能发送潜在网络漏洞等信息。非政府用户不受影响。微软公司认为，这一审查制度将阻碍与安全研究人员和漏洞奖励计划参与者的跨境合作。

意大利发布《2022 至 2026 年意大利国家网络安全战略》

5 月 25 日，意大利政府发布《2022 至 2026 年意大利国家网络安全战略》及《2022 至 2026 年意大利国家网络安全战略实施计划》，公开了意大利未来几年的网络态势路线图。《战略》提出三大基本目标：通过旨在管理和减轻风险的系统性方法保护国家战略资产，通过部署增强的国家监控、检测、分析和响应能力及启动涉及国家网络安全生态系统中所有利益相关者的流程加强响应，有意识和安全地发展能够响应市场需求的数字技术、研究和产业竞争力。

俄罗斯通过《保护关键信息基础设施国家政策基本原则》草案

5 月 20 日，俄罗斯联邦安全委员会会议通过了《保护关键信息基础设施国家政策基本原则》草案。该草案定义了在信息技术部门实施国家政策的目的和机制，特别是计划通过使用国产信息技术提高关键信息基础设施的安全水平。草案决定运用国家力量组织研发人工智能、量子计算技术，创建富有竞争力的电子元件基地和高科技生产区，并开发用于检测、预防和消除网络攻击后果的国家信息系统。此外，草案还将特别关注信息安全领域的专家及技能培训。

RSAC 2022：安全的转型与未来

数字化转型加速，网络安全成生存必需。网络安全行业面临持续创新需求，RSAC 有哪些明确的方向？

RSAC 2022：安全的转型与未来

作者 虎符智库研究员 包世玉 李建平

Talon Cyber Security 夺得 RSAC 创新沙盒冠军，让不少业内人士出乎意料，这其实代表着现实的真实需求与未来方向。RSA 公司 CEO Rohit Ghai“唯一的永恒”主题演讲，诠释了在不断变化的外部环境下，安全行业主动转型与变革的必要性。

普及的新兴技术、不断扩大的攻击面、频发的漏洞，对安全行业来说，唯一不变的是变化。行业推进转型转变的经验将决定下一个常态。

安全的转型与未来

RSA 公司 CEO Rohit Ghai 在演讲“The Only Constant”中为主题“转型”（Transform）做出了解读。Transform 是去年年中确定的 2022 年 RSAC 主题，在当前引起了广泛共鸣。

在开幕主题演讲中，Rohit Ghai 鼓励网络安全领导人主动进行转型——以达到比以往更强大、更好的状态。“安全转型需要重新定位我们的思维。”

Rohit Ghai 提出了三大推动转型的建议：重新思考身份；真相很重要；便利性不应牺牲安全。他认为未来应弄清楚如何以身份为中心进行访问，而不依赖传统访问机制（即密码），这是未来的方向。此外，他认为，保护信息的真实性将成为未来数年网络安全的关键任务。假新闻和错误信息已成为摧毁机构的有力武器。最后，他呼吁该行业放弃其旧的“教条”，不应为了便利而放弃安全性。

RSA 公司 CEO Rohit Ghai 在主题演讲中呼吁行业转型

RSAC 的“转型”主题，反映出机构在面临疫情流行加速的数字化转型所面临的巨大安全挑战。疫情之下，使用云服务的数字化转型成为企业生存的关键。网络安全比以往任何时候都更加重要，网络安全领导者需要进行转型，以保护通过云交付的应用。

实现转型、解决安全挑战的答案就在于创新，创新让蛋糕变大并带来新的好处。

网络安全行业正出现新的变化。业界不断寻找新的技术方法来改善网络安全状况或减少攻击次数。安全投资从强调“预防”转向“检测和响应”，现在这一重点正在再次转移。

首席安全官发现，要减少事件数量和团队负担，需要更好地了解和管理攻击面。现在业界对预防或“威胁与攻击面管理”重新产生了兴趣（Gartner《2022 年安全运营入门》）。在 RSAC 2022 上，攻击面管理是许多参观者最关心的问题。行业客户与安全同行强调考虑由外而内的外部攻击面管理 (EASM) 和网络资产攻击面管理 (CAASM)，来获得目前缺乏的安全可见性。

IBM 收购外部攻击面管理 (EASM) 领域领导厂商 Randori 可以反映出这种趋势。对攻击面和网络资产管理兴趣的增长表明，安全领导者已认识到，要降低网络风险，需要更好地了解网络环境及安全态势。但这并不意味着对安全响应投资不再重要，它与攻击面管理相辅相成。

思科执行副总裁兼安全与协作总经理 Jeetu Patel 表示，“我们需要确保对漏洞管理采取基于风险的方法。对入侵事件的处理，不是依据发生的时间，而是依据构成的风险量。”

业内人士认为，安全产品的创新，应该提高整个软件生命周期的效率，帮助安全团队成为转型的推动者，而不是阻碍者。例如，减少部署到云端的代码漏洞数量，并在应用运行时快速响应出现的问题。

攻击者的速度并未放慢

与会业界人士认为，在某种程度上，我们处于网络军备竞赛中。对供应链、云基础设施和物联网网络的攻击持续增长。SolarWinds 攻击与 Log4j 漏洞等重大安全事件表明：攻击的频率和规模不断增加。

根据 Sophos 在 RSAC 发布的《2022 活跃攻击者报告》，入侵者停留时间比 2021 年增加了 36%，中位数从 11 天增加到 15 天。近一半 (47%) 的攻击是漏洞被利用的结果。例如，ProxyLogon 和 ProxyShell 等容易被利用的漏洞占据显著位置。此外，今年主要趋势是利用面向外部服务的漏洞进行初始访问。这不仅包括 ProxyLogon 和 ProxyShell 漏洞，还包括影响 VPN 和防火墙部署的漏洞。另一个趋势是攻击者依赖通过远程服务进行初始访问。由于缺乏多因素身份验证 (MFA)，攻击者能在不被发现的情况下侵入系统。

索软件攻击几乎无处不在。大量受害者成为勒索软件犯罪分子的牺牲品。这种永远存在的威胁正在发生战术上的一些转变，但没有减弱的迹象。《2022 年度勒索软件状况报告》发现，勒索软件攻击的影响巨大。支付超 100 万美元赎金的受攻击组织增长了 3 倍。

SANS 研究所发布的最危险攻击技术简报是 RSAC 上最受欢迎的活动之一。SANS 研究所专家称，被窃取身份验证令牌、云滥用和易受攻击的备份都是企业在未来需要解决的问题。

以下是 SANS 研究所今年描述的五种最危险的攻击技术：

- **攻击在云端。**随着组织越来越多地使用基于云的服务来存储数据、在互联网上提供应用及开展业务运营，攻击者不仅将云服务作为攻击目标，还利用云产品作为攻击平台。

SANS 研究所情报总监 Katie Nickels 建议组织注意正常的云行为，并寻找潜在的异常值来发现风险。

- **多重身份验证绕过。**多因素身份验证 (MFA) 是一种非常强大的安全力量，但它越来越多地被攻击者滥用。攻击者能够通过几种不同的方法绕过 MFA。Nickels 建议组织有多种 MFA 备份选项来限制风险。
- **备份漏洞。** SANS 研究所研究主任 Johannes Ullrich 认为备份是一种潜在的危险攻击媒介。备份系统

可以访问整个企业的端点和服务器，对攻击者来说是有吸引力的目标。攻击者正在寻找备份系统中的已知漏洞进行利用。Ullrich 建议组织要勤于修补，确保对备份系统的访问是安全的。

● **跟踪软件和蠕虫仍有风险。**SANS 研究所高级讲师 Heather Mahalik 警告说，跟踪软件和蠕虫仍然是用户关注的问题。随着飞马软件（Pegasus）的出现，用户跟踪软件 Stalkerware 再次成为一大安全问题。

在防范跟踪软件和蠕虫方面，Mahalik 建议坚持基本的网络安全要求，包括定期修补、备份和反恶意软件工具。她还建议用户有效地使用多因素身份验证。

● **风险来自太空 。**SANS 研究所首席课程主任 Rob Lee 警告说，新出现的风险来自于非地面互联网通信。在俄乌冲突中，最早攻击目标之一是地面互联网基础设施。马斯克提供星链互联网服务后，攻击者将越来越多地瞄准支持互联网和地面系统的卫星系统。

关基防护需要联合防御模式

在 RSAC 2022 的主题演讲中，美国联邦政府的网络安全领导人鼓励政府和非政府实体之间开展更多合作。

网络安全和基础设施安全局 (CISA) 主管伊斯特利（Jen Easterly）表示，“ 2022 年的网络安全格局看起来并没有太大不同，但确实看到国家黑客和网络犯罪分子变得更加老练。网络安全成为国家安全的当务之急。”她强调将私营和公共部门联合打击恶意网络行为的重要性，因为私营部门通常“拥有更多的可见能力”。SolarWinds 事件不是由美国政府发现的，而是由安全企业 Mandiant 发现的。”

美国国家网络总监克里斯 · 英格利斯表示，这种合作“不是锦上添花，而是锦缎本身。”美国国家安全局 (NSA) 网络安全局局长罗伯特 · 乔伊斯表示，俄乌冲突之后，恶意网络活动增加，进一步证明了在联邦机构和关键基础设施部门的网络安全工作上加倍努力的必要性。

私营部门的合作伙伴关系是建立网络防御的必要组成部分。美国公共部门与私营机构的伙伴关系的重大举措是 2021 年 8 月成立联合网络防御合作组织 (JCDC)。JCDC 是一项开始领导美国网络防御计划发展的倡议。成员包括联邦机构、企业、州和地方政府等。

CISA 主管伊斯特利认为私营安全机构具有更强可见能力。

长期以来，美国政府官员一直主张在网络安全方面建立更强大的公私合作伙伴关系。2022 年与私营部门的协调与合作有所增加。伊斯特利表示：“自从俄乌冲突以来，我们已经开始一起工作、规划和实施运营协作模式，通过技术工具 Slack 近乎实时地共享信息。我们以政府和私营部门以前从未做过的方式真正分享见解、信息和分析。”

SolarWinds 公司 CEO Sudhakar Ramakrishna 呼吁政府和行业在安全情报共享方面加强合作，并承诺派驻员工与美国网络安全和基础设施安全局 (CISA) 密切合作。

Ramakrishna 说，能够有效应对不断变化的威胁形势的唯一方法，是加强公共部门和私营部门之间的真正伙伴关系。 他呼吁“整个软件行业加入这一努力，美国每一家软件或技术公司都委派一名全职员工在 CISA 的指引和指导下工作，以支持威胁情报和信息分享。”

白宫国家网络主管 Chris Inglis 表示，这种合作关系下，不同机构的技能能够相互补充，从攻击者的角度来看，“必须击败所有人方能击败我们中的每个人。”

思科安全与协作执行副总裁 Jeetu Patel 则强调网

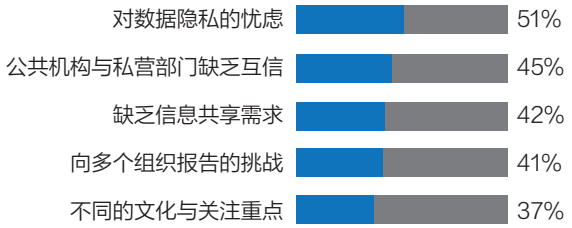
络安全贫困线的理念：由于软件依赖性、共享数据、混合工作等原因，不同机构更加相互联系和依赖，将所有企业提升到安全贫困线以上很重要。

“我们应该考虑保护整个供应链和生态系的安全，而不是单个组织。” 这延伸到为非营利组织和非政府组织提供免费或低成本安全服务，以及大公司帮助小型机构改善安全状况。

与会嘉宾强调，实现公共机构与私营企业的有效合作，建立彼此间的“信任”尤为重要。数据隐私问题和信任问题影响了这种合作伙伴关系的效力。根据 MeriTalk 和 RSAC 的研究，93% 的网络安全决策者认为政府与私营机构合作对国家安全防护至关重要，但只有 34% 的人认为非常有效。92% 的机构积极与合作伙伴共享信息，但 43% 的机构认为，私营部门与政府共享信息比反过来更常见。高达 69% 的网络安全决策者表示，其所在机构对网络安全信息共享保持沉默。

大多数与会者同意，以政府为主导的伙伴关系是前进的方向，但在最佳方法上却没有共识。但改善公共机构和私营部门间的沟通和信任，无疑是降低网络安全风险的关键。

公共机构与私营部门的合作障碍



创新是持续的需求

RSAC 第一天，Talon Cyber Security 夺得了创新沙盒的冠军，让不少业内人士都觉得出乎意料。TalonWork 专为企业打造安全的企业级浏览器：为浏览器提供身份验证、数据丢失预防、零信任控制等原生功能，使组织能够简化其安全防护。

Talon 仿照谷歌提出的浏览器即 OS 的概念，打造出的安全浏览器，其创新点在于加入了上网行为管理等功能，同时为一些线上编辑的文档进行加密处置等。

Talon 并不是唯一一家扩展对安全未来理解的初创公司。本届 RSAC 上另一关键主题是安全工具整合。ESG 高级首席分析师 Jon Oltsik 的新研究表明，组织正在朝着产品集成和多产品安全的方向发展。工具过载和人才短缺将使安全企业在端到端解决方案和安全自动化中脱颖而出。

目前每个安全需求都有单点解决方案，给安全从业者带来一系列新挑战。在过去几年中，CISO 对网络安全工具进行大量投资，给安全运营团队造成信息过载。投资太多不同的工具也给安全团队造成潜在的信息孤岛风险。

安全团队不可避免地必须集成各种工具，来实现全面的安全策略。当务之急是整合、连接和自动化孤立的安全解决方案，以帮助安全团队将时间和精力集中在最高优先级的威胁上。

在本届 RSAC 上，扩展检测响应 (XDR) 得到许多安全人员的关注。扩展检测响应 (XDR) 集成 SIEM、EDR 和 SOAR 解决方案，可连接和分析不同来源的数据，可以将安全工具统一到有效的威胁检测、调查和响应 (TDIR) 工作流程中。扩展检测和响应 (XDR) 为企业整合供应商提供了可行的路线图。

网络安全正迎来有史以来的最高光时刻。网络攻击处于历史最高水平，攻击者针对所有关键部门进行攻击。网络安全不再仅仅是组织的竞争优势，而是生存的必需品。

过去数年中，安全解决支出的增长已超过其他 IT 细分领域。根据 Pitchbook 的数据，2021 年网络安全投资达创纪录的 264 亿美元，比 2020 年增长 2.4 倍。2022 年，全球网络安全预算预计将同比增长 10~13%，而 IT 总预算同比增长 4~5%。

面对激增的安全支出，我们需要思考全球知名安全专家 Mikko Hypponen 在接受采访时的发言：复杂性是安全的最大敌人。代码越多，错误就越多，漏洞就越多。我们应该降低复杂性，但现在这并没有发生，而且恰恰相反。

RSAC 十大热点议题解读

作者 乔思远　奇安信战略研究中心、虎符智库专家

RSAC 2022 年以“转型”（Transform）为主题，被认为是去年主题（Resilience，弹性）的延伸和拓展。从弹性到转型，RSAC 的主题变化透露出网络安全产业的持续变革。

RSAC 2022 的 170 余个主题演讲，主要围绕 10 大热门主题，其中包括：数据与隐私安全（热度 14 ）、身份安全与零信任（热度 14）、软件供应链安全（热度 10）、勒索软件（热度 10）、AI 安全（热度 10）、威胁分析及狩猎（热度 10）、风险管理（热度 9）、云安全（热度 6）、物联网及工业安全（热度 6）、基础设施安全（热度 4）。

从本届 RSAC 的热点议题，可以看出网络安全的多个细分领域都在发生变革。

1 数据与隐私安全

数据与隐私安全是近 5 年来的热点议题。随着数字经济的发展和数据流通需求的增长，其热度持续升高。数据与隐私安全融合了传统安全技术应用和创新技术应用，产生了新的需求和应用场景。数据治理、隐私计算、隐私合规成为数据安全的创新驱动力。

本届 RSAC 的数据安全议题集中在数据保护，如云上行业（如医疗）数据保护、企业数据保护、数据本地化保护政策，以及政府数据交易与授权访问等。在隐私安全方面，热点议题则集中在如何保障基础设施（如 5G）、设备（如汽车），以及应用（如 AI、区块链）的隐私安全方面。

具有代表性的数据安全议题包括：

在“云安全：如何保护云上医疗数据”的议题中，专家以 AWS、Azure 和 DevOps 平台为例，将云上医疗数据包括概括为三点：（1）安全设计，包括身份验证、DevOps、标准、流程。（2）安全执行，包括通道、扫描、策略、受限访问角色。（3）安全运营，包括环境扫描、可用性管理和补丁管理等。最后，专家提出了三条建议：（1）使用云原生配置控制工具控制安全性和成本。(2)通过代码使基础设施和通道民主化。（3）实施透明的 DevOps 文化。

在“让企业员工保护高价值的数据”的议题中，专家从企业内部风险的视角，提出改变了内部风险的 3 个关键驱动因素：（1）数字化转型正在改变我们的合作方式；（2）知识型工作者随时随地展开工作；（3）人们正在频繁换工作，比以往任何时候都快。因此，从控制企业内部风险的角度保护高价值数据，需要做到 3 个 T：透明度（Transparency）、培训（Training）、技术（Technology）。

在“你能抓到我么：保护 5G 中的移动用户隐私”议题中，来自可信连接联盟（TCA）的专家关注的重点围绕国际移动用户身份 (IMSI) 的安全漏洞，以及保障用户身份隐私的方法，提出基于 SIM 卡的加密是唯一可行的方法，包括消费者和工业物联网用例。

在“隐私和区块链悖论”议题中，专家比较了区块链的优点与劣势，提出了区块链用于隐私保护及 GDPR 合规的四个注意事项：（1）一项技术和一项法规——数字世界中的隐私并非仅靠技术就能解决的问题。在技术方面，区块链正在通过在食品信托、集装箱、贸易融资和国际支付等不同领域提供价值的网络取得巨大进步。 尊重数据和交易的隐私是这些项目的核心。（2）起点相反，但基本原则相同——区块链和 GDPR 共享数据隐私的共同原则。 两者都希望监督我们自己的数字私人数据交易和支付（在比特币的情况下），或在 GDPR 的情况下需要与他人共享的个人数据。（3）公共网络中的隐私——隐私并不一定意味着用户需要一种私有区块链网络方法，可以在 GDPR 框架下实现满足公共网络隐私需求的区块链网络。（4）删除权——GDPR 要求之一是个人要求组织及时删除的权利，拥有他们的个人数据以完全删除该数据。

2 身份安全与零信任

身份安全是传统的赛道，零信任理念和云业务应用的发展为身份安全注入新的活力。

随着零信任框架和谷歌零信任应用的出现，零信任成为身份安全领域的新理念与创新热点。随着云应用的发展，云访问安全成为热点。疫情下远程办公的需要使得身份安全再度成为热点。“弹性” 是 2021 年 RSAC 大会的主题，零信任则被认为是建设“弹性”网络的安全基础设施。

本届 RSAC 的身份安全议题集中在多云环境的身份认证、生物识别技术应用，以及身份认证机制面临的风险等。在零信任方向，热点议题包括传统零信任的缺点、新的零信任机制，以及零信任在工业系统中的应用。

具有代表性的身份安全议题包括：

在“为什么零信任网络访问被破坏，以及如何修复它”议题中，来自 Palo Alto 的专家指出基于零信任的 ZTNA1.0 方案存在诸多缺陷，包括违反最小特权原则、没有对用户行为进行持续的跟踪和授权、没有流量检测、没有数据保护、无法保障应用程序安全等。专家提出了 ZTNA2.0 的方案，以解决上述问题。通过在第 7 层基于 App-ID 识别应用程序充分实现最小权限原则；一旦授予对应用程序的访问权限，就会根据设备姿势、用户行为和应用程序行为的变化不断评估信任度；提供对所有流量的深入和持续检查，甚至是允许的连接以防止所有威胁，包括 0day 威胁；跨企业使用的所有应用程序提供一致的数据保护，包括私有应用程序和 SaaS，具有单一 DLP 策略；始终如一地保护整个企业使用的所有应用程序，包括现代云原生应用、传统私有应用和 SaaS 应用。

在“零信任架构的构建”议题中，来自 NIST 的专家分享了国家卓越网络安全中心 NCCoE 实施 ZTA 零

信任架构项目。部署方式包括增强的身份治理 (EIG)、微分段、软件定义边界 (SDP)。整个架构包括 ZT 内核组件、终端安全、数据安全、安全分析及 ICAM。应用场景包括员工访问公司资源、员工访问互联网资源、承包商访问公司和互联网资源、企业内的服务器间通信、与业务合作伙伴的跨企业协作、利用企业资源提高信任评分 / 信心水平等。

在“为工业控制系统带来零信任”议题中，专家分析了工业控制系统面临的风险点，提出了在工业控制系统中部署零信任的方法：（1）OT 和 IT 边界：在企业网络、工厂系统和现场之间建立边界，分割网络。（2）OT 资产：屏蔽和监控无法运行安全软件或打补丁的工业端点。（3）OT 网络：使用适应现场网络中使用的工业协议和技术的网络安全。（4）离线操作：保护为维护而引入的可移动媒体和外部设备。（4）SOC/CSIRT：监控整个环境以简化威胁检测和事件响应。

在“面对 / 关闭：使用生物识别技术进行身份验证的战斗”议题中，来自思科的专家提出了 DeepFake 等技术对人脸识别和身份认证带来的技术风险，以及相应的法律风险，并提出改善的建议：（1）了解有关人脸识别和人工智能的更多信息，盘点 FR 认证和其他应用程序。（2）对 FR 申请进行法律风险评估，将 FR 整合到安全风险评估 / 管理流程中。（3）建设完整的治理体系，实施治理控制。

3 软件供应链安全

受贸易战和供应链攻击事件影响，软件供应链安全成为热点。美国商务部和国土安全部的软件供应链安全规范、代码安全和软件开发安全被高度重视。代码安全与开发过程已深度结合，强调软件供应链的安全监管与协同。开发安全和代码安全是软件供应链安全的主要抓手，并呈现融合发展的趋势。

本届 RSAC 的软件供应链安全议题集中在供应链的脆弱性，相关法律和政策等。在技术方面，热点议题则集中在软件开发安全，如 DevSecOps。

具有代表性的软件供应链安全议题包括：

在“安全的软件供应链是否可行”的议题中，专家提出当前世界软件供应链已经是高度发达的网状结构，威胁可能来自供应链的任何层面，包括恶意供应商、错误 / 易受攻击的软件、未经授权擅自修改开发或交付等。为应对软件供应链安全威胁，需要采取的措施包括供应链体系认证、供应商文件、软件测试、连续的提升、对开源软件的检测等。具体包括：对供应链软件的成熟度进行现实评估，制定安全计划以及可达到和可扩展的目标。确定对阻碍者的加速监控 / 响应，了解企业内部软件组织的安全态势。在开发和第三方代码方面获得供应链指导委员会的批准。获得对安全软件的内部承诺，在所有合同中增加供应链安全要求，对供应商的软件进行抽查等。

在“构建企业级 DevSecOps 基础架构：经验教训”的议题中，专家指出软件开发安全面临的挑战，包括：（1）对应用程序的安全状态缺乏统一的看法和理解。（2）如何实现代码分析管理及保障安全信息源的多样性。（3）开发者缺乏支持，开发团队之间缺乏信息共享。

为应对挑战，专家提出了企业级 DevSecOps 解决方案，包括：（1）由库存组件和开源构建的软件框架，将软件扫描工具打包成 docker 镜像的统一方式，Docker 化的扫描工具可以插入到许多不同的 CI 管道中。（2）存储库 / 项目与产品和团队之间的衔接。基于团队添加项目和数据，确保代码 / 工件 / 程序集 / docker 图像 / 云帐户可以链接到产品和团队。（3）为所有安全漏洞提供通用数据模型和统一 GUI。允许根据需要添加新的扫描工具或安全信息源，实现漏洞的标准化展示。（4）提供部门 / 产品级别汇总报告。包括存储库 / 工件级别的细粒度漏洞报告，在部门 / 产品级别汇总漏洞，展示跨部门 / 产品的安全成熟度等。

4 勒索软件

勒索软件成为 2021 年美国首要的网络安全威胁。根据 FBI 统计，2021 年勒索软件攻击了至少 649 个美国关键基础设施，其中包括美国最大燃油、燃气管道运营商科洛尼尔公司遭到黑客网络攻击勒索，导致供应中断和燃料短缺的事件。2021 年美国成立了勒索软件工作组（RTF），由来自行业、政府、执法部门、民间社会和国际组织的 60 多位专家组成，倡导统一、积极、全面、公私合营的反勒索软件运动。

本届 RSAC 的勒索软件议题集中在对勒索软件的分析、防护，以及应对勒索攻击的恢复能力等方面。

具有代表性的勒索软议题包括：

在“勒索软件现实清单：防止攻击的 5 种方法”议题中，专家提出了防止勒索软件攻击的 5 种方法，包括：（1）封堵漏洞。勒索软件团伙通常利用过去两年内的 CVE，目前了解到被利用最多的包括 MS Exchange、SolarWinds Serv-U、Log4J、Accellion、SonicWall、PrintNightmare 和 SMBv1。（2）知道何时丢失了密钥。核心关注点包括凭据盗窃和初始访问代理（IAB）。凭据盗窃常用的手段包括 AZORult、Predator the Thief、Kpot、MARS、Redline、Racoon、Mars Stealer。应对 IAB 的措施包括 IAB 出售对多个威胁参与者 inc. 的访问权限。 勒索软件团伙在实际勒索软件攻击之前，通常通过地下论坛出售对公司的访问权早期识别可以节省数百万美元；通过 ZoomInfo 或 RocketReach 类型工具识别受害者等。（3）了解网络犯罪分子，学

习他们的常用手段。例如，Conti 小组正在积极利用 Scripts Github repos、Cobalt Strike、CVE PoC 等，经常使用非恶意工具来获得他们的目标。这些资源是开放的，防御者也可以学习同样的资源。（4）深入了解勒索软件机制，发现恶意软件爆发之前的行为痕迹。攻击者严重依赖非恶意工具，而传统的网络安全控制关注过多的恶意文件，却忽略了行为才是关键。因此应重点关注攻击者使用工具的行为。（5）创建减速带和检查点。采取包括多因素身份验证、网络分段、限制浏览器 cookie 寿命、活动目录安全等措施，加强纵深防御使得攻击者横向移动更加困难。

5 AI 安全

本届 RSAC 的 AI 安全议题集中在 AI 训练和应用中的数据与隐私安全、AI 开源工具安全、AI 测试安全等 AI 自身安全，以及将 AI 技术用于威胁分析和 0day 网络攻击。

随着海量数据的积累、计算能力的发展、机器学习技术创新，图像识别、语音识别、自然语言翻译等人工智能技术得到普遍部署和广泛应用。AI 对于传统计算机安全领域的研究也产生了重大影响，除了利用 AI 来构建各种恶意检测、攻击识别系统，黑客也可能利用 AI 达到更精准的攻击。

同时，AI 自身的安全性变得前所未有的重要，如果应对利用数据投毒、深度伪造等技术干扰破坏 AI 的正常学习与应用，也成为网络安全领域面临的新课题。

具有代表性的 AI 安全议题包括：

在“AI 的隐私和合规性——开源工具和行业看法”议题中，来自 IBM 的专家分析了面向 AI 应用的隐私保护技术，如差分隐私、匿名化、分布式计算和加密技术等，以及各种技术的优缺点。IBM 专家认为，从行业视角看，AI 隐私保护应具备以下特点：（1）防御应该是非破坏性的。大多数组织已经拥有复杂的机器学习设计和运营流程，解决方案应该以最小的中断集成到这些流程中。（2）产品应设计成人工智能隐私工具包，“一键式”解决方案更易于学习，具有良好的默认参数有助于入门，以及可解释的可视化首选项。（3）可扩展性和性能。一些隐私保护方法非常适合学术工作，但不要扩展到企业工作负载，工具需要自动化和高效的算法，和基于风险评估的模型优先级。在此基础上，IBM 推出了用于 AI 隐私的开源工具，能够实现模型匿名化和数据最小化，并展示了相关的应用案例。

在“利用人工智能和深度学习对抗 0day 网络攻击”议题中，来自 Check Point 的专家认为面对当前网络威胁困境，基于 AI 的安全技术表现出高效阻断攻击、最佳威胁捕获率、接近零误报的特点，只有 AI 才能保证网络安全。Check Point 搭建了威胁云 ThreatCloud，通过 30 多个 AI 引擎实现不同的安全功能，主要包括：（1）检测未知恶意软件 – 受感染主机检测、沙盒静态分析、沙盒动态分析引擎；（2）检测网络钓鱼 – 邮件静态分析、移动零钓鱼检测、反钓鱼 AI 引擎；（3）提升准确性 – 网络 AI 引擎聚合器、移动 AI 引擎聚合器、机器验证签名引擎；（4）异常检测 – 云网络异常检测引擎；（5）战场狩猎 – 活动狩猎引擎；（6）揭露隐形漏洞 – 分析师头脑、恶意活动检测引擎；（7）分类 – 文档元分类器矢量化家族分类器、机器学习相似度模型、MRAT 分类器等。

6 威胁分析及狩猎

网络攻击技术和方法不断升级换代，攻击者从脚本小子、黑产犯罪团伙向国家级组织演进，攻击能力不断提高，攻击技术不断升级；威胁利用从已知到未知不断发展变化。

威胁狩猎是一种主动识别攻击痕迹的方法，由威胁猎人利用威胁分析工具、威胁情报和实践经验来积极筛选、分析网络和端点数据，寻找可疑的异常或正在进行的攻击痕迹。近年来威胁狩猎工具的自动化水平不断提高，逐渐成为应对高级持续威胁的重要手段。

本届 RSAC 的在威胁分析及狩猎议题集中在全球网络威胁态势、基于 AI 的自动化威胁分析技术，以及

威胁狩猎实践。

具有代表性的威胁分析及狩猎议题包括：

在“2022 年网络安全状况：从大离职到全球威胁”议题中，ISACA 专家分享了 2022 年网络安全状况报告。根据 ISACA 的研究，在网络威胁态势方面，2021 年企业最关注的五大网络安全影响包括：组织的声誉、数据泄露对客户造成的伤害、供应链攻击造成业务中断、商业秘密的丢失、组织的股票价格、财务状况。五大网络安全威胁分别为：网络犯罪、黑客、内部威胁、国家威胁、内部误操作。五大网络攻击方式分别为：社会工程学、APT 攻击、安全配置错误、勒索软件、未打补丁的系统等。在人力方面，当前全球网络安全从业人员数量严重不足。在 2021 年有 63% 的企业网络安全职位有空缺，五分之一的企业表示需要六个月以上才能找到合格的空缺职位的网络安全候选人。其中空缺最大的细分领域包括云安全（52%）、数据保护（47%）、身份安全（46%）、应急响应（43%）、DevSecOps（36%）。

在“CHRYSALIS：人工智能增强的威胁猎手和法医时代”议题中，专家介绍了将数据科学和人工智能引入威胁狩猎和数字取证进该领域的进步的技术：（1）ML&TH 联结学习用于异常分析的技术；（2）机器学习用于恶意软件分析并实现检测和分类的技术；（3）基于机器学习揭露恶意软件的技术，包括使用带有预训练模型的 ML 进行恶意软件检测、使用 SqueezeNet 和逻辑回归模型、使用卷积过滤器提取特征以将其分类为恶意软件；（4）基于机器学习实现内存取证的技术，包括用于识别受损数据集中的特定模式，使用 Volatility 3 输出应用 ML 算法来寻找可疑行为，并可以与 pslist、psscan、pstree、malfind、netscan 等一起使用；（5）基于机器学习实现深度日志分析的技术，包括从标记的数据中学习以分类为异常或正常条目，在大量系统日志中使用 LSTM 识别异常， IDS/防火墙日志以检测 DDoS 和端口扫描等；（6）基于机器学习实现流量分析的技术，包括远超传统系统能力的定制化深度监控、执行聚类以发现异常并区分异常值、在大型数据集中发现未知威胁等。

7 风险管理

网络威胁是利用电子信息和系统中的漏洞的恶意攻击，而安全风险管理旨在降低网络攻击的可能性和影响。通过识别、评估和减轻企业电子信息和系统的风险，实施安全控制以防止网络威胁。

面向关键基础设施和重要行业的高级持续威胁日益严重，企业必须建立风险评估机制，使用威胁情报界定风险，开展安全测试等一系列风险管理措施，从而实现体系化的网络安全防护。

本届 RSAC 的风险管理议题集中在网络风险分析及风险管理的合规模型等方面。

具有代表性的风险管理议题包括：

在“有针对性、统一和协调的服务，以更好地降低风险”议题中，专家认为由于新冠疫情带来的居家工作和“大离职”使得云服务提供商必须加速开展安全托管业务，而急于通过 MSSP 解决这些挑战是以牺牲其他领域的资源 / 风险为代价的，在许多情况下，企业过度补偿检测和响应领域的新工具和服务，而牺牲了他们的识别、预防和恢复策略，因此需要开展相应的评估和规划，评估的内容主要包括识别、防护、检测、响应、恢复。评估的过程包括：（1）需求评估，包括明显被忽视的领域、目前资源不足且风险太大的地区、存在明显技能差距的领域、您可能在现有工具或服务中有重叠的领域、内部资源可能不可行或不建议的领域；（2）使用安全框架来指导评估；（3）将调查结果与 MSSP 服务进行比较。

8 云安全

云应用的普及导致相关安全问题的热度持续增强。云安全赛道在一直演进，细分领域、技术方向不断演化，从以容器安全为代表的基础设施安全，到平台层面 API 安全，再到 SaaS 层面业务安全。基于云原生的

威胁管理，数字调查取证，云安全管理平台，资产管理等成为今年云安全的重点议题。

本届 RSAC 的云安全议题集中在云上的数据安全、身份安全等方面，以及多云环境的安全架构。

具有代表性的云安全议题包括：

在“安全左移：现代云安全的十大最具颠覆性的想法”议题中，专家提出安全左移的思想，认为在当前云安全响应太慢、太晚、缺少应用程序上下文、无法修复的现状下，应重新考虑以运行时为中心的云安全方法，主要包括：（1）以开发人员为中心，安全性必须集成到开发者平台中，包括代码库、业务流程等（GitHub、GitLabs、Jenkins、Jira……）。（2）拥抱 IaC 安全性，IaC 安全性将成为云安全的基石（VM、CSPM、CIEM 全部基于 IaC 扫描左移）。（3）补丁即代码：采用基于 IaC 和拉取请求的不可变运行时原则和补丁作为代码。（4）AppSec 的回归：不能忽视 SAST 和 SCA 的 AppSec 规则，它们是云安全策略中最重要的部分。（5）无代理方法：云安全供应商必须利用云 API 来实现无代理和持续的云安全，例如，将 VM 转换为基于 API 的云原生 VM。（6）运行时安全仍然很重要，并且 EPP 供应商必须采用云架构（如 eBPF）。（7）微分段 /ZTNA、的 IAM 策略

非常复杂，应寻求自动化解决方案。（8）持续部署安全网关，并考虑整个云应用程序生命周期的变化。（9）策略即代码，用一个单一的策略即代码统一， 考虑开放标准而不是以供应商为中心。（10）了解自身现状，大型企业将持续部署混合云，而中小企业则通常选择单一公有云。

9 物联网及工业安全

物联网及工业安全由于其庞大的终端规模及潜在的安全威胁而受到关注。近年来物联网技术正在加速向各行业渗透，智慧工业、智慧城市、智慧交通、智慧健康、智慧能源等将成为产业物联网连接数增长最快的领域。利用物联网终端的挖矿、设备劫持事件频发，智能医疗、交通、家居产品不断爆出安全漏洞，并且造成不可逆的生命财产损失，从而使得物联网及工业安全成为热点议题。

本届 RSAC 的物联网及工业安全议题集中在终端设备的漏洞检测、可信机制及安全模块方面。

具有代表性的物联网及工业安全议题包括：

在“防篡改元件如何保护物联网”议题中，来自可信连接联盟（TCA）的专家指出，到 2025 年，物联网连接数将达到 240 亿，而对物联网连接的安全防护能力则严重不足，这既包括对单个设备的近距离攻击，也包括云端的远程攻击。而防篡改元件可以实现基于 SIM、eSIM、eSE 的快速认证与数据安全传输能力。

10 基础设施安全

在前几届 RSAC 上，基础设施安全话题相对冷门，今年热度有所回升。一方面因为过去两年美国的重要基础设施大规模遭受勒索软件和供应链攻击的威胁，此外 5G 和工业互联网的建设进入到应用阶段，以能源互联网为代表的产业应用引起了更多的重视。

本届 RSAC 的基础设施安全议题集中在关键基础设施的网络攻防和安全运营方面。

具有代表性的基础设施安全议题包括：

在“分布式能源基础设施的入侵与防护”议题中，专家提出到 2024 年能源互联网市场将达 2000 亿美元。能源互联网安全是一个新的领域，需要不同的网络安全架构：保护系统 / 平台（例如 DERMS、ADMS），确保公用事业和第三方发电资源的连接，验证第三方发电源、聚合器和逆变器供应商的数据的完整性，检测第三方电源上的异常和潜在恶意活动并预测潜在的下游影响。因此需要建立供应链安全防护机制，检测并防御来自供应链上下游的攻击，以应对类似 SolarWinds 事件的攻击。

结语

从本届 RSAC 的热点议题可以看出，网络安全的许多细分领域都在发生变革。

数据与隐私安全在寻求具体应用场景的解决方案以实现产业落地；身份安全与零信任在寻求新的架构以弥补实践中发现的不足；软件供应链安全在尝试构建企业级开发安全架构；应对勒索软件则有了体系化的组织和方法；AI 安全在探讨自身的安全合规以及在对抗零日网络攻击中的应用；云安全在探索安全左移的运营商安全。

今年热点议题是对 RSAC2021 的网络安全“弹性”主题的回应，也是在网络安全行业进入深水区，如何解决诸多不确定性问题的积极尝试，对于我国网络安全建设和产业发展具有重要的参考价值。

RSAC 2022 24 款热门产品

RSAC 2022大会自疫情爆发以来首次恢复线下活动，全球网络安全厂商携最新安全产品在展会亮相。 网络安全产业处于高速发展中，各种极具创新精神和价值的新产品、新技术层出不穷，进一步丰富了网络安全行业的产品图谱。

今年参展的产品主要围绕身份和访问安全、应用安全、SaaS 服务和安全运营中心 (SoC) 增强功能。此外，语音欺诈监控工具、攻击面管理平台、人工智能电子邮件安全平台等也引入瞩目。

下面盘点一下 RSAC 2022 的热门的网络安全产品。

1 AppGate 零信任网络访问方案（SDP 6.0）

SDP 6.0 是 AppGate 的零信任网络访问 (ZTNA) 解决方案的最新版本。增加了新的风险模型功能，可让用户扩展其现有企业安全工具的价值和范围，以简化和加速零信任部署。Appgate SDP 6.0 的新风险模型功能使客户能够将高 / 中 / 低敏感度级别分配给特定的工作负载和资源。基于用户已有的安全工具，针对被访问资源的敏感性，SDP6.0 为用户提供一种简单、灵活的方法来衡量登录时的用户 / 设备风险。然后，风险模型根据风险评分动态调整访问权限。

2 Armis 资产漏洞管理（AVM）

Armis 资产漏洞管理 (AVM) 是一种端到端资产漏洞生命周期管理解决方案，支持 IT、OT（运营技术）、ICS（事件指挥系统）、IoMT（医疗物联网）和 IIoT（工业物联网）。在 RSA 会议上，Armis 展示了 AVM 中包含的更新功能，它提供了组织环境的完整资产和漏洞视图、基于风险的优先级及通过自动化和跟踪漏洞管理生命周期的综合仪表板减少平均修复时间。

3 BigID 数据安全解决方案（SmallID）

SmallID 是一种云原生的数据安全按需解决方案，可帮助客户减少攻击面，识别高风险数据，并自动识别“暗”数据（已收集但未用于分析的数据）跨云。SmallID 使用 BigID 专有的机器学习技术来自动发现和分类敏感数据，识别影子和暗数据，并简化合规。

4 Checkmarx 应用安全视图（Fusion）

Checkmarx Fusion 为应用、组件交互和材料清单提供了单一的集成视图。该平台会在软件生命周期的所有阶段生成安全扫描结果，以关联漏洞并确定漏洞的优先级，从而首先指导最关键问题的修复。Checkmarx Fusion 是应用安全 (AST) 平台 Checkmarx one 的一部分。Checkmarx Fusion 支持多引擎扫描关联和跨引擎扫描结果的基于上下文的风险优先级。

5 DNSFilter 数据导出工具（Data Export）

数据导出是一种新工具，旨在让安全团队加快整体威胁检测和响应策略。它自动将 DNSFilter 查询日志数据导出到领先的 SIEM（安全信息和事件管理）和安全监控解决方案，以便通过多个数据源进行聚合、分析和操作。这将有助于减少手动任务并提供对 DNS 的可见性，从而为组织创建完整的安全图景。

6 Forinet 数字风险保护服务 (Fortirecon)

Fortirecon 是一种数字风险保护服务 (DRPS)，它使用机器学习、自动化和人类智能来提供对组织外部攻击面的可见性。Forinet 表示，Fortirecon 有三重功效，包括外部攻击面管理 (EASM)、品牌保护 (BP) 和以对手为中心的情报 (ACI)，用于在侦察阶段检测和反击攻击，以帮助安全人员节省大量时间和降低风险。

7 Gurucul 安全运营和分析平台

Gurucul 安全和运营分析是一个云原生的模块化平台，它将 UEBA、NTA、SOAR 和 IAA 等安全运营中心 (SoC) 解决方案整合到一个单一的访问中，并增加了身份威胁检

测和响应 (ITDR)。该平台强调身份安全，旨在对抗与网络钓鱼、社会工程、凭证盗窃和供应链攻击相关的复杂攻击。

8 Hunters SoC 平台

Hunters SoC 平台推出了新的升级，以推进和简化安全运营工作流程。新功能包括整个安全运营工作流程的自动化、引入风险评分的威胁优先级、数据规范化及对无限数据注入的降噪支持。这种常见 SoC 任务的自动化预计将使数据和安全工程师能够专注于更高价值、领域和组织特定的威胁。

9 Mandiant：MDRP

Mandiant Digital Risk Protection (MDRP) 使用专有的扩展检测和响应 (XDR)，它与来自多个供应商的安全系统一起使用，以提供组织攻击面的情报支持视图。此次发布的产品与 Mandiant Advantage 数字威胁监控的普遍可用性相结合，该监控将与 MDRP 一起安装在 Mandiant Advantage 中。MDRP 将提供对外部暴露以及威胁分析和风险识别的可见性。

10 Noname API security platform 3.0

Noname API 安全平台的最新版本为遵守任何环境、市场和法规要求提供了全球支持。全球支持为该解决方案提供跨各种云和区域的 API 可见性，并识别跨区域的问题和模式，不受流量和环境复杂性影响。它还支持遵守各个地区的现行法规，包括 PCI-DSS、PII 和数据驻留要求。

11 Optiv：网络恢复解决方案 (CRS)

网络恢复解决方案 (CRS) 为组织提供战术建议和技术，以保护并从网络攻击中快速恢复。该解决方案通过自动化工作流程识别并优先处理业务关键资产。该公司将在 RSA 上展示它如何使用上下文关键技术通过数据仓库、数据隔离、物理隔离备份解决方案来备份基本数据、应用程序和系统。

12 RSA 身份和访问管理方案（ID Plus）

ID Plus 是一种基于 SaaS 的身份和访问管理 (IAM) 解决方案，为客户提供云、本地和混合部署的选择。ID Plus 是一款内置于 DS100 的新工具，该工具是 RSA 的新硬件验证器，专为 RSA 的零信任客户而设计。DS100 是一种无密码身份验证器，它使用 FIDO（快速在线身份验证）协议和一次性密码解决方案。该身份验证器是一款基于云的产品，可插拔使用。

13 SentinelOne 漏洞扫描修复工具

Singularity Vulnerability Mapping 是 SentinelOne 为 Ivanti 提供的集成工具，利用后者的统一 IT 平台和 Sentinel 自己的 Singularity XDR 提供自主网络和漏洞扫描及快速修复。Singularity Vulnerability Mapping 可以与 Ranger 的 IoT 网络发现系统和 SentinelOne 的 Storyline Active Response (STAR) 自动威胁搜寻、检测和响应工具一起使用，以帮助分析师确定补丁的优先级并降低风险。

14 BlackBerry 零信任网络访问 工具

黑莓展示了 CylanceGateway 零信任网络访问 (ZTNA) 工具，可为用户提供网络和设备监测，上下文关联和持续身份验证，以限制对受信任、经过身份验证和已知用户、设备的访问。工具可以保护任何网络、任何设备的访问、使用 Cylance 人工智能来降低风险并提供 0day 网络钓鱼检测，从而有效降低勒索软件和其他网络安全威胁。此外，还为自带设备 (BYOD) 部署提供安全连接，并使用 Mitre Att&ck 框架规则检测横向移动攻击。

15 Cisco Security Cloud

思科详细介绍了新的总体安全战略，重点推出酝酿依旧的 Cisco Plus 产品，用于统一安全访问服务边缘 (SASE)。思科安全云平台将在思科产品体系中占据重要地位，基于开放标准的统一平台将确保跨混合云和多云环境的安全性，并具有安全连接位于任何地方人员、应用和设备的能力，实现大规模的威胁预防、检测、响应和补救措施。

16 Palo Alto Networks

Palo Alto Networks 展示的 Prisma 云原生安全产

品的新功能，引起业界的广泛关注。近段时间，Palo Alto Networks 不断推出安全产品：3 月公布一款供应链安全领域的产品，用以寻找软件供应链中的潜在漏洞或错误配置；2 月推出针对托管服务提供商 Prisma SASE 新功能，包括分层多租户云管理平台和开放性 API 框架。

17 SailPoint 身份安全产品

身份安全公司 SailPoint 展示了两款新产品——SailPoint Identity Security Cloud Business 和 SailPoint Identity Security Cloud Business Plus，后者提供更多产品来发现、保护和管理整个混合基础架构中的身份。SailPoint 身份安全云业务包可以为用户提供必要的身份安全功能，并利用人工智能和机器学习来构建更强大的身份安全。

18 Pindrop 语音安全产品

语音防欺诈提供商 Pindrop 展示了最新产品。其语音安全技术的新功能包括预测年龄范围、预测口语和监控语音验证欺诈的方法。Pindrop 发展趋势迅猛，美国多家大型银行成为其客户，保护数亿用户免受基于语音的欺诈和攻击。

19 Orca 云安全

Orca Security 最近的产品开发动作主要是“上下文感知安全”，被用于开发早期识别和预防云应用安全问题，以及针对云原生应用的攻击路径分析和业务影响评分。该产品考虑了当前的运行环境和部署的代码，以提高准确性，并通过上下文和优先级警报等措施监控生产环境的风险。

20 Randori 攻击面管理服务

IBM 宣布收购的 Randori 在攻击面管理和攻击性网络安全服务上有着独到优势，IBM 计划将 Randori 的 ASM 平台与其扩展检测和响应 (XDR) 产品 IBM Security QRadar 集成，从而就能够保持攻击面的实时可见性。此外，IBM 还将使用 Randori 的持续红队攻击测试 (CART) 来改进 X-Force Red 进攻性安全服务。

21 Abnormal Security

Abnormal Security 主要业务包括保护企业和机构组织避免受到针对性的电子邮件攻击，旗下云电子邮件安全 (ICES) 平台可以和 Microsoft 365 集成，产品的创新之处在于结合当前云原生环境的发展和需求，孵化出了基于 AI 人工智能技术的电子邮件安全防护机制。

22 DoControl

DoControl 是一家美国数据访问控制服务商，展示了 SaaS 应用程序数据访问监视，编排和修复所需的自动化自助服务工具。公司采用独特的，以客户为中心的方法来应对流行的 SaaS 应用程序中的劳动密集型安全风险管理和数据泄露防护挑战。

23 Snyk 开发者安全平台

网络安全独角兽公司 Snyk 独特的“安全智能”工具帮助开发者持续监测可能发生的漏洞，并不断自动化安全性能升级。Snyk 帮助开发者在开发生命周期中一以贯之地查找、修复和监测代码的脆弱性，让开发者更好地应对纷繁复杂的微服务、API，以及日益增长的复杂性。

24 Fortanix 区块链安全产品

初创公司 Fortanix 展示了两个区块链安全产品：Fortanix Non-Custodial Warm Wallet 通过双因素身份验证令牌，确保数字资产不会在未经同意的情况下被钱包提供商滥用。Fortanix Ignite One-Time Signer 有助于验证区块链交易的合法性。新工具与 Fortanix 数据安全管理器集成，这是一套专为区块链、加密货币和去中心化金融业务设计的服务。

瑞兽白泽：一场持续和攻击者斗智斗勇的四年往事

话说李逵在接老母上梁山的途中，行至沂水县西门外，只听见城门附近有人大喊：“案犯第一名宋江，第二名戴宗，第三名李逵……”

听见有人叫自己的名字，李逵忍不住凑上前去看到，赫然三张海捕文书贴在墙头，上面画着李逵等三人的画像。

李逵乐了，连连调侃说画得不像。话还没说完，朱贵却从身后一把拉住李逵，朝着弟弟朱富开的酒店而去，担心有人眼疾手快，认出他将其送官。

李逵似乎并不买账，一边嚷嚷着朱贵认错了人，一边抱怨凭什么他们的人头就值一万、五千贯，自己人头只值三千。

或许是画的真的不像，并没有人认出在江州法场“杀风了”的李逵，到家里才被亲哥哥李达叫嚷着要将其送官。但即便如此，在没有照相技术的年代，画像却是发布通缉令、协助侦破案件的最佳选择之一，不知道多少江洋大盗因此着了道。

然而直到 19 世纪 80 年代，一个叫伯尔蒂龙的人，才正式开创了“头像描述法”，即根据语言描述画出目标头像，从而将模拟画像纳入到案件侦破的科学体系。

20 世纪 40 年代中期，在国际上通用的方法是“人像组合法”，其原理就是把不同种类的相貌特征，通过不同的排列组合制作出模拟画像。当时的“拼图库”是一个旅行箱大小的“人像组合箱”，里面装满了代表不同类型的五官塑料片。

随着计算机技术的发展，世界各国都积攒了大量具有本国特征的拼图库，开发出了电脑人像组合系统。在人工画像师的配合下，哪怕是只剩下腐烂的尸体或者含糊不清的语言描述，想要知道犯罪嫌疑人大概长什么样子，并不是一件特别困难的事情。

可现在的问题是，如果犯罪的那一头只是几台冰冷的机器，总不能画个电脑或者服务器的形状出来吧。

IP 封禁与黑白名单

根据 TCP/IP 协议的规定，每一台接入互联网的设备，都会被分配一个 IP 地址。一台设备想要通过互联网访问另一台设备，就得自报家门，亮出自己的 IP 地址。

所以如果不想让某些机器访问的话，比如，遭到源自某个 IP 的网络入侵，除了拔网线，最直接有效的方法就是把对应的 IP 地址给“遮住”，俗称 IP 封禁。

过去、现在及将来的相当长一段时间内，IP 封禁都是处置网络入侵的必选手段之一。作为目前使用最广泛的网络安全设备，防火墙最重要的功能之一，就是阻断来自某些特定 IP 的网络访问。

不过，封 IP 得讲证据，不能靠主观臆断。否则一个不小心封错了或者封漏了，都会让人很难受。

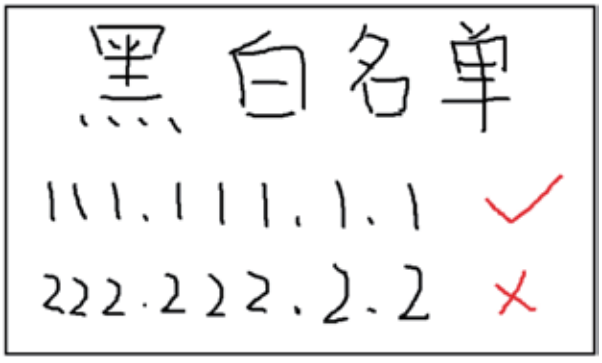
所以前些年，人们搞了黑白名单，把值得信任的 IP 放在白名单中，被发现经常干坏事的 IP 放在黑名单中。凡是上了黑名单的一律封禁，凡是在白名单里面的一律放行。

不过，黑白名单本身提供的信息非常有限，充其量就是公布了一个“名字”而已。而且从访问侧封禁 IP 其

实也是一个效果非常有限的手段，下面我们一个个来说。

喜欢看刑侦剧的都知道，证据往往能回答两个非常重要的问题，一个叫作案手法，另一个叫作案动机，而这些信息都是日后法院判决、量刑的重要依据。比如，正当防卫和过当防卫、故意杀人和过失致人死亡，尽管结果可能相同，但刑罚却相差甚远。

遗憾的是，黑白名单除了告诉你是好是坏，并不能提供其他更有价值的信息。



更何况，为了绕过这两个名单，攻击者也煞费苦心钻研攻击技术，跳板机、傀儡机……这一套全家桶上来，让黑白名单也不那么灵了：黑 IP 不见得都在黑名单里，白名单里的白 IP 也不见得那么白。

那么问题来了，当安全设备检测到来自某个 IP 的异常访问之后，安全人员如何确定是不是真正遭到攻击了？

对方到底想干什么？是一次大范围的端口扫描还是定向的 APT 渗透？

如果是定向攻击的话，对方利用了什么漏洞，植入了什么木马？

我该怎么处置？置之不理吗？封禁一天、两天，还是永封？封禁之后攻击就不会发生了吗？风险就排除了吗？

显然，简单的非黑即白回答不了这些问题。实际上，每一条告警的背后，都是不同的人、怀着不同的目的、干着各种各样的事情。如果只关注行为本身而忽略了行为主体，那只会淹没在无止境的告警中无法自拔，从而忽略了真正有威胁的攻击者。

并且简单的一封了之，并不会让有恶意的主体停止他的行动，毕竟更换 IP 的成本低的令人发指。

每每遇到这种情况的时候，安全人员不禁连连挠头，恨不得顺着网线就钻过去，看看对面是个什么样的牛鬼蛇神。防了半天连攻击者是何许人还不知道，简直是荒唐。

说起来，就是缺乏攻击者本身的相关情报。

楚云飞在进攻受阻后，面对部下送进来的一堆情报根本提不起兴趣，但唯独在听到对手是李云龙的二师时，就一下来了精神。

那么如果有一个情报平台，上面的情报能够直接告诉我们攻击者是什么样的人、经常使用什么样的攻击手法、攻击目的到底是窃取数据还是勒索钱财亦或是伺机破坏，这样日常安全分析工作就可以有的放矢，针对不同的人（威胁主体）进行针对性的防御或跟踪。

这就好比同样是盗窃，入室盗窃的受重视程度就应该高一些，团伙流窜作案的危害性可能就要比一个人小偷小摸危害性更大。

后来，这个情报平台在奇安信被称为白泽。

通万物之情，知鬼神之事

白泽平台的研发始于 2017 年年中。

彼时发生了一件至今还余波未消的网络安全事

件——永恒之蓝勒索病毒事件，数以万计的计算机因此感染，加之一些其他的网络攻击，所以奇安信在短时间内，接到了大量的网络安全应急响应需求。

安服人员有个好习惯，会一并把所有发现的安全事件都给处理掉，绝不仅限于永恒之蓝。

应急次数多了，一线安服人员在处置安全事件的时候，经常会在不同的单位，遇到来自同一个攻击来源 IP 发起的网络攻击。

这就有意思了。

于是有人提出了这么一个需求，能不能做一个数据库，可以把攻击源的相关信息都放进去，需要的时候一查就知道攻击者是谁了。同一个攻击者在近似的时间内，发起的网络攻击都差不多。

类似做法并不是没有先例。在早些年，定向攻击远没有现在这么普遍，因此同样一款病毒往往会批量感染大量计算机，因此在病毒查杀领域有一项使用非常广泛的方法叫作云查杀，其本质就是将病毒样本都放在云上，可以将捕获到的可疑样本与之进行比对。

说起来很简单，但问题又回到了搜集证据这里，想要准确描述一个攻击主体，就得在一个相当长的时间窗口内，对其进行持续的跟踪观察。病毒查杀领域的这个跟踪观察是各个杀毒软件的“云查”模块，而攻击者类的呢?

那么如果想要做到这一点，刑侦的办法通常是派出若干名侦察员，对嫌疑人进行长期的跟踪，甚至卧底调查，而网络安全的方法是派出探针。

单单看名字就知道，探针是网络空间的“侦察员”。它们通常部署在一些关键节点上，负责搜集“路过的”威胁主体的相关情报。奇安信的这些探针被部署在了大大小小数十万个互联网应用及蜜罐节点上，能够从每天数亿的数据量中，获取超过 10 万条攻击者信息。

或许很多人都想不到，部分活跃的攻击者或者攻击团伙在十多年前搞的事情，现如今还能在白泽平台检索到。

不过，千万不要以为收集数据是个非常简单的事情，它对探针的能力要求非常高。这就好比摄像头拍摄画面不清晰、拍摄有死角，对于案件侦破都是非常不利的。

下面这张图直观地展现了奇安信探针的强大数据收集能力。

在这样的数据视野加持下，白泽平台才有能力证明哪些攻击源头是广撒网式的黑产扫描器，哪些攻击源头是肆意传播的僵尸网络，哪些攻击源头是进行安全测试的白帽子。

否则在不了解攻击者的情况下，同样是端口扫描，安全人员该如何确定是一次大范围的扫描，还是 APT 定向攻击的前奏试探呢?

这也是白泽平台之所以叫白泽的根本原因。

在中国古代神话中，白泽是传说中的瑞兽，身上有一千只眼睛，熟知天下各类妖魔鬼怪，有“通万物之情，知鬼神之事”之称，在唐宋年间常被绣在枕头上或挂在门口用以辟邪。用白泽平台负责人林子翔的话来说，他希望奇安信的白泽，也可以熟知网络空间中的各类“妖魔鬼怪”。

一波三折

只有白泽平台知道还不行，白泽平台得让防守方知道。所以，相比黑白名单，白泽平台就是实实在在给攻击者画像了。

其实收集数据对奇安信的难度并没有太大，对于这样一个体量的网络安全公司，其探针的分布范围非常广泛，因此可以保证极广的数据视野。

不太好解决的是下面两件事情:

第一，攻击 IP 和背后的攻击者并不是一对一，而是

多对多，并且攻击者更换 IP 是再常见不过的事情。如果想要对一个攻击者进行长时间的观测，必须要知道他什么时候换了 IP，换了什么 IP。

第二，分析≠聚合。白泽平台输出的应该是分析处理的结果，而不是一大堆看起来有点关联的数据。例如，数据源 A 说某 IP 发起了某某攻击，数据源 B 说某 IP 上绑定有某个网站，数据源 C 说某 IP 访问了 SRC，这一组数据能够说明什么问题呢?

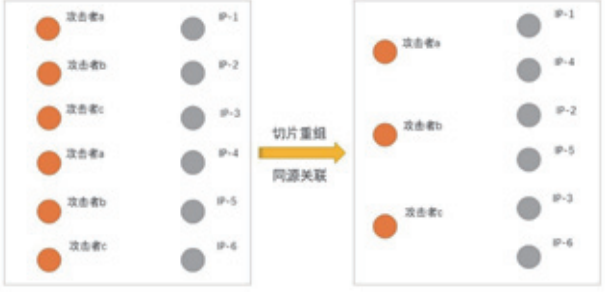
为了解决这两个问题，林子翔的第一个想法就是看看公司有没有可以复用的组件，如关联分析等，但遗憾的是当时的安全分析组件和白泽平台想要的安全分析逻辑完全不同，很难复用。

第二个想法就是看看能不能站在前人的肩膀上。不过在转了一圈之后，林子翔发现白泽平台想要解决的问题和场景几乎毫无经验可借鉴，尽管市面上也出现了一些针对威胁主体进行分析的平台，但基本上都停留在 IP 信息聚合的层面，可以浅层次的分析出一些 IP 背后的威胁主体的历史动作，但并没有从动机和能力两个层面输出结论或辅助判断的依据。

面对前无古人的窘境，只有自己摸着石头过河才是唯一出路。

思索良久，研发团队提出了一个大胆的想法：既然 IP 和攻击者不存在强关联，那就设置一个规则，今天发现的攻击 IP 在今天过去之后，就认为攻击者已经更换了 IP，基于这个规则将攻击 IP 和攻击者打乱，然后依靠不同来源的数据，将具有相同特征的攻击进行重新组合。

这个过程有点类似于遗传学基因的分离定律和自由组合定律，大概就是下图这个意思。



这项技术在奇安信被称作切片重组和同源的分析引擎， 把攻击者和 IP 的关系厘清之后，就可以摆脱观测攻击者逃不开 IP 的限制了。

正当白泽平台意气风发准备大展宏图的时候，现实却给了它当头一棒。“白泽平台好是好，可是你的数据我都用不了啊。”质疑的声音不绝于耳。

这句话把白泽团队给噎住了。一个很大的问题是，当时大部分安全产品的关注核心是通过检测威胁行为而产生告警，而没有在产品的分析逻辑中对威胁主体进行建模。

举个例子，同样是找持刀的杀人犯，安全设备通常关注的是“挥刀”这个行为，但查出来的有可能是厨师在切菜或者是屠户在杀猪，安全厂商则希望利用各种技术让检测挥刀更加准确，而不至于把挥手看成了挥刀；白泽平台的思路是研究挥刀的人，通过各种不同维度数据判断其到底是杀人犯还是厨师或者是屠户。

这就导致了一个问题，白泽平台生产的数据，并不能像黑白名单一样，让安全设备自动使用。

无法解决自动化问题，白泽平台的落地使用可以说无从谈起，充其量只能是少数分析师手里的“高级玩具”。

没有明确场景且看不到收益的日子，对于白泽团队来说真的很难熬，仿佛这一拳打在了棉花上。不少人开始打起了退堂鼓，以至于一个日增十万、总量百亿级别的攻击者数据库，最少的时候只有几个人在维护。

为了给团队同时也给自己打气，林子翔经常半开玩笑地对团队说：“别灰心，想想你们的毕业设计，有几个能真正用在生产环境的？大家就当做科研了……”

好在功夫不负有心人。林子翔他们终于琢磨出来一套新的安全分析体系：白泽平台和其他检测设备分工合作，检测设备负责分析威胁行为产生告警，白泽平台则将这些告警收集起来后，生成一条条事件，同时基于自身数据库对这些事件进行攻击者分析，并将最终分析结果输出。

有了自动化的手段，白泽平台才有可能和其他检测手段一样，真正意义上服务于网络安全建设，并且大幅提升检测准确率。

牛刀小试

白泽平台研发完成后，并没有第一时间推向市场，而是在奇安信内部磨炼内功。历经四年的沉淀和三次重大版本迭代，白泽平台终于迎来了表演的舞台——北京冬奥会。

作为四年一度的冰雪运动盛会，盯上冬奥会的各色人等可不少，有组织严密的 APT 组织、有浑水摸鱼的民间散盗、当然也有趁机炫技的白帽子……为了搞清楚对手是谁，自然少不了白泽平台来盘一盘他们。

有数据统计，在冬奥重保期间，共有近千条关键的攻击者 IP 被提交到白泽系统进行画像。

其中，不隐藏自己的好人（安全厂商或者民间白帽子进行安全测试）或非恶意攻击者（操作目的不是恶意的，但行为本身会触发告警）占 26.3%；

不必隐藏或不会隐藏自己的坏人（如普通的僵木蠕毒、新手黑客）占 52.5%；

精心伪装，但仍然能够被精准画像的高级攻击者（包括 APT 和黑客高手、高级白帽子）占 1.3%；

19.9% 的告警 IP 后经确认后，绝大多数为正常业务流量触发的告警（因配置、流程不规范等原因触发告警）或其他安全威胁；

仅有 0.1% 的攻击者可以确定是高级威胁，但并不能完成精确画像，且高级威胁无一漏网。

这样的分析结果与上亿级别的告警相比，可以说是安全检测技术迈出的一大步。

这里有一个真实有趣的小故事。

有一天，奇安信一线重保工程师在对冬奥系统的攻击告警中，发现了一个来自境外的 IP 地址，其行为高度可疑，非常像 APT 攻击前期的测试或者情报搜集行为。

这个结果一经发现，所有人都捏了一把汗，立即提交到白泽系统上进行分析。经过白泽分析发现，这个攻击者的同源资产中，关联了若干个国内 IP，其中一个 IP 的行为特征和某公司白帽子的安全测试行为非常吻合。

因此，重保研判组判断，这应该是一名精心伪装的白帽子在进行安全测试，而不是来自境外的 APT 攻击。

事实证明了白泽平台的分析结果。

据说该公司的白帽子在知道自己被发现时大吃了一惊，用他的话说，作为一名资深白帽黑客，自己的伪装手法屡试不爽，安全测试行为还从来没被发现过，没想到这次竟然栽在了白泽平台手里。

道阻且长

白泽平台成长的大部分时间，是在不理解的声音中度过的。

“你们白泽平台这个攻击者画像不就是攻击溯源么？”不断有人问出这个问题。林子翔也只好耐着性子一遍遍解释：“白泽平台的攻击者画像技术是为了分析出这个攻击者是什么类型，而不是这个攻击者是谁。”

一直以来，网络安全行业都有一句很无奈的话：攻防视野不对等，防守方没办法事先知道攻击者是谁，也没办法知道攻击者会从什么地方攻进来，导致攻击成本低、防御成本高。

但我们应该听说过张网已待或者以逸待劳这两个成语。

当白泽平台可以识别出网络威胁主体之后，实际上真正高威胁的，尤其是那种长期惦记你的威胁主体，就完全暴露在了防守方面前。防守方可以用高强度跟踪、诱捕、反制等技术进行针对。

这样安全工作就不再是“救火队员”式的出了问题再应急，而进化成了“上帝视野”，将分析师视野聚焦到高威胁的威胁主体可以将安全事件化解在他成功之前。

即便如此，白泽平台也还有很长的路要走。

“当一个单位 / 一个客户真正需要掌握网络空间战场状况的时候，白泽才会发挥出全部的作用。”林子翔说，白泽平台网络安全治理方法论中的一个环节，其关键在于基于威胁主体的网络安全治理方法。

目前，只有业内部分头部的顶尖客户才会有一些向这个方向上发展的需求。但奇安信坚信这一天即将到来，因为单位的 IT 基础设施在成长，网络安全行业在成长，甚至我们的对手也在成长，总有一天他们会需要飞机将他们送到马车送不到的地方。安

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

1年走完3年路
汽车行业网络安全如何“弯道超车”？广汽乘用车交出一份答卷

作者 研究员 张少波

原本三年的网络安全规划，如何缩短到一年内快速完成？如何在应对各类网络威胁和攻击的同时，确保业务稳定运行、避免中断？如何对纷杂繁琐的安全运营，进行直观的效果评估？……广汽乘用车在数字化转型过程中，不仅快速补齐了内网安全建设短板，还探索建立了更直观、可量化的成熟度模型，在极短时间内，网络安全水平跃居行业前列，并树立了高效建设、持续运营的标杆典范。

网络安全建设迫在眉睫 将三年规划缩短到一年完成

作为世界500强的汽车业龙头，广汽集团近年积极践行数字化转型战略，不断朝着“用户认可的营销数字化行业标杆企业”的企业使命迈进。广汽乘用车贯彻集团的数字化战略，在MES、DMS、数字化办公、财务等领域已经卓有成效，相对成熟，同时在生产、工控环境的数字化建设也在全面展开。随之而来的各类网络安全风险，成为数字化继续深入的重要挑战。

“汽车企业对生产和管理环境的稳定性、可用性要求极高，一旦因为网络攻击而停产或业务停顿，哪怕时间只有几分钟，其损失也是巨大的。”广汽乘用车副总经理黄永生表示，近几年来全球车企因被网络攻击、勒索病毒等造成停产或经济损失的报道屡见不鲜，加上主管部门对安全合规的严格要求，广汽乘用车的网络安全建设已迫在眉睫。

2019年，广汽乘用车邀请专业机构进行了一次自查，发现网络安全水平低于业界平均水平。在网络安全咨询

图：广汽乘用车有限公司

公司的五级模型中，广汽乘用车当时仅有零星的准则或技术手段，未融入到公司的制度和流程当中，处于“低于标准”或者“非正式”阶段。可见，网络安全建设已经到了时不我待的地步。

“最初，即 2019 年，我们结合公司网络安全现状，并参考同行的建设周期，制定了 3 年规划，然而领导要求将三年规划缩短到一年实施完成，即从‘非正式’提升至‘标准化’水平。”黄总表示。

时间紧、任务重、要求高……在当时看来，这无疑是一个几乎不可能完成的任务。然而在公司总经理张跃赛的带领和支持下，以及网络安全咨询公司、奇安信等专业合作伙伴的全力实施下，广汽乘用车内网安全建设最终如期实现了目标。

体系规划、常态落地 一年达成三年目标的“神秘武器”

为什么能够在短短一年内，网络安全部门能实现三年的目标？黄总在规划和组织保障等层面，总结了几方面经验。

首先是网络安全咨询公司为广汽乘用车量身定制了网络安全成熟度模型，让网络安全建设和运营路径清晰、目标具体、效果可量化，从而少走很多弯路。

其次是安全运营建设贯彻了“三化六防”的指导思想。通过安全建设“体系化”、安全运营“常态化”、安全效果“实战化”的思想，解决以往安全离散化、碎片化、单点化等突出问题。

最后是一把手责任制，公司自上而下的整体重视，确保人员团队无短板。网络安全是一项‘一把手’工程，由广汽乘用车党委书记兼总经理牵头成立广汽乘用车网络安全委员会组织，为安全运营提供了强大的组织架构保障。

有了高屋建瓴的体系化规划，再加上强大的组织保障，广汽乘用车的网络安全建设可以说是火力全开、成果显著。在具体落实上，广汽乘用车将各项工作定期化、常态化，比如，每年至少举行 1 次漏洞扫描、10 次渗透测试、2 次应急响应演练活动，以及 1 次网络安全宣传月和 1 次员工网络安全培训。通过这些未雨绸缪的措施，提前发现安全短板和薄弱环节，加速整改夯实基础，让攻击者无机可乘。

图：广汽乘用车 2021 网络安全成熟度

以漏洞扫描和渗透测试为例，安全部门定期开展漏扫及渗透的检查，发现系统主机、应用系统等漏洞，并提供整改建议及对策，杜绝漏洞被利用的风险。通过对 400 多台主机的扫描，共扫描到严重、高危、中危漏洞 4599 个，按计划完成整改后，将使技术领域成熟度提升 25%。

在应急响应演练方面，广汽乘用车邀请奇安信等专业网络安全公司，开展多场

实战化攻防演练，提升当突发网络安全事件时，提供事件分析、溯源、恢复等服务的实战化能力。

2021 年的网络安全宣传月活动，也取得了立竿见影的效果。该活动累计面向 3700 余名员工推送了日常网络安全及安全法规知识屏保共 12 版，让员工在日常办公间隙也能随时学习相关网络安全知识。为了验证效果，网络安全办公室随机向公司内 2000 名员工发送钓鱼邮件，进行网络安全意识测试，点击钓鱼链接提交了个人信息数据的人数由去年的 25% 下降至今年的 5%。

网络安全成熟度接近 4.0 告警逐月递减

经过一年的攻坚，规划的 10 项安全工作计划全部完成，整体成熟度从“非正式”提升至“标准化”水平。根据网络安全成熟度评分，广汽乘用车已达到了近 4.0 分数的成绩，在整个广汽集团中，排名前三，超过了国际业界的平均分 3.6 分，并接近了业界标杆的 4.1 分。

这其中，奇安信提供的以态势感知与安全运营平台（NGSOC）等为代表的产品，为广汽乘用车安全运营提供了强大的技术支撑。而在制度方面，基于广汽乘用车现状，针对常见的业务场景，双方一起规范了日常运维 & 运营处理流程体系，为安全运营提供制度保障。

目前，在该平台的正常运行之下，广汽乘用车整体的“综合安全风险值” 从导入前的 88 分（危急），降低到 2021 年 7 月验收时的 55 分（高危），到 2022 年 4 月，更是进一步降低到目前的 24 分（中危）。

图：广汽乘用车综合安全风险值

以中高危威胁告警举例，自接入 NGSOC 后，威胁告警数量每个月呈下降趋势。以 2021 年 4 月为例，当月中高危告警总计达 322,829 条，到 5 月快速下降到 51,369 条，6 月更是降至 49,251 条。同时，弱口令、木马病毒、外网攻击等告警数量整体都呈现了明显的整体下降趋势。

不仅如此，在广汽乘用车的 5 次重大节假日安全值守中，凭借广汽团队和奇安信驻场团队的紧密配合，依托 NGSOC 发现了多起攻击告警，经研判分析和溯源，

图：广汽乘用车中高危告警趋势图

图：广汽乘用车网络安全运营态势状况

图：广汽乘用车网络安全运营效果分析

及时封堵了攻击 IP，将安全威胁消匿于无形。尤其在 2021 年广州市网信办组织的攻防演练活动中，广汽乘用车作为防守方，取得了核心目标“零失陷”的优异成绩。

未来规划：三层面发力 为数字化转型筑牢安全底座

“网络安全建设只有起点，没有终点”。截至目前，广汽乘用车已经完成了 1 个平台（态势感知与安全运营平台）、4 个系统（终端及虚拟化安全管理系统、网络安全准入系统、上网行为管理系统、业务流量清洗系统）的建设。对于未来，黄总认为，将充分汲取之前 NGSOC 平台运营经验的基础，在三个方面继续发力。

第一是扩大安全运营的范围，除了内网，将终端、服务器等都纳入到整个安全运营体系中，同时在工控内网内，建立起工控安全态势感知与安全运营平台，增强威胁发现和响应能力。第二是继续增强 NGSOC 为核心的平台能力，通过导入资产、漏洞、SOAR 等工具，并对既有规则、制度、流程优化，建立资产与漏洞管理的常态化机制，安全事件响应机制等。最后是全面提升安全运营团队的能力水平，包括通过培训、认证等提升人员整体能力，增补安全运营专岗人员，避免人员能力成为运营短板。

汽车工业是国民经济的支柱产业，数字化转型正在不断加速，而在拥抱数字化的过程中，各种意料之外的网络安全风险正在接踵而来。黄总表示，除了通用网络安全，车联网安全、数据安全、工控安全等都将成为汽车安全中最重要的部分，广汽乘用车将继续在各个领域强化网络安全建设，为数字化转型夯实安全底座。安

你不是一个人在战斗

——走近奇安信网络探针事业部负责人刘洪亮

作者 公关部 孙丽芳

从 5 月 19 日上午开始，奇安信网络探针事业部负责人刘洪亮的手机就响个不停。为了不吵到同事，他后来不得不把手机的来电提醒音给关了。

“都是打过来咨询数据跨境卫士的。”

就在前一天，刘洪亮负责的数据跨境卫士非常低调地进行了发布。虽然对这款产品确实有信心，但市场的反应比刘洪亮此前预料的明显更加热烈。

“北京当时正受新冠疫情的影响，好几个区都要求居家办公，所以我们没有举办线下的发布会，仅仅是由公关部写了一篇名为《奇安信发布数据跨境卫士 为企业数据跨境流动提供合规保障》的稿件，沟通几家媒体发了出去。”

没有行业领导背书，也没有圈内大咖站台，仅凭一篇新闻稿就引发了市场的高度关注，这到底是一款怎样的产品？我们还是先从操刀者刘洪亮说起。

机会留给有准备的人

2002 年，从数学系本科毕业后，刘洪亮先在一家事业单位做教辅材料编写工作。“觉得很不适应，工作比较无聊”。一年后，刘洪亮扔了铁饭碗去读研深造，这次学的是自己喜欢的计算机，网络安全方向。

2014 年，已在网络安全行业滚打历练多年的刘洪亮加盟奇安信，几年下来，业绩出众。2019 年，刘洪亮带领三四十个同事向董事长齐向东请缨，成立了一个新的部门——网络探针事业部，隶属公司的创新 BG。

“我喜欢做点新的东西挑战一下。要是让我一直维护或者搞一个产品的话，可能我就会无聊。而创新 BG 基本上就是新方向比较多。”

2021 年，爱创新的刘洪亮遇到一个好机会。

这一年，数据跨境流动引发了全民关注。一方面，

《数据出境安全评估办法（征求意见稿）》《网络数据安全管理条例（征求意见稿）》陆续发布，对个人敏感信息、重要数据等出境，进行了全面明确的法律规定。同年，数据跨境安全的事件屡次成为社会焦点。6 月 30 日，国内某网约车平台“悄悄”赴美上市，在上市第三天就收到国内网络安全审查办公室针对该企业启动网络

安全审查的公告，原因是“防范国家数据安全风险，维护国家安全”。

数据跨境合规显然已经成为新的市场刚需，而奇安信对此早有洞察。

刘前伟所在的战略规划设计院负责给公司领导做战略决策支撑。“数据安全是国家战略，是行业的发展趋势，所以我们一直在对这个领域进行研究，规划了数据安全的九大方向，里面有一个是 API 安全，数据跨境就是它的一个分支。刚好去年又赶上两个法出台，所以我们判断数据跨境这一块肯定要大爆发。在奇安信这种体量的公司，这肯定是不能丢掉的一环，剩下的只是团队人选问题。而跨境这块和刘洪亮过去搞的另外一个产品 API 安全卫士的底层技术逻辑是一样的，只不过是不同的场景下关注的东西不一样。API 关注在攻防侧有没有攻击，跨境关注重要数据、敏感数据有没有出境。”

2021 年 12 月，公司产管委组织众多产线对数据跨境产品进行了专题研讨。最终，领走任务的正是刘洪亮。

你不是一个人在战斗

有合规驱动和技术积累，数据跨境产品的问世似乎顺理成章，但事情并没有这么简单。“主要是想不清楚市场，不知道具体的应用场景是怎样的，我们的产品是设计给哪些客户的？他们的具体需求是什么？这些都是问题。”刘洪亮心存疑虑。

刘前伟很理解刘洪亮的处境。“其实做创新挺不容易的，新产品从研发到发布，至少要半年甚至更长的时间，相当于你得提前透支你的一部分资源。过去的产品还在售卖，服务要做好，产品要优化，还要再匀出来一波人去做新的东西。在这个新领域，你不但要搞定技术，还要想清楚市场。”

相对成熟市场而言，开拓空白市场的难度显而易见。

好在，刘洪亮不是一个人在战斗。

在数据安全领域做了很久研究的刘前伟是刘洪亮最好的参谋。每隔几天，两个人就要碰一碰，讨论跨境数据产品相关的市场方向，存量的客户在哪，未来的客户在哪。

公司解决方案负责人罗海龙也经常参加讨论。补短板方案中的五件套（特权账号管理、堡垒机、数据库审计、API 安全卫士和数据安全态势感知）是解决政企数据安全问题的当务之急，数据跨境及隐私卫士则可从数据合规切入市场 。

如果说刘前伟、罗海龙的助力属于情理之中，有一个人的加入绝对是意料之外。

“让我对这个事儿最终坚定的是咱法务部的负责人马兰。”

2022 年 3 月的一天，一名销售找到刘洪亮，说有一家律所的律师想咨询一下数据跨境的解决方案怎么做。

“当时我就很奇怪，我们平时接触的都是信息部门，怎么律师还关心这事？我就赶紧给马兰打了个电话。一聊发现，马兰在这方面很有研究”。

“我其实一直和战略规划部的同事在探讨这个事儿。因为我本身是法律专业的，网络安全法、数据安全法和个人信息保护法出来以后，合规很大程度上是由法律口发起的。因为，基于三大法的具体实施条例和管理办法还没有出，所以其实大家并不知道合规怎么做，审计报告可以找审计师出，但这个领域没有第三方评估公司。在这种情况下，市场迫不得已就选择了请律师来出具合规报告和法律风险提示。所以刘洪亮打电话说想做个数据跨境的工具，又了解到有律师在做跨境数据合规业务，问我能不能帮找几个律师一起聊聊？我说这太没问题了，我平时就聊得很多。”

雷厉风行的马兰在之后一周的时间内，给刘洪亮约了三家律师事务所的数据合规业务合伙人面聊。

这几场跨界交流中，马兰充当了“翻译”的角色。“我挺喜欢这种感觉的，我其实也一直在思考如何体现法务的商业价值和核心竞争力。如果说法务只是固守着原来的那些工作内容，如审核公司合同、公司合规情况等，我觉得永远也不可能成为公司的核心。我后来就发现数据合规赛道是完全需要法律和技术相结合的，这正是我们法务和咱们公司所擅长的。所以我就不停的去跟销售、

战规、产品线的同事及律师客户去聊，我希望能用我对法律和市场的了解，去帮助同事开发出新的契合市场需求的产品。”

三轮面聊下来，刘洪亮的信心大增。“因为这几个合规业务合伙人都在讲，数据合规这一块现在刚刚起步，所以大家现在只做高频出现的需求，而跨境数据的合规就属于这种需求。比如说一个中国的企业，我在海外有一些分支机构，那我的数据到底出去了没？还有，比如我过去采购了一些海外的产品和服务，是不是也面临数据跨境的问题。尤其是现在我们的业务系统跑到云上去了，那在后台运行的云端会不会连到美国的服务器、欧洲的服务器？企业于是纷纷找律所来评估自己的数据跨境是否合规。这个需求很大，只是目前还没传导到安全公司，都集中在律所那个层面去了。”

交流中，刘洪亮了解到当前律所评估企业数据跨境是否合规的通常做法就是调查问卷。这种方式的缺陷显而易见。它的前提是建立在企业自己清晰知道哪一些数据进行了跨境，律师再站在法律法规的视角，去判定这些数据出境的合规性和合理性。

“首先最大的问题是企业并不明确知道自己都有哪些数据进行了跨境；其次填完问卷也还是搞不清楚，律师没有技术手段去看这个东西到底实际情况是怎样的。律师们迫切需要一个工具能帮他们把这事干了，这其实就是我们要做的这个东西。再延伸下来的话，其实数据是流动的，律所给你做的评估只是一个项目，不管是一周也好还是一个月，做完就完事了，但是后续随着你的业务变化，数据也会变化。对企业来说，其实需要一个持续监测的产品能实时帮自己查看现在是否合规。与律师的交流，给了我一个新的视角去看这个产品，原来有很大一块市场，我之前自己都没有看到。”

悉心打磨 全力冲刺

磨刀不误砍柴工，通过和刘前伟、罗海龙的充分沟通，以及和律师们的深度交流，刘洪亮清晰了市场方向，坚定了信心，数据跨境卫士的雏形已经在心里勾勒清楚。

但实际的开发工作并不一帆风顺。

“首先是缺人，我们部门今年并行开发6个新产品，跨境数据卫士之前没在规划内，所以根本就没人。”

人的问题必须解决，刘洪亮找到创新BG负责人孔德亮。孔德亮非常支持这项工作，专门调配了一笔费用。刘洪亮迅速组建了一支团队。

“第二个就是数据安全的东西太新了，对团队的挑战很大。虽然之前我们做流量探针有一些技术积累，但是两者并不完全一样。所以我们又成立了一支数据运营团队，专门运营各种数据的规则，那段时间把 leader 逼的都快崩溃了，都觉得自己不适合干这个。因为我们做数据安全相关的产品全是在碰数据，而每个客户的数据都不一样，且不同客户对重要数据的定义是不一样的，制定规则的人得了解行业，还要自己去找这类数据的样本，然后还得能把它识别出来，这确实很有难度。有些行业数据我们根本就不清楚，比如，一些信贷相关的金融数据，染色体相关的医疗数据，我们没有相关的知识积累，压力确实非常大。”

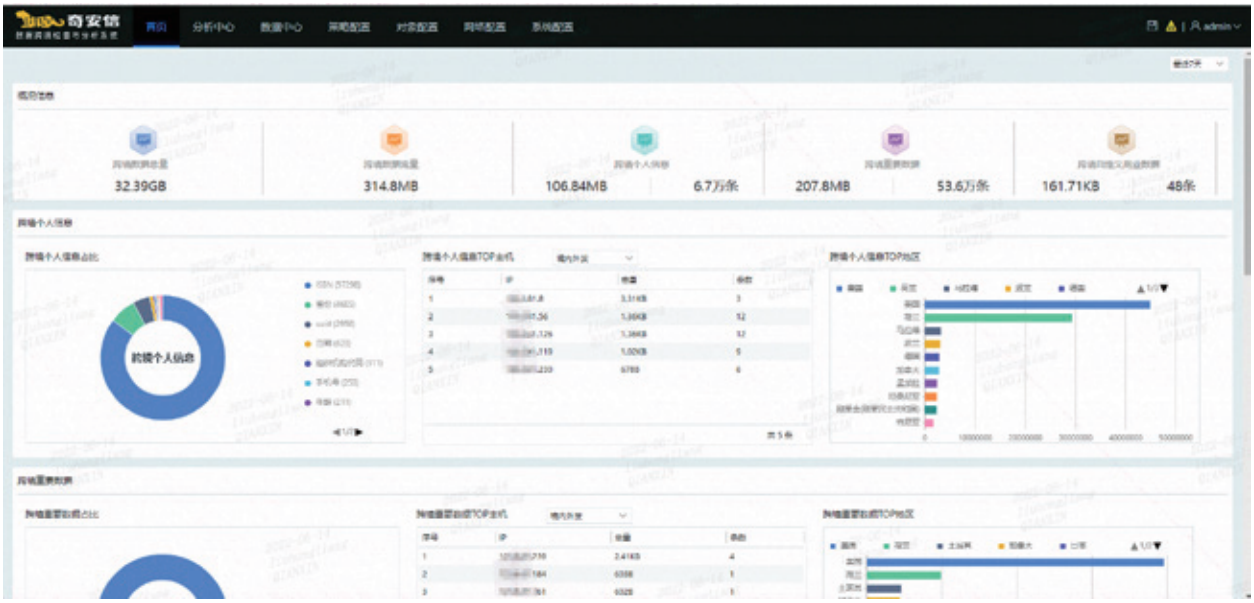
不过，技术上的困难没有困住刘洪亮和团队。刘洪亮带领大家一起先梳理出若干种技术手段，再找到足够的样本，用这些技术手段把大部分行业的数据覆盖掉。打通技术之后，刘洪亮组织大家做精细化的数据运营，把工作划分得非常细，每一块都安排专人去做，相当于建立了一条流水线，这样对每个岗位的人员要求不那么集中了，效率得到了总体提升。

第三个问题是进度压力。按照规划，数据跨境卫士在5月份就要投放市场。这也就意味着，集中研发的时间只有一个多月。

“我们感受到市场对跨境数据安全的需求太强烈了。5月份其实是我拍脑袋拍的一个时间点，因为想要产品的需求太多太迫切了。不过，对于从网络流量里提取数据这件事，我们是非常自信的。”

如期发布 始终协同

挑战难度，自己给自己加码，这是刘洪亮的一贯风



数据跨境卫士运行界面

格。而这次，刘洪亮又挑战成功了。5 月 18 日，奇安信跨境数据卫士如期对外发布。

作为数据安全建设中重要的一环，跨境数据卫士不仅能解决企业跨境传输的数据能满足《数据安全法》《个人信息保护法》、数据跨境监管等合规要求，还能对敏感数据的跨境流动情况进行全局、清晰和直观的掌控。

“把数据跨境卫士放置在企业的互联网出入口，就是与外界建立通信的地方，企业所有对外流出的数据都会在流量当中体现，那么将我们的产品部署在这块，对这些流量进行具体分析，将流量里面所带的个人信息、重要数据、商业数据等进行数据提取，在产品里面形成一个可视化的界面，供企业浏览。可以清晰的在界面上看到，我们企业数据出境都包含了哪些数据，涉及个人信息相关的，涉及的重要数据、商业数据等。这样通过我们的产品，就可以很好地对企业出境数据进行统计分析展现，个人信息出去了多少，重要数据出去了多少，出去了多少量，出去了多少条。因为在个人信息保护法里面有明确规定，当企业的个人信息出境了多少 G 或多少条时，会触发法律红线，比如，身份证号、姓名、征信报告等一共出去了10万条，那么就会面临着罚款通报，通过我们这款产品可以自动化的将企业的出境数据进行整合，形成一眼可知、一眼可查、一眼可见。”

清晰的产品定位直击客户痛点。“香港的一家金融客户，还有深圳的一个律所联盟，看到我们的产品发布新闻稿之后就想办法找到了我们，希望能做进一步交流。产品发布后的两天，我接到了几十个这类的需求。我们的产品经理正在给各个行业的客户做客户画像，先挑了几个行业，重点去推，现在有两个车企马上要进行试用了。同时，我们也在加班加点完善产品的技术细节。”

产品虽然已经上市，接下来的工作还有很多。刘洪亮的“助力团”也在继续出谋出力。

刘洪亮一直和刘前伟保持高频沟通，他用一句东北俗语概括了两个人的关系。“我们俩从去年开始到现在，都是两天不聊三天早早的，也就是说，两天不聊的话，第三天早早的就要聊。因为战略规划设计院对整个数据安全这套体系，包括国内外的相关产品和方案，研究得

非常透。”

而前期给了刘洪亮很大支持的马兰，甚至从幕后走到了台前，直接帮产线“带货”。

5 月 21 日，法律圈召开了一个数据合规线上论坛，马兰受邀进行发言。现场，她向大家重点推介了数据跨境卫士。讲解过程中，不断有参加论坛的律师提问，大家的反应非常热烈。

“法务和技术之间的语言和思维体系有很大的差别，中间得有一个衔接，能把数据合规这个问题从法律的角度和技术的角度，串在一起讲明白。所以这种情况下，我们要大量的去跟律师事务所合作，律师可以充当客户和我们之间的衔接桥梁。而我们的技术单独去和律师沟通还是存在难度，所以他们来找我，我就尽我所能去帮忙。”

协同作战的情况不止存在于数据跨境卫士。

目前，创新 BG 中成立了数据安全专班，内部不再分产品线，也打通了部门界限，围绕现有的几款数据安全产品，产品线、战规、解决方案高效合作，协同推进。

“接下来我们就是把数据跨境卫士全面推向市场，在市场中进行完善和优化。”刘洪亮的脚步越来越坚定。

6 月 9 日，国家市场监督管理总局、国家互联网信息办公室发布《关于开展数据安全管理认证工作的公告》，决定开展数据安全管理认证工作。这意味着数据安全管理认证有章可循或将进入常态化监管阶段。

“我觉得数据安全的市场非常大。未来，我希望能在自己的领域里不断地前进。这不光是我，也是所有奇安信人的目标和追求，因为我们的公司文化就是这样。在这里，你不是一个人在战斗，全公司所有人齐心协力，每天都在拼命地往前冲。”安

数据跨境卫士团队合影

规划快一步

奇安信

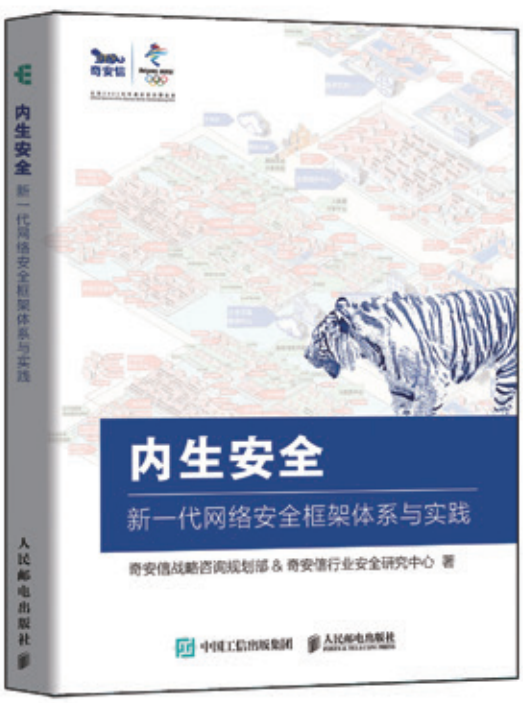
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

数据安全大考
四大丢分细节，你都踩坑了吗?

作者 研究员 魏开元

2022 年高考结束了，让职场人感叹幸亏毕业早的作文题、让考生祈祷“韦神附体”的数学也都随之落下了帷幕。

作为人生中首个重要的“三岔路口”，高考承载了太多太多，以至于在那些早已远离高考十几二十年的朋友中，还能听到当年我要是多考几分就能怎样怎样的声音。

诚然，对于普通人而言，想要考高分是一件非常困难的事情，但是考一个相对还不错的分数，却是有迹可循。对于高考而言，基础题比例大概是 80%，只有稳稳拿下这些分数，并在有余力的基础上攻坚高难度题目，才能考取一个理想的成绩。尤其是今年高考，陡然增加的试题难度，让仅仅抓住基础题显得更加重要。

不过即便是学霸，也不敢百分之百保证基础题一分不丢。作为考生，必须得学会识别考试过程中的一个又一个坑。

同样的道理，在数据安全领域也适用。随着《数据安全法》《个人信息保护法》等相关法律法规的出台，政企机构不得不思考如何在“数据安全大考”中，考取一个好成绩。

对此奇安信认为，面对日益严峻的数据安全形势，大量政企机构依然处在数据“裸奔”状态，只有首先解决了裸奔问题，才能做好后续的系统治理和持续运营。

那么，在解决数据裸奔的过程中，都会遇到哪些坑呢?

第一，特权账号管理薄弱

笔作为考生书写答案的唯一工具，按照规定，考生应当使用 0.5mm 黑色签字笔和 2B 铅笔，在规定的地方规范答题。可每年总有一些考生不当回事，有用蓝笔、红笔的，有使用非 2B（如 6H、6B）等或者不合格的 2B 铅笔的，有答题卡涂错位置的，有字写得自己都不认识的，甚至有将答案写在答题框外面的，等等，这些都有可能导致机器阅卷出现异常，从而丢掉本应该得到的分数。

同样，作为通往企业数据大门的“钥匙”，在业务流程中对重要的数据进行访问或操作都需要经过特权账号，其重要性几乎等同于考试用笔。特权账号的使用人群非常复杂，包括数据采集者、数据分析师、数据生产人员、开发人员、运维人员等，覆盖数据库、中间件、网络设备、安全设备、虚拟机、服务器等。一旦特权账号使用不当或者被窃取，都会给数据安全带来非常大的隐患。

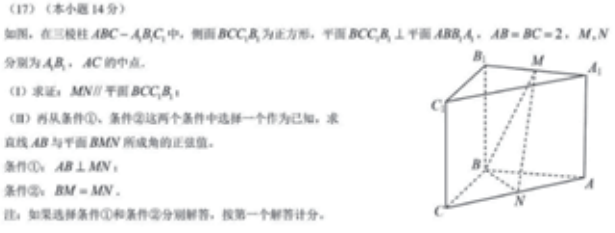
特权账号存在的最常见问题莫过于普遍使用 123456 之类的弱口令了，且没有设置口令强度或者定期修改的规则，破解起来几乎不费吹灰之力。比如，乌克兰武装部队的“第聂伯罗”军事自动化控制系统就使用了 admin/123456 的弱口令，甚至在被破解之后还不以为然。

另外一个问题就是对特权账号无感知，内部大量存在私自创建的、废弃但尚未销毁的、甚至是多人共用的特权账号，一旦相关用户出现问题，都不知道从何查起。

针对这部分问题，奇安信特权账号管理系统能够主动发现各类基础设施资源的账号分布、识别账号风险（包括弱口令、僵尸账号、幽灵账号、长期未改密账号，账号违规提权等）、管理账号使用，实现对各类基础设施资源账号的全生命周期管理。

第二，权限控制措施不力

考生在做几何题时，通常会用到做辅助线的方法。例如，2022 年高考数学北京卷立体几何题第一问中，考生需要证明线面平行，则通常需要在该面上引入一条辅助线，并通过证明线线平行得到线面平行的结论。


（17）（本小题 14 分）
如图，在三棱柱 $ABC-A_1B_1C_1$ 中，侧面 BCC_1B_1 为正方形，平面 $BCC_1B_1 \perp$ 平面 ABB_1A_1，$AB=BC=2$，M，N 分别为 A_1B_1，AC 的中点。
（I）求证：MN // 平面 BCC_1B_1；
（II）再从条件①、条件②这两个条件中选择一个作为已知，求直线 AB 与平面 BMN 所成角的正弦值。
条件①：$AB \perp MN$；
条件②：$BM=MN$。
注：如果选择条件①和条件②分别解答，按第一个解答计分。

但在有些时候尤其是题目难度较大时，会引入多条辅助线，这就导致考生经常会陷入一个僵局：要是这两条边相等、这两个角相等……结论不就出来了么。在脑袋不那么清醒的情况下，考生很容易就会犯下错误，将原本假设的两边相等 / 两个角相等误认为是已知条件，超越了题设赋予考生的“权限”，从而导致解题过程全部错误。

与之类似的是，数据的访问和使用也必须遵守一定的权限。然而，动态化、多样化的访问和接入，改变了信息化环境，极易引发权限管理不清、监督不力的情况，从而导致对访问数据的身份没有认证、对访问数据的权限没有监督，以及对访问数据的行为没有审计和控制，很容易引发数据安全事故。

例如，近两年比较火热的程序员跑路删库事件，无一例外都给企业造成了严重的损失。作为离职或者即将离职的员工，其访问数据的权限应当受到一定的限制，访问数据的行为也应当受到严格的管控和事后的审计，才能最大限度的杜绝此类事件发生。

对此，奇安信网神运维审计系统能够实现对企事业 IT 中心的网络设备、数据库、安全设备、主机系统、中间件等资源统一运维管理和审计，为客户提供集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计等功能，满足全行业运维审计规范要求。

同时，奇安信数据库审计与防护系统通过大数据分区搜索技术提供高效检索审计记录能力，快速定位事件原因，帮助用户事后生成合规报告，提供有效电子取证信息，用于数据安全事故的追根溯源，加强内外部数据库网络行为的监控与审计。

第三，API 疏于防护

作为阔别象牙塔多年却唯一没有还给老师的技能，作文可以说是每年高考期间都被热议最多的话题之一了。今年高考语文全国甲卷作文材料来源于红楼梦，就有大量网友认为作文题目真难懂，甚至有人评价说曹雪芹来了都要直呼高手。

实际上，写作文的最大坑就是审题，考生很容易搞不清楚材料中的关键点在哪，理解是否正确，一旦审题出现偏差，文章写得再好，分数也不会太高。要想审题不出现偏差，就得认真从作文材料中找出关键要点，并将出题人的真正意图“调用”出来，并反馈在文章里。

在 IT 系统中，能够起到数据调用作用的组件叫作应用程序接口（API），它能够帮助应用程序非常方便地获取并使用第三方数据。随着数据流动性的大幅增加，API 的使用几乎无处不在。

与此同时，针对 API 的攻击正在成为攻击者窃取数据的重要途径之一。据 Salt Labs 发布的《2022 年第一季度 API 安全状况报告》显示，过去 12 个月，恶意 API 流量增加了 681%，95% 的组织都经历了 API 安全事件。例如，2021 年 6 月，黑客通过领英的 API 漏洞，获取到领英 7 亿多用户的个人数据，并在暗网公开销售；2021 年 12 月，国内某证券公司客户信息数据，以每日 1 万多条的量级在数据交易平台被售卖，经证实为内部 API 管控疏忽导致。

究其原因，主要包括 API 资产不清，无法有效管理；API 安全检测和安全分析能力缺失及 API 安全管控、安全防护无有效方案。

面对此情形，奇安信 API 安全卫士具有基于自动化发现并可视化展示及管理 API 能力，在检测传统 Web 攻击同时，还可检测和预警 API 传输中的敏感数据，建立基于用户访问行为的用户画像或行为模型，发现 API 未认证访问、弱口令登录、未授权访问、异常访问行为等。

第四，风险感知能力缺失

除了作文，另外一个吸引人眼球的话题就是提前交卷的考生了。但对于做题速度快的考生来说，答完题后认真检查一遍能够最大限度地避免低级错误的发生。尤其是在数学和物理考试最后一道解答题，尽管题目难度不小，但绝大多数情况下最终结果都相对简单，数据不会太大，如果最终算出来的结果太复杂（如根号里面套根号、小数点后面大几位甚至十几位），就要想想自己是不是算错了，或者是没有化简成最终结果。这就要求考生要有对已经发生的错误，有充分的感知能力。

（20）（本小题 13 分）

设$\{a_n\}$和$\{b_n\}$是两个等差数列，记

$$c_n=\max\{b_1-a_1n,b_2-a_2n,\ldots,b_n-a_nn\}(n=1,2,3,\ldots),$$

其中 $\max\{x_1,x_2,\ldots,x_s\}$表示 $x_1,x_2,\ldots,x_s$ 这 s 个数中最大的数.

（Ⅰ）若 $a_n=n$，$b_n=2n-1$，求 c_1,c_2,c_3 的值，并证明$\{c_n\}$是等差数列；

（Ⅱ）证明：或者对任意正数 M，存在正整数 m，当 $n\geq m$ 时，

$\frac{c_n}{n}>M$；或者存在正整数 m，使得 $c_m,c_{m+1},c_{m+2},\ldots$ 是等差数列.

而在数据安全中，政企机构对于已经发生的数据泄露事件感知能力普遍偏弱。这主要是由于政企机构普遍缺乏多维度的数据安全风险感知能力。即使对特权账号、访问权限、访问行为进行了监控审计，但都是单一维度，无法掌握全貌，导致风险感知不及时，甚至安全事件已经发生还不知情。主要表现为后台操作无法审计、发生事故无法溯源；访问行为缺乏记录，风险访问无法识别；海量日志无法分析，风险感知能力缺失。

IBM 报告显示，2021 年识别一起数据泄露事件平均需要 212 天，遏制一起数据泄露事件平均需要 75 天，总生命周期为 287 天，这对于降低损失是极为不利的。

对此，奇安信数据安全态势感知运营中心能够主动扫描数据资产，识别敏感数据，建立数据目录并分类分级，检查敏感数据驻留风险，建立敏感数据分布态势，通过全流量深度解析，自动梳理涉敏资产，建立敏感数据流动态势，及时发现可疑行为。

特权账号管理、堡垒机、数据库审计、API 安全卫士和数据安全态势感知作为奇安信最新数据安全五件套，能够帮助政企机构在数据安全建设过程中的“补短板、防裸奔”期间，针对特权账号的全生命周期统一管理、访问的安全管控与审计、数据访问行为的审计、API 接口的防护与态势感知建立的多维度监控，进行全方位的数据安全保障，避免踩到上述四大坑。安

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

威胁情报中心

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

大事记

齐向东出席 2022 数博会：数据安全是“东数西算”的底板工程

5 月 26 日，2022 中国国际大数据产业博览会召开，奇安信集团董事长齐向东在“东数西算：构建国家算力网络体系”论坛上指出，“东数西算”是我国发展数字经济的重要举措，同时海量数据的“裸奔”是数据安全的首要问题，奇安信未来将全力助力贵州“东数西算”稳健发展。

针对目前政企机构重要数据资产的防护需求，齐向东从北京冬奥数据安全建设实践中，总结出了补数据安全短板的三大关键措施：第一、盘清家底。系统梳理业务系统、应用、数据等，掌握重要的数据存在哪、谁在使用、如何使用，梳理已有安全措施是否应用于重要数据资产的环境，形成数据资产梳理报告。第二、分级分类。针对不同级别的数据，制定不同的安全策略。第三、精细防护。围绕重要数据资产进行精细化安全防护，来提高整体防护水平。

奇安信举行百余场冬奥网络安全“零事故”经验分享会

为充分发挥好、运用好“冬奥遗产”，2022 年 6 月，奇安信举行了百余场冬奥网络安全“零事故”经验分享会，其中包括人民银行、平安集团、北汽集团、宁德时代、中国人寿、贵州省委网信办、上海市委网信办等重点企业和政府机构，覆盖 32 个省、市、自治区。

今年 3 月，北京 2022 年冬奥会和冬残奥会组织委员会向奇安信发来感谢信，并提出希望奇安信认真总结相关经验，形成“奥运遗产”。为此，奇安信专门成立冬奥网络安全保障“零事故”经验宣讲团，面向银行、通信、电力、制造业、医疗等重点关基行业举办百余场经验分享会，积极推广实战化、可落地、可复制的网络安全技术方案，为网络强国筑牢安全底板。

扩展云安全运营之路 奇安信云安全再获信通院认可

6 月 10 日，由中国信通院主办的“可信安全 · 安全运营发展论坛”上，中国信通院云大所副所长栗蔚发布了 2022 年可信云安全的最新评估结果。

作为奇安信打磨多年，兼顾云计算环境特性和客户安全运营管理需求的平台型

产品，奇安信云安全运营中心（CSC）顺利通过本次“安全运营中心能力评估”，结合奇安信在云安全和安全运营两个领域的优势资源，为云安全运营“从无到有，从有到优”贡献自身价值。

奇安信与吐鲁番市合作共建吐鲁番市网络安全教育基地正式揭牌

6 月 13 日，吐鲁番市网络安全教育基地在吐鲁番职业技术学院正式揭牌。

作为“政、校、企”三方合作的网络安全项目，吐鲁番市网络安全教育基地是由湖南省援建，吐鲁番市委网信办、吐鲁番职业技术学院、奇安信集团共同打造的新一代网络安全专业人才培养和网络安全宣教教育基地。

基地设有网络安全教育展厅、网络安全攻防实验室、网络安全认证培训中心及学术报告厅等专业硬件设施，配备有认证实训平台、攻防应用软件等一批专业应用平台，收集了大量网络安全宣传视频资料，未来将建设成为吐鲁番市党员干部的网络安全教育基地、重点行业网络安全工作人员的培训基地、网络安全知识技能宣传普及基地，持续为新疆乃至整个西北地区的高速发展提供信息安全助力。

共筑发电行业网络安全“护城河” 奇安信与国电南自达成战略合作

6 月 13 日，奇安信与国电南京自动化股份有限公司签署战略合作协议，并为“网络安全联合实验室”揭牌。

根据协议，双方将就发电行业工控网络安全、内生安全、新技术研究与创新应用等方面展开全面合作，共同打造发电行业网络安全产业新生态。同时，双方还将重点围绕联合实验室建设、保障发电行业网络与信息安全联合开展科研攻关。

奇安信集团受邀亮相 RSAC2022 展示冬奥网络安全“零事故”创新

一年一度的全球网络安全盛会——RSAC2022 于美国时间 6 月 6 日开幕，奇安信集团受邀亮相，全面展示守护北京冬奥网络安全“零事故”的“中国方案”。

奇安信集团携多款先进的网络安全产品亮相 RSAC 线下展区，全方位展示在北京冬奥网络安全保障中发挥

重要作用、实现“零事故”世界纪录的多款产品：威胁监测与分析系统（天眼）、奇安信终端安全管理系统（天擎）、威胁情报平台、安全编排自动化与响应系统（SOAR）、Web 安全网关（SWG）等。

奇安信公益基金会“眼明心安”项目启动 为西藏眼疾患儿点亮未来

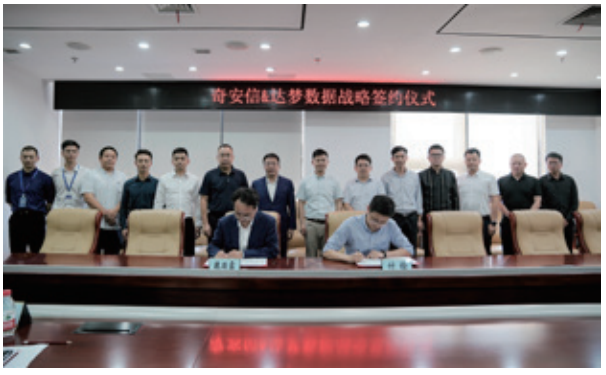
6 月 6 日，在第 27 个全国爱眼日之际，由北京白求恩公益基金会与北大医学（包括北京大学人民医院、北京大学第一医院、北京大学第三医院）眼科专业力量携手共同发起，北京奇安信公益基金会支持的“白求恩 · 眼明心安——西藏儿童盲及低视力诊疗能力提升项目”正式启动。

在项目实施过程中，北京白求恩公益基金会、北京奇安信公益基金会、北京大学人民医院各司其职，整合资源，以实现“促进眼科专业人才培养，助推西藏自治区眼科医疗服务高质量发展，不断提高人民的眼健康水平”的目标。

奇安信与达梦数据达成战略合作 打造国产数据库一体化产品

5 月 31 日，奇安信集团与武汉达梦数据库股份有限公司签署战略合作协议。双方将基于信创的数据安全技术和产品创新、信创的数据安全方案开发和应用推广等方面展开深入合作。

奇安信集团总裁吴云坤表示，探索和实践信创领域的安全可靠技术发展，尤其是基于信创的数据安全技术发展，保障国家经济社会数字化转型中的数据生产力安全发展，将是达梦数据和奇安信共同的责任和使命。奇安信也将调集公司优势资源，组织专班，以专项攻坚方式，集中优势技术、产品、能力、服务资源，积极推进双方合作项目落地。



2021 中国网站安全报告：11.5 万个网站被报告安全漏洞 14.6 万个

近日，奇安信行业安全研究中心等内部多部门联合

发布《2021 中国网站安全报告》，从高危端口暴露、第三方漏洞报告、网站攻击拦截、DDoS 攻击、僵尸网络等维度，对 2021 年国内网站安全的整体状况展开了深入的分析与研究。

《报告》显示，2021 年全年，补天漏洞响应平台共收录全国各类网站安全漏洞146,293个，共涉及网站 115,243 个；奇安信网站卫士共为全国 40.3 万个网站拦截各类网站攻击 95.1 亿次，平均每天拦截攻击 2,604.9 万次；奇安信技术研究院累计监测到全国 28.7 万个 IP 遭到 84.2 万次 DDoS 攻击。

奇安信集团与南京航空航天大学达成战略合作 打造安全协同创新中心

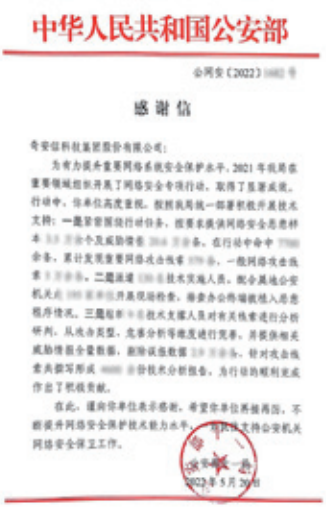
5 月 26 日，奇安信集团与南京航空航天大学签署战略合作协议，双方将围绕专业共建与人才培养、打造航空工业互联网安全协同创新中心、共建数字校园安全运营体系等方面展开深入合作。

根据协议，校企双方将成立协同创新合作领导小组，重点在三方面达成合作：在专业共建与人才培养方面，双方充分发挥在航空航天和网络空间安全行业领域的技术优势，打造网络空间安全协同育人平台，联合建设网络安全国家一流课程；在共建安全创新中心方面，将围绕工业互联网、工业领域的数据安全与隐私保护、无人机安全防护、物联网等重点和前沿领域，共同开展技术研究和创新探索，力争成为该领域国内领先、世界一流的创新中心；在建设数字校园安全运营体系方面，将奇安信在冬奥中形成的安全运行保障能力和成果在南航落地实施，逐步建立完善基于内生安全框架及零信任等先进技术的数字校园网络安全运营体系和运营模式。

荣誉墙

圆满完成网络安全专项行动任务 奇安信获公安部感谢信

近日，公安部向奇安信集团发来感谢信，以表彰奇安信在 2021 年公安部网络安全专项行动中，支持网络安全保卫工作所做出的积极贡献。作为新一代网络安全企业，奇安信充分发挥自身优势，组织专业力量，调动资源，全面支持专


中华人民共和国公安部

感 谢 信

项行动，并圆满完成任务。

据悉，此次专项行动，是公安部专门针对国家关键基础设施领域开展的安全检查工作。奇安信集团作为网络安全企业，在行动中充分发挥扎实的人员、技术、专业等方面优势，积极开展工作。

奇安信获冬奥网络安全保障“表现突出单位”荣誉称号

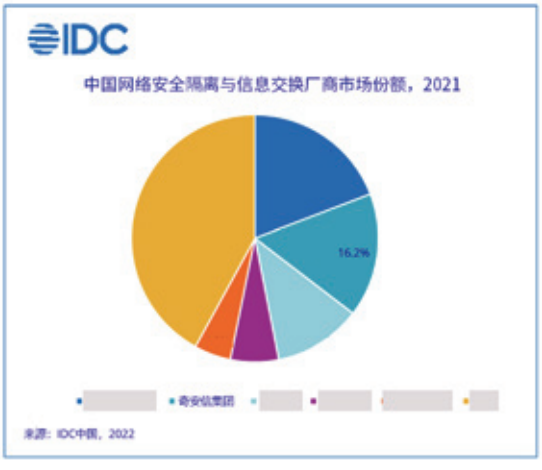
近日，北京冬奥会网络安全工作协调小组（中央网信办）发出感谢信，对奇安信集团在北京 2022 年冬奥会和冬残奥会网络安全保障工作中提高站位、精心组织，以高度的政治责任感和历史使命感完成相关任务，特予以表扬。

北京冬奥会网络安全工作协调小组（中央网信办）授予奇安信集团“表现突出单位”荣誉称号，授予奇安信集团董事长齐向东、副总裁张翀斌、关基总体部安全架构部总经理尹智清“表现突出个人”荣誉称号；同时，授予奇安信集团首席战略官、副总裁刘勇，党委副书记、副总裁蒋虎“积极参与个人”荣誉称号。

连续多年位居前列 奇安信安全隔离与信息交换系统市场份额持续扩大

近日，全球领先的 IT 研究和咨询机构 IDC 发布《中国安全隔离与信息交换市场份额，2021：场景落地加速，市场稳定发展》研究报告，奇安信凭借其安全隔离与信息交换产品在市场上的长期高光表现，增长率持续扩大，以 16.2% 的市场份额连续多年位居市场前列。

据了解，网闸产品是一款极具“中国特色”的产品，由于其安全隔离性强、安全级别高的特点，在国家力推的等级保护和重要行业安全建设规范中被广泛采用，历史上被认为是一款强合规驱动的安全产品。



奇安信开源软件供应链安全技术应用方案获 2022 数博会“新技术”奖

5 月 26 日，2022 数博会领先科技成果奖获奖名单正式公布。“奇安信开源软件供应链安全检测关键技术与产业化应用”荣获 2022 领先科技成果奖“新技术”奖。

在北京 2022 年冬奥会和冬残奥会期间，该项目成果应用于软件供应链安全预警工具的升级工作。针对冬奥网络安全环境中软件来源复杂、安全窗口短暂的需求，通过模块化能力扩展，将开源软件识别数量从 800 万提高至 3000 万，可识别的开源代码模块数量从 2 万提高到超过 8 万，漏洞库中包含的漏洞数量从 3 万提升到 12 万，明显增强了对冬奥赛事系统软件供应链的安全预警能力。

奇安信“95015”获数博会领先科技成果奖

2022 数博会“数博发布”环节正式公布了领先科技成果奖项目 55 项，其中，“新产品”24 项、“新技术”26 项、“商业模式”5 项。“奇安信冬奥网络安全应急响应 95015 公共服务平台”获领先科技成果奖“商业模式”荣誉。

“奇安信冬奥网络安全应急响应 95015 公共服务平台”目前已覆盖全国 31 个省份、2 个特别行政区，有 2000 多名具备攻防能力的应急响应工程师和 100 多名资深安全专家，7*24H 随时待命，2 小时内可到达现场处置。自 2016 年以来，奇安信依托网络安全应急响应 95015 公共服务平台，开展了丰富的应急响应实践，处置政企机构网络安全应急事件 4000 起，投入工时超过 250000 小时，为党政军企解决网络安全问题，获得客户高度认可和一致好评。

2022 IT 市场权威榜单：奇安信获九项荣誉

近日，赛迪发布“2022 IT 市场权威榜单”，奇安信集团获得“新一代信息技术领军企业”“新一代信息技术领袖人物”“新一代信息技术创新产品”“数字化创新实战案例”四大类别共计九个奖项，全面肯定了奇安信在信息技术领域的技术实力和创新能力。

奇安信科技集团股份有限公司荣获“新一代信息技术领军企业”，奇安信集团董事长齐向东获“新一代信息技术领袖人物”荣誉，“奇安信北京冬奥会网络安全保障任务”荣获“数字化创新实践案例”。奇安信网神态势感知与安全运营平台（NGSOC）、奇安信天擎终端安全管理系统、奇安信网神云锁服务器安全管理系统、奇安信网神云安全运营中心（CSC）、奇安信网神威胁监测与分析系统（天眼）、奇安信特权账号管理系统（PAM）6 款在北京冬奥网络安全保障中发挥重要作用的网络安全产品，在本次榜单中被评选为“新一代信息技术创新产品”。

APP 违规收集个人信息风险分析报告（2022 年第一季度）

发布机构　奇安信病毒影响中心

概要

2022 年第一季度，奇安信病毒响应中心共收录全国应用市场新增 APP 活跃样本近 30 万个。本报告依据《APP 违法违规收集使用个人信息行为认定方法》等内容要求，使用奇安信自研安卓动态引擎 QADE 对新增 APP 样本进行抽样检测，重点评估“无提示收集个人信息”和“高频次收集个人信息”两种最为常见、影响较深的合规性问题。

报告发现，APP 违规收集个人信息的现象仍然十分普遍，平均每 5 个 APP 中，就有一个存在违规收集个人信息的风险。部分存在违规收集个人信息风险的 APP 社会影响面巨大，网上购物、生活休闲、办公商务等常用 APP 的违规风险问题最为突出。此外，八成以上的违规个人信息收集行为是由于 APP 集成了某些不规范的第三方 SDK，或者是没有对第三方 SDK 收集个人信息的行为进行声明造成的。

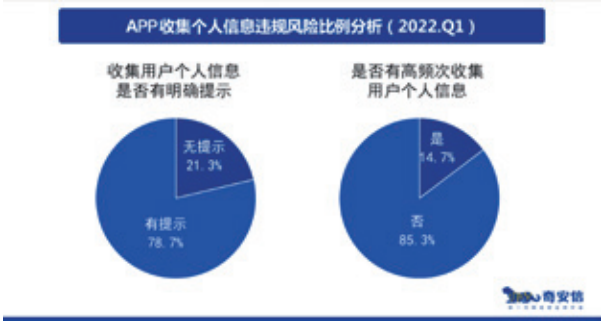
第一章 流行 APP 违规风险形势分析

随着互联网和移动设备的发展，手机已成为人人都拥有的设备，APP 的流行使人们对 APP 违规收集个人信息的风险更加担忧。为切实加强用户个人信息保护，工业和信息化部为此发布了一系列的相关法律法规和监管标准通知，并在全国范围内组织开展 APP 违法违规收集使用个人信息专项治理工作。

一、 存在违规风险的 APP 规模

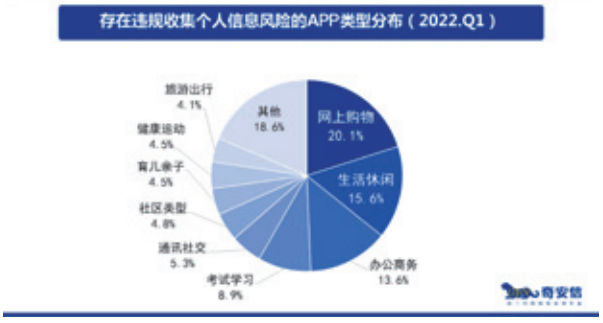
2022 年第一季度，在针对近 30 万个新增活跃 APP 样本的抽样检测中，存在“无提示收集个人信息”风险和“高频次收集个人信息”风险的 APP，分别占到检测样本总量的 21.3% 和 14.7%。总体来看，平均每 5 个 APP 中，就会有一个存在个人信息收集方面的违规风险。

本季度检出的所有存在违规风险的 APP 中，至少有 1 款下载量超过 1 亿次，4 款下载量超过 1000 万次，19 款下载量超过 100 万次。仅这 24 款 APP 就至少影响国内超过 2 亿用户。



二、存在违规风险的 APP 类型

从 APP 类型来看，在 2022 年第一季度的检测中，存在违规风险最多的 APP 是网上购物类 APP，约占所有存在违规风险 APP 总数的 20.1%。其次是生活休闲类，占比为 15.6%。办公商务类排名第三，占比 13.6%。

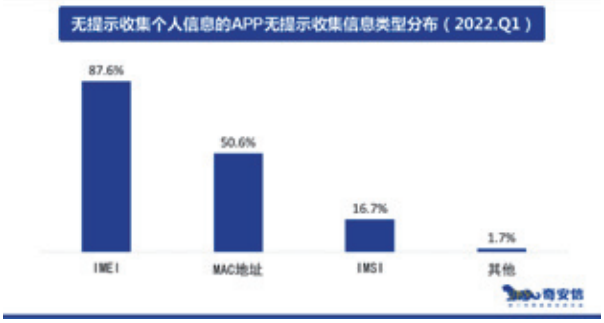


第二章 典型 APP 违规风险形势分析

一、无提示收集个人信息类型分析

在所有存在“ 无提示收集个人信息”风险的 APP 中，IMEI、MAC 地址和 IMSI 是 APP 静默收集个人信息最主要的 3 个类型。其中，87.6% 会无提示收集 IMEI 信息，50.6% 会无提示收集 MAC 地址，16.7% 会无提示

收集 IMSI 信息，而无提示收集其他个人信息的情况，仅占 1.7%。



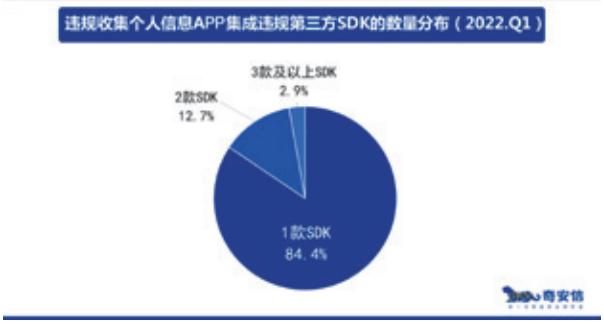
二、高频次收集个人信息情况分析

在 2022 年第一季度检测的所有新增活跃 APP 样本中，一百秒内收集用户个人信息超过 2 次（包含 2 次）的 APP 占到了所有被检测 APP 总量的 14.7%。在所有存在高频次收集个人信息风险的 APP 中，每一百秒收集个人信息次数大于等于 2 次，但低于 5 次的 APP 约占 44.0%；6~10 次的占比 28.7%，11~20 次的占比 18.8%，大于 20 次的占比 8.5%。

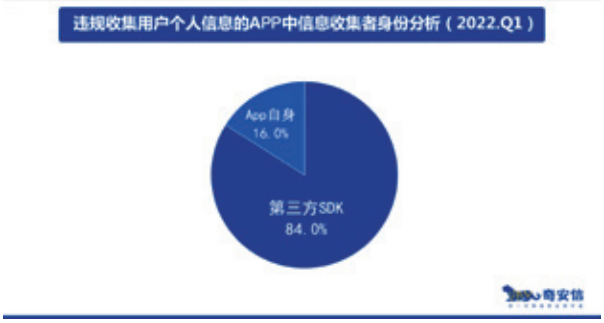
在本季度的检测中，发现某款收集个人信息最为频繁 APP，在一百秒内对 IMEI 信息收集了 138 次，平均每秒 1.38 次。

第三章 违规个人信息收集者分析

APP 对于用户个人信息的收集，未必都是由 APP 自身来完成的，很多时候是因为 APP 集成了第三方 SDK，而第三方 SDK 存在个人信息收集行为。统计显示，在所有存在“无提示收集个人信息”和“高频次收集个人信息”风险的 APP 中，对用户信息进行违规收集的，84.0% 属于第三方 SDK 行为，仅有 16.0% 属于 APP 自身行为。检测还发现，有两款知名的第三方 SDK，分别覆盖了存在违规行为的 APP 总量的 29.0% 和 21.0%。



统计显示，在所有集成了违规收集个人信息 SDK 的 APP 中，只集成了 1 款违规 SDK 的 APP 占比为 84.4%，集成了 2 款违规 SDK 的 APP 占比为 12.7%，另有 2.9% 的 App 集成 3 款及以上的违规 SDK。



附：发布机构介绍

奇安信病毒响应中心是奇安信集团旗下的专业病毒鉴定及响应团队。中心以奇安信核心云平台为基础，拥有每日千万级样本检测及处置能力、每日亿级安全数据关联分析能力。结合多年反病毒核心安全技术、运营经验，基于集团自主研发的 QOWL 和 QDE 引擎，形成跨平台木马病毒查杀能力与漏洞修复能力，并且具有强大的大数据分析能力，可以实现全平台安全和防护预警能力。

奇安信
新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结
从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

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

网络安全 中国代表队 | 奇安信

2022年北京冬奥会胜利闭幕

“零事故”

奇安信圆满完成冬奥会网络安全保障任务

奇安信蝉联“中国网安产业竞争力50强”第一名

6月23日，中国网络安全产业联盟（CCIA）
揭晓“2022年中国网安产业竞争力50强”榜单。
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，
奇安信蝉联第一名。

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	天融信科技集团股份有限公司
5	华为技术有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	阿里云计算有限公司
9	新华三技术有限公司
10	杭州安恒信息技术股份有限公司
11	360政企安全集团
12	亚信安全科技股份有限公司
13	成都卫士通信息产业股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司