内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

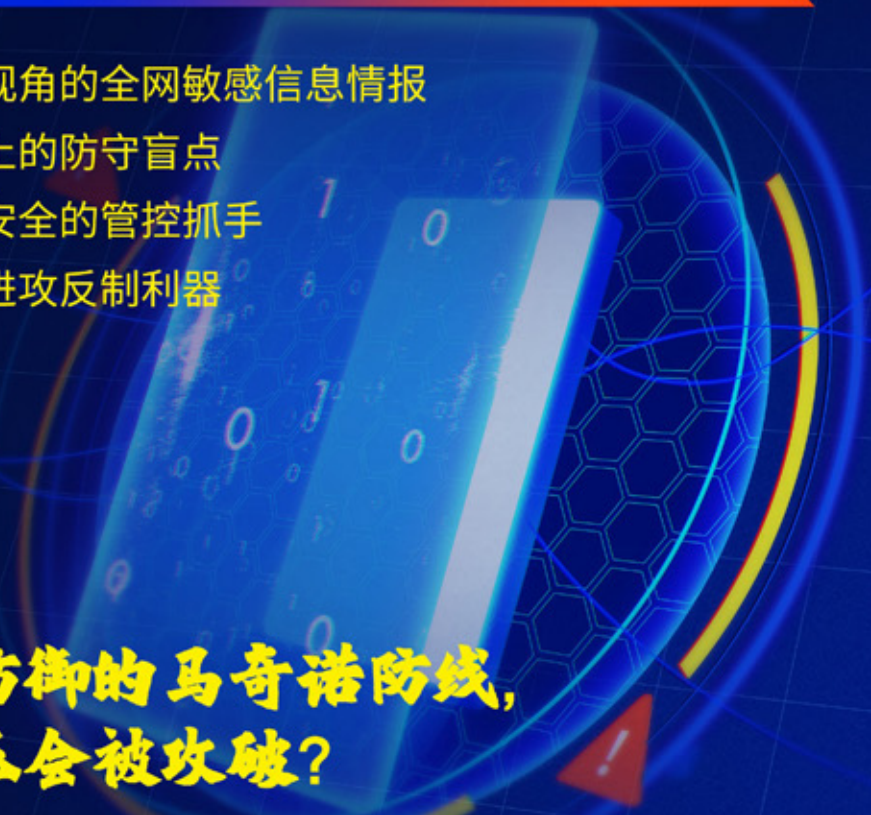
警惕！数据出境安全风险 P12

第19期
2022 年 7 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

你做过数据出境安全体检吗?

近日，某机构因数据出境问题遭重罚，令数据出境安全问题再受关注。

但在很多政企机构眼里，数据出境似乎是一个很遥远的话题。因为自身没有任何海外业务的机构，似乎完全不必考虑数据出境风险。

但奇安信安全专家在协助国家机构进行数据流量分析时发现，数据出境问题涉及的机构众多，一些机构所处理的数据在悄然中竟然被动出境，却毫不自知。

因此，时至今日，很多机构对于自身有多少跨境数据传输行为，跨境传输了哪些数据，是否包括敏感信息，仍然是一头雾水。

这与我们突飞猛进的数字化不无关系。在政企机构的数字化过程中，应用日益增多，数据量也越来越丰富，相互的交互更是令数据流向日益复杂。

在数据出境问题上，很多机构都面临着这样的难题：数据庞杂，难以理清数据资产；对于数据的流向，难以做到明细洞察；对于从网络上流动的数据，难以实现持续监测。

此外，出境的形式众多，不局限于数据境外存储：既包括将数据传输、存储至境外的物理越境行为，也包括从境外可以访问、调用境内数据的情形，还包括数据在我国境内能被外籍主体接触或访问到的情形；既包括业务需要的主动出境行为，也包括毫不自知的被动出境行为。被动出境中还包括防护不当的被动出境，和使用第三方平台的被动出境。

面对文件传输，Web 访问，数据库访问，网邮、VPN、即时通信、文件服务等各种数据出境行为，面对结构化数据、非结构化数据、半结构化数据等不同数据类型，依靠传统的手段难以发现数据主动和被动出境问题。你可能需要开展一次全面的数据出境的安全体检，利用技术手段发现潜在的风险。

基于先进的数据流量采集与还原能力、数据跨境传输检测能力、数据跨境内容识别能力、数据跨境敏感数据检测能力的奇安信数据跨境卫士，你不妨一试!

总编辑

李建平

2022 年 7 月 1 日

CONTEN

目录

安全态势

月度专题

警示！数据出境安全风险

与多数人的理解不同，数据出境安全风险其实不仅限于拥有跨国业务的机构，而是广泛涉及各类政府单位与企事业机构。数据出境的方式多种多样，可能不知不觉中就出现数据跨境，面临刑事责任的法律风险。

P12

TS

奇安资讯

《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 2122- 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 7 月 26 日
发行对象：奇安信集团内部

事件篇

国内曝出多起重大网络安全事件，我国上百个重要信息系统被美国植入木马程序，“国防七校”西北工业大学遭受境外网络攻击，学习通疑似泄露 1.7 亿用户数据。

因遭遇大规模网络攻击，这个国家政务网络被迫关闭

据 Security Affairs 7 月 18 日消息，欧洲东南部国家阿尔巴尼亚政府披露，该国前一天遭遇大规模网络攻击。一次来自国外的大规模犯罪行动袭击了国家信息社会局（AKSHI）的服务器，为应对攻击，该局被迫关闭政府系统。大部分面向民众的服务项目被中断，只有部分重要服务（如线上报税）仍在运行，原因是运行它们的服务器并未受到攻击覆盖。该国前总理指责，政府在 AKSHI 中汇集了太多政务服务。

印度地方洪水监测系统遭勒索软件攻击，水文数据全部被加密

据 Hindustan Times 7 月 7 日消息，印度果阿州洪水监测系统遭到勒索软件攻击，攻击者要求支付加密货币，以解密洪水监测站的数据。负责维护数据的州政府水资源部向警方报告称，所有文件已被加密，扩展名为 eking，无法再被访问。洪水监测系统、自动雨量计和气象仪的数据存储在该州首府的水资源部总部服务器中，由 ASTRA Microwave Products 有限公司维护。由于被黑客攻击，该部门现在无法访问不同站点的数据，并丢失了所有的旧数据。

网络攻击致使美国多个州无法发放失业救济金

据美联社 7 月 1 日消息，美国软件公司 Geographic Solutions 遭受网络攻击，导致多个州成千上万民众的失业救济金和求职援助受到影响。Geographic Solutions 是田纳西州等多个州的失业系统供应商，该公司在 6 月 26 日称将中断服务，预计 7 月 4 日重新上线。期间田纳西州的失业救济金网站无法访问，约 1.2 万人无法领取救济金。路易斯安那州、内布拉斯加州等州的救济金网站也均无法访问。

网络攻击迫使挪威主要政务网站瘫痪数小时

据美联社 6 月 29 日消息，挪威国家数据网络遭大规模 DDoS 攻击，导致在线服务停摆，国内公共与私营网站瘫痪数小时。挪威首相 Jonas Gahr Støre 称，攻击未造成任何重大损失。挪威国家安全局负责人称，幕后黑手疑似某亲俄黑客团伙。俄乌战争的网络空间对抗风险已经扩散，欧洲立陶宛、意大利、德国等多国近期均受到侵害。

中国上百个重要信息系统被美国植入木马程序

据环球网 6 月 29 日消息，国家计算机病毒应急处理中心和 360 公司分别发布专题研究报告，同日披露美国国家安全局（NSA）所属的又一款网络攻击武器“酸狐狸”漏洞攻击武器平台。报告称，“酸狐狸”的默认木马程序“验证器”的不同版本曾在中国上百个重要信息系统中运行，其植入时间远远早于“酸狐狸平台”及其组件被公开曝光时间，说明 NSA 对至少上百个中国国内的重要信息系统实施网络攻击。时至今日，多个“验证器”木马程序仍在一些信息系统中运行，向 NSA 总部传送情报。

伊朗国有钢铁寡头遭网络攻击，工厂被迫停产

据美联社 6 月 28 日消息，伊朗国有钢铁寡头公司胡齐斯坦称，由于“网络攻击”后引发的“技术问题”，工厂不得不停工，恢复时间将另行通知。黑客团伙“Gonieshke Darande”宣称对此负责，并发布了一段疑似工厂监控画面，显示生产线上一台重型机械出现故障引发了大火，该团伙还宣称对去年伊朗加油站大面积关闭事件负责。安全专家称，向钢铁厂等工业控制系统目标下手，无疑代表着网络攻势的升级。

QQ 出现大规模盗号！自动群发低俗不雅内容，官方回应

据南方都市报 6 月 27 日消息，26 日晚间，标题为“QQ 盗号”“QQ 回应大批账号被盗”的词条相继登上微博热搜。大量 QQ 用户反映，自己的 QQ 账号被盗后，向好友或在群聊中发送色情图片等不良信息，随后用户账号因被检测到违规行为而遭到封禁。27 日上午，腾讯 QQ 官方微博发文回应称，自 6 月 26 日晚 10 时左右收到部分用户反馈的 QQ 账号被盗一事，经调查发现，主要原因系用户扫描过不法分子伪造的游戏登录二维码并授权登录，该登录行为被黑产团伙劫持并记录，随后被不法分子利用，发送不良图片广告。

“国防七校”西北工业大学遭受境外网络攻击

综合消息，西北工业大学官方公众号 6 月 22 日发布公开声明，近期，该校电子邮件系统遭受网络攻击，报警后经公安机关初步判定，是境外黑客组织和不法分子发起的网络攻击行为。据悉，该校电子邮件系统发现一批以科研评审，答辩邀请和出国通知等为主题的钓鱼邮件，内含木马程序，引诱部分师生点击链接，非法获取师生电子邮箱登录权限，致使相关邮件数据出现被窃取风险。同时，部分教职工的个人上网电脑中也发现遭受网络攻击的痕迹。上述发送钓鱼邮件和发起网络攻击的行为，对西北工业大学校内信息系统和广大师生的重要数据造成重大安全威胁。

学习通疑泄露 1.7 亿用户数据，官方称公安已介入

据南方都市报 6 月 21 日消息，有公众号发文称，高校学习软件“学习通”数据库信息疑似大规模泄露，包含姓名、手机号、性别、学校、学号、邮箱等信息，数量疑达 1 亿 7273 万条。对此，学习通发微博回应称，不存储用户明文密码，理论上用户密码不会泄露，“公司确认网上传言密码泄露是不实的”。学习通还称收到用户数据疑似泄露的消息后已连续技术排查十余小时，暂未发现明确的用户信息泄露证据，且公安机关已经介入调查。

漏洞篇

谷歌 Chrome 官方披露 WebRTC 组件远程代码执行漏洞（CVE-2022-2294），称该漏洞已遭到在野利用，基于 Chromium 项目的软件均受影响，建议用户尽快自查更新。

Node.js dll 劫持漏洞安全风险通告

7月14日，奇安信 CERT 监测到 Node.js dll 劫持漏洞（CVE-2022-32223），在 Node.js 中存在 dll 劫持漏洞，攻击者可以通过 dll 劫持向 Node.js 内注入恶意 dll，从而执行代码。目前，奇安信 CERT 已成功复现该漏洞。鉴于该漏洞影响范围极大，建议用户尽快做好自查及防护。

OpenSSL 远程代码执行漏洞安全通报

7月6日，国家信息安全漏洞库（CNNVD）收到关于 OpenSSL 安全漏洞（CVE-2022-2274）情况的报送。成功利用此漏洞的攻击者，可造成目标机器内存损坏，进而在目标机器远程执行代码。OpenSSL 3.0.4 版本受漏洞影响。目前，OpenSSL 官方已发布新版本修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

Chrome 浏览器远程代码执行漏洞安全风险通告

7月5日，奇安信 CERT 监测到 Google Chrome 官方发布 Google Chrome 远程代码执行漏洞（CVE-2022-2294）通告，同时已监测到在野利用。Google Chrome WebRTC（网络实时通信）组件中存在基于堆的缓冲区溢出漏洞，成功利用此漏洞可导致程序崩溃甚至任意代码执行。鉴于此漏洞影响较大，建议用户尽快做好自查及防护。

Apache Tomcat 拒绝服务漏洞安全风险通告

7月1日，奇安信 CERT 监测到 Apache Tomcat 拒绝服务漏洞（CVE-2022-29885）的 PoC 在互联网上公开，当 Apache Tomcat 开启集群配置，且通过 NioReceiver 通信时，无论服务端是否配置 EncryptInterceptor，攻击者均可构造特制请求导致目标服务器拒绝服务。鉴于此漏洞影响范围较大，建议用户尽快做好自查及防护。

Splunk Enterprise 远程代码执行漏洞安全风险通告

6月22日，奇安信 CERT 监测到 Splunk 发布 Splunk Enterprise 远程代码执行漏洞通告，Splunk Enterprise 部署服务器 9.0 之前的版本存在远程代码执行漏洞，允许客户端将转发器捆绑包通过该服务器部署到其他部署客户端。控制了通用转发器端点的攻击者可利用该漏洞在订阅部署服务器的所有其他通用转发器端点上执行任意代码。鉴于这些漏洞影响范围极大，建议用户尽快做好自查及防护。

对抗篇

国内攻防演习 6 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 6 月，奇安信 Z-Team 团队共承接攻防演习服务 52 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 2 场，地市级攻防演习 16 场，客户自主攻防演习 30 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	51	64	88	101	31	188	318	1987

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有互联网业务平台漏洞、业务系统敏感信息泄露、内部人员对钓鱼攻击防范意识不足、内部网络安全防护措施缺乏、内网弱口令及口令复用普遍等。具体情况如下：

1、应用更新不及时，历史漏洞存在较为普遍

本月任务中发现，被攻陷目标互联网侧应用漏洞以历史漏洞为主，如外部应用中 shiro 组件漏洞、Weblogic 漏洞、Log4j2 漏洞、任意文件上传等漏洞，大多是因为没有及时更新升级造成的。这些漏洞的存在，是目标网络的重大安全威胁。

2、弱口令仍是严重的内网安全隐患

本月任务中因目标外网防护相对严密，互联网侧应用系统仅存在少量弱口令，弱口令或口令复用问题主要存在于内网，常见的是未修改安全应用默认口令、管理员为多台设备设置同一口令。本月某目标内网因大量不同类型的设备服务器使用同一口令，直接导致大量内网服务器被攻陷。

3、供应链对网络安全至关重要

本月任务中多个目标网络通过供应链攻击实现突破，主要针对目标网络平台或应用系统供应商开展突破工作，通过获取的相关产品源码挖掘漏洞，最终通过漏洞利用，打开目标网络防线突破口。供应链安全是网络安全构建的重要组成部分，对于网络安全至关重要。

4、访问策略缺陷是严重的安全隐患

本月任务中目标业务系统存在未授权访问问题，未授权访问大部分是因为对外部接入的安全配置或权限认证的相关策略设置存在缺陷。授权页面存在缺陷导致攻击者可以直接访问系统、变更系统权限，产生数据库或网站目录等敏感信息泄露，未授权访问漏洞利用成为外部突破的重要途径之一。

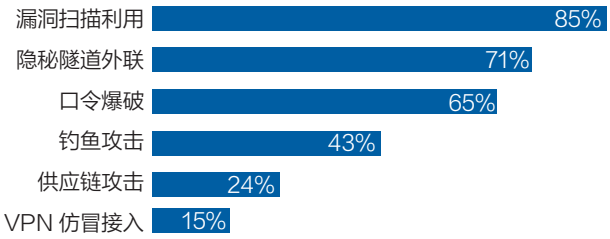
5、钓鱼攻击是实现突破的有力辅助

本月任务中钓鱼攻击主要是针对金融目标人员，金融行业网络安全体系建设比较完善，防护相对严密，互联网侧系统可利用漏洞和其他突破途径较少。钓鱼攻击主要向安全意识相对薄弱的客服或商务等人员展开，最终实现外部突破。

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实现，内网横向拓展以弱口令、口令复用及内部应用漏洞为主。使用的主要技术手段分布如下：

攻击手段分布



1、漏洞扫描利用

本月任务中客户网络安全体系建设相对完善，外网突破主要依靠漏洞利用实现。突破利用的漏洞以历史漏洞为主，这些漏洞多因互联网侧应用组件存在安全缺陷，且未及时更新、修复导致的。这些漏洞的存在是目标网络安全的重要威胁。

2、隐蔽隧道外联

本月任务中因客户网络安全防护水平较高，绝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网络穿透。主要利用转发工具在目标网络外部接口实现端口转发通信或建立通信隧道，从而实现从互联网到目标内网的访问，对存在多层网络隔离的目标核心内网，也要进行多层转发才能实现对核心业务网络的接入访问。

3、口令爆破

本月任务中弱口令爆破和口令复用全部存在于目标内网，主要针对目标内网的相关网络应用、安全设备和服务器。通过搜集目标网络中各种设备安装的默认口令、弱口令来分析其密码组合规律，从而实现快速爆破。

4、钓鱼攻击

本月任务中针对安全体系建设比较完善、防护相对严密的客户目标，很难从外部系统找到可突破内网的漏洞，难以直接突破，所以主要针对客服、人事、内部管理人员、运维人员、开发人员进行钓鱼攻击，以此作为目标网络的重点突破口。

5、供应链攻击

本月任务中供应链攻击以系统 Git 源码泄露为主，可从中获取外网重要账户名、密码信息或内网数据库安全部署信息，获取的信息可直接用于网络渗透。还可以对泄露的 Git 源码进行代码审计，由此发现系统漏洞，通过漏洞利用实现管理员仿冒登录。

6、VPN 仿冒接入

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

四、典型攻击手段实现案例

1、外部漏洞利用

（1）某目标管控系统存在 CVE-2021-219721 漏洞，通过漏洞利用获取该系统权限，并可控 27 台虚拟机、1 台主机和 1 个集群服务器。

（2）某目标监控系统存在 Struts2 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。

（3）某目标交易中心存在 Log4j2 远程命令执行漏洞，通过该漏洞利用成功获取到服务器权限、数据库权限及 Web 网站权限。

2、口令爆破

（1）某目标邮件系统存在弱口令漏洞，可通过口令爆破直接登录该系统获取管理员账户，重置所有人的邮箱密码，获取所有人的邮件信息、邮件中的敏感信息等。

（2）某目标堡垒机存在弱口令漏洞，可通过漏洞利用获取堡垒机权限，控制 7 台主机，并获取所有客户信息，包括身份、电话号码、交易记录、账号金额等敏感信息，及实时交易明细。

（3）某目标认证平台存在弱口令漏洞，可通过漏洞利用获取后台管理员权限。

3、钓鱼攻击

（1）通过添加某目标客户经理微信好友，以业务交流发送木马文件，并成功上线控制其终端，可登录多个内部系统。

（2）通过访问某目标微信小程序 APP，点击联系客服，进入客服聊天框发送木马文件，点击上线导出浏览器密码获得某目标小程序 APP 后台管理员权限。

（3）通过前期信息收集发现某公司邮箱账号，利用代理投标发送邮件进行钓鱼攻击，并成功上线 3 台个人终端，获得管理员权限，成功进入公司内网。

4、供应链攻击

（1）某目标业务系统 Github 源码泄露，直接从中获取管理认证信息，进一步拓展利用。

（2）某目标核心业务相关的多个业务系统源码被发布在互联网上，可以公开搜集，并可直接被用来突破。

5、VPN 仿冒接入

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

政策篇

国内，网信办接连发布《数据出境安全评估办法》《个人信息出境标准合同规定（征求意见稿）》，为规范数据安全出境作出重要制度安排；

国际上，美国总统拜登签署两项网络安全法案，今年以来美国已有五项网络安全法案签署生效，数量远超往年。

国内

网信办公布《数据出境安全评估办法》

7 月 7 日，国家互联网信息办公室发布《数据出境安全评估办法》，自 2022 年 9 月 1 日起施行。《办法》明确规定，数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估适用本办法。《办法》规定了应当申报数据出境安全评估的情形，提出了数据出境安全评估的具体要求，规定数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，并明确重点评估事项，在数据出境安全评估有效期内发生影响数据出境安全的情形，应当重新申报评估。

网信办《个人信息出境标准合同规定（征求意见稿）》公开征求意见

6 月 30 日，国家互联网信息办公室发布《个人信息出境标准合同规定（征求意见稿）》及《个人信息出境标准合同》。《征求意见》稿规定，个人信息处理者同时符合下列情形的，可以通过签订标准合同的方式向境外提供个人信息：（1）非关键信息基础设施运营者；（2）处理个人信息不满 100 万人的；（3）自上年 1 月 1 日起累计向境外提供未达到 10 万人个人信息的；（4）自上年 1 月 1 日起累计向境外提供未达到 1 万人敏感个人信息的。

国务院印发《关于加强数字政府建设的指导意见》

6 月 23 日，国务院发布《关于加强数字政府建设的指导意见》。《指导意见》明确数字政府建设的七方面重点任务，包括构建协同高效的政府数字化履职能力体系、构建数字政府全方位安全保障体系、构建科学规范的数字政府建设制度规则体系、构建开放共享的数据资源体系、以数字政府建设全面引领驱动数字化发展等方面。安全方面，《指导意见》要求强化安全管理责任，落实安全制度要求，提升安全保障能力，提高自主可控水平，筑牢数字政府建设安全防线。

反电信网络诈骗法（草案二次审议稿）征求意见

6 月 21 日，十三届全国人大常委会第三十五次会议对《反电信网络诈骗法（草案二次审议稿）》进行审议。24 日，中国人大网发布《反电信网络诈骗法（草案二次审议稿）》，公开征求意见。提请审议的二次审议稿作出以下主要修改：（1）提高法律责任部分的罚款幅度，加大违法行为惩处力度，加强跨境电信网络诈骗的治理措施；（2）完善涉诈资金链治理，有效防范涉诈洗钱活动；（3）扩大反诈宣传义务主体，增强宣传防范实效，

提高公众防范意识和防范能力；（4）进一步区分不同情形，加强反电信网络诈骗的精准防范。

《交通运输行业网络安全等级保护基本要求》发布

6 月 9 日，行业标准《交通运输行业网络安全等级保护基本要求》正式发布，将于 9 月 9 日正式实施。本标准规定了交通运输行业网络安全的基本保护要求，在现有国家标准的基础框架上，细化和补充要求指标，增加行业需求的指标项。为网络信息系统安全建设和管理提供了系统性、针对性和可行性的指导和服务，推动行业网络安全设计、建设、验收、运行与管理工作标准化、规范化。

美国网络安全审查委员会发布首份审查报告

7 月 14 日，美国国土安全部牵头运营的网络安全审查委员会发布首份报告指出，去年年底曝光的 Log4j 漏洞已成为“流行病”，将在未来十年甚至更长时间持续引发风险。这份报告耗时约五个月，调研了约 80 个组织，并与行业、外国政府及安全专家开展交流，还包括漏洞发现者所在国家中国政府。该委员会提出了 19 条建议，以供各实体在 Log4j 漏洞威胁下采用。

EDPB、EDPS 就“欧盟健康数据空间”提案发布联合意见

7 月 14 日，欧洲数据保护委员会（EDPB）公布了其和欧洲数据保护监督员（EDPS）对欧盟委员会关于欧洲健康数据空间提案的联合意见。EDPB 和 EDPS 表示，支持加强个人对其健康数据控制的想法，但提请联合立法者注意一些首要问题，如澄清提案的规定和 GDPR、成员国法律及欧洲倡议的规定之间的关系，健康医疗应用的数据不支持二次利用，电子健康数据存储本地化等。

美国 NIST 发布抗量子攻击的新算法

7 月 5 日，美国国家标准与技术研究院（NIST）公布了 4 种新的加密算法，用于保护联邦政府计算机和应用系统应对新型量子计算的网络攻击。这 4 种加密算法将成为 2024 年之前 NIST 后量子密码标准的一部分，分别为 CRYSTALS-Kyber、CRYSTALS-Dilithium、FALCON 和 SPHINCS+。其中，CRYSTALS-Kyber 用于通用加密用途；CRYSTALS-Dilithium、FALCON 和 SPHINCS+ 用于数字签名和身份验证。

德国发布太空基础设施安全保护指南

6 月 30 日，德国联邦信息安全办公室（BSI）发布了空间基础设施 IT 基线保护配置文件。该文件由空中客车防务与航天公司、德国航空航天中心下辖德国航天局与 BSI 等机构花费一年时间起草发布。文件定义了卫星网络安全的最低要求。文件涵盖卫星生命周期内的各个阶段，包括设计、测试、运输、试运行和最终退役。此外，还涉及支持航天器自身的网络和应用，再到子网、服务器机房等层级。

美国总统拜登签署两项法案，加强政府网络安全

6 月 21 日，美国总统拜登签署了两项法案，旨在加强联邦、州及地方政府的网络安全措施。《联邦网络劳动力轮岗计划法》建议设立一项计划，允许网络安全专业人员通过轮岗的形式接触多个联邦机构，提高自身专业知识。《州和地方政府网络安全法》旨在改善国土安全部与各州及地方政府在网络安全方面的协同能力。2022 年以来，美国已有五项网络安全法案签署生效，数量远超往年。

警惕！
数据出境安全风险

与多数人的理解不同，数据出境安全风险不仅限于拥有跨国业务的机构，而且广泛涉及各类政府单位与企事业机构。数据出境的方式多种多样，可能在不知不觉中就会出现数据被动出境，面临刑事责任的法律风险。

数据出境合规需把握三个阶段、解决三大难题

作者 奇安信网络探针事业部负责人 刘洪亮

数据出境是我国数据合规领域的重要话题。《数据出境安全评估办法》（以下简称《评估方法》）、《个人信息出境标准合同规定（征求意见稿）》等法规的相继发布，标志着《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》规定的数据出境安全评估制度正式落地，也意味着数据出境监管的细化和加强。

值得指出的是，涉及数据出境的绝不仅限于拥有国际业务的企业，数据交互和应用系统的增多，令大量的政企机构都有可能面临数据出境的安全风险问题。

例如，国内某些电商企业，因为使用了第三方平台或者软件，不知不觉间部分业务数据已经跨境流出；在开展数据跨境分析时，国内某市的区政府，被发现有重要数据被海外下载的情况，成为数据被动出境的案例。

对广大政企机构来说，经常面对数据资产不清、数据流向不明、数据流出多变的局面，奇安信认为，在数据出境合规建设上需把握三个阶段，解决好三大难题。

一、数据出境事关国家安全

目前，数据出境已从个人信息泛化到包括了非个人信息的一切数据范围。数据不受限制的跨境流动，可能会引发用户数据易被泄露、滥用等问题，给企业带来技术管理、资产管理和组织管理上的问题；尤其是关键信息基础设施数据等重要数据，涵盖了国计民生的方方面面。一旦处理不当，在出境过程中被非法获取、非法利用，将给国家安全带来严重威胁。

行业专家普遍认为，确保数据跨境流动安全，成为维

护国家安全和推进国际数据治理的重要课题。

但目前数据跨境的方式多样，既包括将数据传输、存储至境外，也包括从境外可以访问、调用境内数据的情况。对于大量政企机构来说，需要改变“数据出境安全风险”仅涉及拥有国际业务的企业，这一错误的认识。

总结奇安信所处理的事件，目前涉及数据出境安全风险的主要有三种类型：

1、拥有跨国业务的企业；

2、由于防护不当导致数据被动跨境的政企机构；

3、使用第三方平台或者软件导致部分数据被动跨境的机构。

从涉及用户的类型来看，很多政企用户涉及第二类被动出境的情况，其中包括不少政府机构。奇安信在协助相关机构分析数据流量时，发现很多政府相关信息和文件有被下载的情况。第三类情况在中小型电商平台比较普遍。

二、出境合规建设的三个重要阶段

根据对《评估办法》的解读，以及对数据出境安全评估流程的梳理，我们把数据出境安全合规建设分为三个重要阶段，分别是事前的风险自评估阶段、安全评估阶段及持续监测监督阶段。

第一阶段：风险自评估阶段。

摸清家底、了解现状是第一步。企业的业务系统与数据资产众多且复杂，进行数据资产的全面盘点非常重要。此后，需要有技术手段对流出境外的数据进行全面的梳理和监测，清晰的看到自己都有哪些数据流出境外，当前流出了多少，都流向了哪里，进而摸清当前数据出境的实际情况。

第二阶段：安全评估阶段。

进行全面的风险自评估并申请安全评估，形成申请报告，并通过省网信办上送国家网信部门。

国家网信部门受理申报后，根据申报情况，组织国务院有关部门、省级网信部门、专门机构等进行安全评估，数据出境安全评估的结果有效期为 2 年。

第三阶段：持续监测监督阶段。

企业的业务是持续发展的，数据是动态变化的，只进行事前自评估是无法满足企业持续合规的要求的。《评估办法》中也有明确要求，事前评估和持续监测监督相结合，实现数据出境的持续合规。

三、数据出境合规需解决三个难题

对于政企机构来说，确保数据能满足《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《评估办法》等法规的合规要求，需要能清晰掌握业务数据、个人信息、重要数据等敏感数据的跨境流动情况——在看清数据流向的同时，能清晰、直观的看到带有个人信息、重要数据的敏感数据是通过什么人、在什么时间、什么地点、通过什么方式、发送到哪里。

但随着数字化转型的深化，业务上云和大数据的应用，使 IT 环境越来越复杂，应用系统越来越多，数据交互越来越庞杂。再加上更多的数据来源、更多的应用数据调用、更多的外部合作，政企机构存在数据资产不清、流向不明的情况。

因此，政企机构在数据出境领域面临着三个难题：第一个难题是如何厘清数据资产，明确自己数据资产的属性、量级；第二个难题是如何明细数据流向；第三个难题是从网络上流动的数据如何持续监测，同时避免数据被动出境。

四、合规建设离不开技术手段的支撑

无论是风险自评估阶段，还是持续监测监督阶段，都需要有技术手段进行支撑，否则企业就无法在事前了解现状，日常运行中由于业务变化导致出境数据发生变化也无法及时掌握。

奇安信数据跨境卫士正是基于政企的诉求研发的一款产品，可以在两个重要阶段协助企业进行数据出境的合规建设，帮助企业清晰掌握业务数据、重要数据、个人信息等敏感数据跨境流动详情，做到对跨境数据流转的可知、可视、可查。

其中在风险自评估阶段，它可以帮助企业理清当前都有哪些数据通过网络流向了哪里，并自动输出数据资产流向表单。

而在持续监测监督阶段，数据跨境卫士可以持续的帮助企业进行数据出境的监测监督工作，无论数据有什么样的变化，数据跨境卫士都会自动帮助企业进行监测和提取，持续输出数据资产流向表单，并根据监管规则，提供风险预警及告警能力。

数据跨境卫士的领先流量采集与还原能力、数据跨境传输检测能力、数据跨境内容识别能力、数据跨境敏感数据检测能力，可以帮助政企机构实现保障合规、可查可验、看清流向、持续监测等价值。

首先是助力合规。根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《数据出境安全评估办法》跨境数据监管等合规要求，进行网络流动数据的发现和合规性检查；其次是可查可验，清晰掌握业务数据、重要数据及个人信息等敏感数据跨境流动详情；第三是看清流向，可以全面了解 WHO（什么人）、WHEN（什么时间）、WHERE（什么地点）、HOW（什么方式）、WHAT（什么数据）等整个数据跨境流转的整个过程，实现全局掌控；最后是持续监测，持续监测企业通过网络的数据跨境流动的详情，及时发现出境数据的变化情况，助力企业持续合规。

当前，我国数据跨境需求逐渐凸显。根据国家互联网信息办公室对外的数据显示，从 2017 年到 2021 年，我国数字经济规模从 27 万亿元增长到超 45 万亿元，稳居世界第二。数字经济发展动能正在加速释放，对外数字经济将迎来极大的发展空间，数据跨境传输的需求逐渐增多，在经济交流过程中合法合规使用数据，将成为国家安全和企业发展的重中之重。奇安信预计，数据跨境安全将有上百亿元的市场规模。

数据出境安全的十四个焦点问题

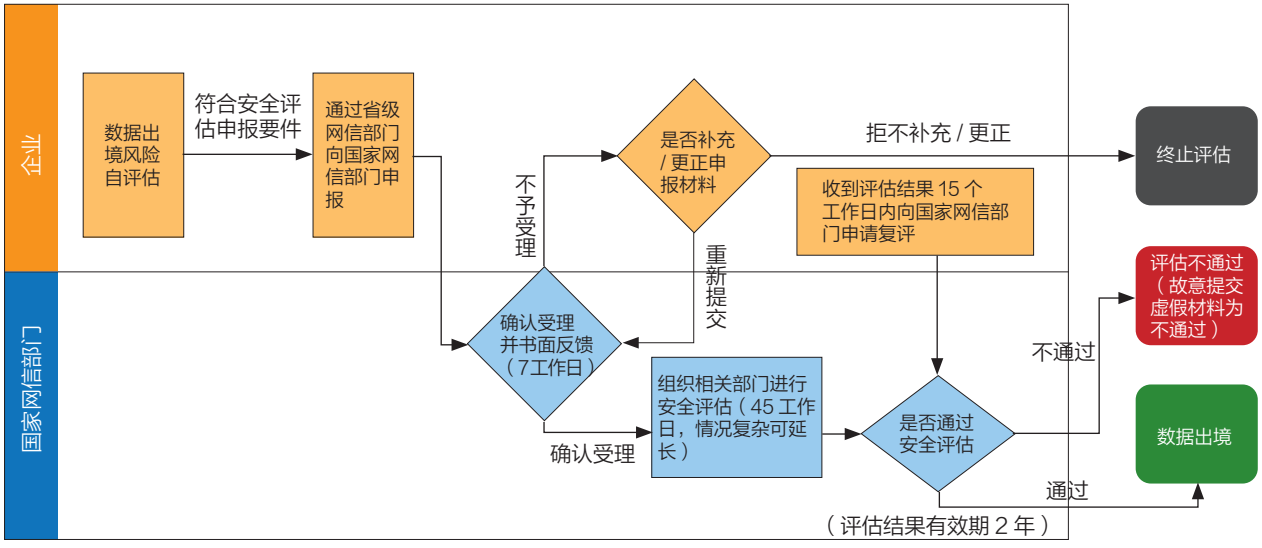
作者 中伦律师事务所 陈际红 吴佳蔚 杨润 于楚佳

自《网络安全法》于 2017 年生效以来，其所确立的数据出境安全评估制度就广受关注。历经多个版本和多轮征求意见之后，国家互联网信息办公室于 2022 年 7 月 7 日颁布《数据出境安全评估办法》（以下简称“《办法》”），并将于 9 月 1 日正式实施。本《办法》体现了监管机构兼顾维护数据流动安全和促进数字经济发展的价值取向，为企业跨境数据合规义务的落地实施提供了更为确定的指引。

我们选取企业视角中所关注的十四个焦点问题进行讨论。

1. 如何开展数据出境安全评估?

依照《办法》的规定，数据出境安全评估的流程如下：



2. 什么是“数据出境”？第二条的“向境外提供”包括什么场景?

《办法》适用于数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估的情形。

国家网信办就《办法》答记者问中进一步明确，《办法》所称数据出境活动主要包括：一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外。二是数据处理者收集和产生的数据存储在境内、境外的机构、组织或个人可以访问或者调用。

总结而言，判断是否构成《办法》所规制的数据出境，需满足以下要素：

（1）数据类型：境内运营中收集和产生的重要数据或个人信息；

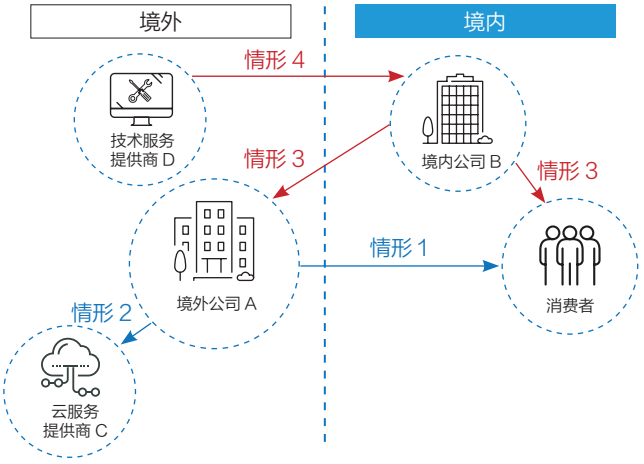
（2）出境的方式：向境外提供，包括物理跨越和远程访问；

（3）境外的含义：中华人民共和国大陆地区以外的其他国家 / 地区，包括港澳台地区[1]；以及

（4）开展数据出境活动的双方：涉及数据传输方和数据接收方[2]。

还有一个业界普遍关注的问题，即《个人信息保护法》（以下简称“《个保法》”）第三条第二款所规定的在境外直接处理境内自然人个人信息的活动是否适用《办法》，即如果境外的数据处理者所收集境内自然人个人信息的数量达到《办法》第四条规定的门槛，是否也要申请安全评估？之前业内普遍观点认为，《个保法》第三条第二款规定的处理活动，会导致《个保法》对境外的个人信息处理者直接适用，但第三章规定的个人信息跨境提供的规则不适用。该观点的逻辑是，该处理活动中，仅存在适用《个保法》的个人信息处理者单方，并无境外接收方，也就没有发生个人信息处理者向境外（另一方）提供个人信息的行为。GDPR 在此问题上亦是这样的逻辑。但是，在信安标委 6 月 24 日发布的《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》中，将此场景纳入到安全认证机制的范围，就此引发了比较大的争议。

从《办法》的文字逻辑看，比如，第二条规定的“数据处理者向境外提供”，第九条规定的“数据处理者应当在与境外接收方订立的法律文件…”，如果没有进一步的官方明确，我们倾向于认为《办法》的适用不包括《个保法》第三条第二款规定的处理活动。但是，如果未来监管机构将境外个人信息处理者在境内设立的专



- 某境外公司 A 在中国大陆地区境内无实体

情形 1: A 公司直接面向大陆地区消费者提供 APP 及相关服务，涉及收集处理消费者个人信息，根据《个保法》第三条第二款直接适用《个保法》，与消费者之间不构成数据出境

情形 2: 在情形 1 的基础上，A 公司在境外使用云服务器 C 存储其收集的来自大陆地区消费者的个人信息，A 与 C 之间构成数据出境

- 某境外公司 A 在中国大陆地区境内有子公司 B

情形 3: B 公司面向大陆地区消费者提供 APP 及相关服务，涉及收集处理消费者个人信息。为了总部业务管理的目的，B 会将其所收集的个人信息同步给其总部 A，B 与 C 之间构成数据出境

情形 4: B 公司所使用的某个 IT 系统是境外技术服务提供 D 协助在大陆地区本地化部署的，且 D 会远程访问该 IT 系统进行日常运维及的 bug 修复，B 与 D 之间构成数据出境

图：主要的数据出境情形判断示例

1 参考《中华人民共和国出境入境管理法》第八十九条的定义，出境是指中国内地前往其他国家或者地区，由中国内地前往香港特别行政区、澳门特别行政区，由中国大陆前往台湾地区。因此，我们认为将大陆地区境内收集和产生的重要数据和个人信息提供至港澳台地区也属于数据出境。

2 参考 EDPB《关于 GDPR 第 3 条与根据第五章的数据国际转移规定在适用时相关作用的 05/2021 准则（公开征求意见稿）》（Guidelines 05/2021）on the Interplay between the application of Article 3 and the provisions on international transfer as per Chapter V of the GDPR (version for public consultation)），为了符合数据跨境传输跨境的条件，必须有一个控制者或处理者披露数据（data exporter）和一个不同的数据控制者或处理者接收或被给予访问数据（data importer）。

《信息安全技术 重要数据识别指南（征求意见稿）》5 重要数据的识别因素。

《信息安全技术 数据出境安全指南（征求意见稿）》附录 A.27

门机构或者指定代表拟制为境内的数据处理者，进而适用《办法》进行安全评估，亦非不可能。

3. 如何理解风险自评估程序？与《个保法》第五十五条的 PIA 是什么关系？

根据《办法》第五条，数据处理者在向境外提供数据前应当开展数据出境风险自评估，因此，风险自评估程序是开展数据跨境活动和申报安全评估的必备前置程序。风险自评估可以由数据处理者自己进行，也可以引入第三方专业机构协助进行，《办法》第五条规定了自评估的重点评估事项。

根据《个保法》第五十五条规定，个人信息处理者在向境外提供个人信息前需进行个人信息保护影响评估（“PIA”）。那么，《个保法》第五十五条规定的 PIA 与《办法》规定的自评估和申报评估三者间是什么关系呢？ 应该说，三个评估的目标和方法论是基本一致的，即通过对数据处理活动的梳理，发现潜在风险点，判断所采取的管理措施和技术措施是否充分。但是，三个评估程序所重点关注的风险因素又有明显的区别：

PIA 主要关注数据处理活动对个人权益造成的影响，比如，数据处理活动是否会对个人信息主体依照《个保法》所享有的各项权益带来损害或者有所减损，但不会涉及重要数据；自评估属于自行发现风险的程序，除了 PIA 所关注的风险因素，还要重点关注跨境因素带来的风险，如出境数据的状况、境外接收方的承诺、所采取的措施、安全能力等，以及跨境处理活动的技术风险，跨境行权渠道等；而对于申报评估程序，除了个人合法权益的保护，该程序更加关注跨境数据活动对国家安全、公共利益带来的风险，如要考察境外接收方所在国家或地区的政策法律环境、同等保护原则是否得到落实、各方遵守中国法律的情况等。申报评估程序，一方面是对数据处理者所提交的自评估报告进行核查，另一方面，站在国家更宏大的角度，审视数据出境活动对国家安全和公共利益的影响。

4. 触发“数据出境安全评估”的情形有哪些？

根据《办法》第四条，结合《网络安全法》《数据安全法》及《个人信息保护法》等法律法规中的规定，以下情形会触发数据出境安全评估。

（1）出境的数据包含重要数据，而不论数据处理者是否构成关键信息基础设施运营者（“CIIO”）；

（2）数据处理者构成特殊主体：数据处理者是 CIIO，向境外提供个人信息；

（3）数据处理者所处理的数据量超过门槛：①处理个人信息达到 100 万人以上；或②自上年 1 月 1 日起累计向境外提供超过 10 万人个人信息或 1 万人敏感个人信息。

5.“数据出境安全评估”与“数据本地存储”是什么关系？

综合各个层次立法的规定，对在境内运营中收集和产生的数据，需要进行“本地存储”的，大体包括以下情形：

（1）CIIO 在境内运营中收集和产生的个人信息和重要数据（《网络安全法》第三十七条，《数据安全法》第三十一条）；

（2）CIIO 和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内（《个人信息保护法》第四十条）；

（3）国家机关处理的个人信息（《个人信息保护法》第三十六条）；

（4）汽车数据构成重要数据的，应当依法在境内存储（汽车数据安全管理若干规定（试行）第十一条）；

（5）其他对特定行业数据的本地存储要求，如金融、医疗健康、测绘等数据。

从以上分析可以看出，如果法律规定了数据本地存储的义务，一旦要实施跨境传输，必然会触发安全评估的要求。反过来，对于《办法》规定的需要申报安

	数据出境安全评估的触发情形	数据本地存储要求情形
特殊主体	关键信息基础设施运营者收集和产生的重要数据和个人信息《网安法》第三十七条，《数安法》第三十一条，《个保法》第四十条，《办法》第四条	关键信息基础设施运营者收集和产生的重要数据和个人信息《网安法》第三十七条，《数安法》第三十一条，《个保法》第四十条
	国家机关处理的个人信息《个保法》第三十六条	国家机关处理的个人信息《个保法》第三十六条
特殊场景	所出境的数据中包含重要数据《办法》第四条	/
	处理个人信息达到100万人以上《办法》第四条	处理个人信息达到网信部门规定数量《个保法》第四十条
	累计向境外提供超过10万人个人信息或1万人个人敏感信息《办法》第四条	/

全评估的情形，是否一定会触发数据本地存储的义务？尤其是①处理个人信息达到100万人以上；或②自上年1月1日起累计向境外提供超过10万人个人信息或1万人敏感个人信息的情形。虽然法律暂未明确，但我们倾向于认为本地存储和跨境安全评估是保障数据安全的一体两面。同时，结合《个保法》第四十条的规定，“处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内”，而《办法》所规定的100万、10万和1万的门槛，构成《个保法》第四十条所指的“国家网信部门规定数量”，因此《办法》规定的需要申报安全评估的情形将触发数据本地存储的义务。

6. 如何计算个人信息的量？

如问题4所述，在两种数据出境安全评估的触发场景下涉及计算个人信息的量：

(1) 处理个人信息达到100万人以上

a）计算标准：100万个人信息主体，即人数为100万；

b）计算主体：构成数据传输方的个人信息处理者。我们理解此处是指单个的个人信息处理者，如果某集团公司内涉及多个实体，如果没有数据混同或融合的情况，我们认为应按照不同实体分别计算；

c）计算范围：个人信息处理者范围内所有个人信息处理场景所涉及主体的总量，既包括外部客户、用户等，也包括内部员工。

(2) 自上年1月1日起累计向境外提供超过10万人个人信息或1万人个人敏感信息

计算时需注意以下几点。

a）计算标准：10万个或1万个个人信息主体，即涉及传输的个人信息主体的数量累计为10万人（若传输的是个人敏感信息，涉及传输的个人信息主体的数据量累计为1万人）；

b）计算主体：构成数据传输方的个人信息处理者。若同一个个人信息处理者涉及向不同的数据接收方提供

个人信息，所涉及的个人信息主体的数量应当累计计算；

c）累计标准：《办法》承接了《个人信息出境标准合同规定（征求意见稿）》的累计起算点，初次明晰了起算点为自上年 1 月 1 日起，与此对应的可能存在的清零和重新计算的制度设计，一定程度打消了企业关于“只要我有跨境业务，迟早会落入本地化和安全评估范围”的疑虑。

7. 关键信息基础设施运营者是如何识别的?

要判断是否落入《办法》的适用范围，就要判断企业是否构成 CIIO。

依据 2021 年颁布的《关键信息基础设施安全保护条例》（以下简称“《关基条例》”）第二条，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。依据《关基条例》第十条，由保护工作部门根据其制定的认定规则负责组织认定本行业、本领域的关键信息基础设施，并将认定结果通知运营者。基于此，企业一旦被认定为关键信息基础设施的运营者将会收到相关主管部门的通知。可以理解，企业如未收到主管部门的认定关键信息基础设施的运营者的通知，企业可以暂时认为自己不是 CIIO。

8. 重要数据是如何识别的?

依据《办法》第十九条，重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。据此可以判断，重要数据的识别主要聚焦于数据的性质和对国家安全和公共利益影响。重要数据采用的是定性与定量相结合判断的方法。若单条信息对国家安全可能造成影响的，单条信息亦可能构成重要数据，如国家战略物资的储备量。但若单条或少量信息不会影响国家安全或社会公共利益，但覆盖较大范围或较长时间的，或是涉及某些重要区域或时期的信息集合亦可能构成重要数据 。

从实务角度出发，虽然《数据安全法》规定由各地区、各部门负责确定本地区、本部门及相关行业、领域的重要数据目录，但目前仅汽车领域出台了《汽车数据安全管理若干规定（试行）》对此做出尝试，其他领域的重要数据识别指南仍有待进一步细化。

从企业自评估实践角度出发，企业存在判断难度。我们建议企业采取定性与定量相结合的方式，密切关注立法实践，适时征求相应主管部门的意见。

9. 申报评估中的“拟订立的法律文件”与标准合同条款是什么关系?

按照《办法》第六条要求，申报出境安全评估，要提交数据处理者与境外接收方“拟订立的法律文件”。其与《个保法》第三十八条所规定的跨境传输机制之一——标准合同条款在数据出境语境下，对于保护个人信息主体权益的价值取向和内容设置或有重合，但是法律效果不同。标准合同是与安全评估并列的跨境传输机制，企业在无需安全评估的前提下可以选择签署标准合同条款。此外，与标准合同条款最大的区别在于还应包含对于重要数据保护的内容（如涉及重要数据出境）。

结合《办法》第九条对“拟订立的法律文件”内容的要求，我们理解：

（1）若向境外提供的数据仅包括个人信息，数据处理者与境外接收方所订立的法律文件可以参考标准合同的内容或直接将标准合同作为“拟订立的法律文件”；

（2）若向境外提供的数据还包括重要数据，标准合同中对于传输双方的权利义务的约定同样具有参考意义。

10. 哪些机构会参与数据出境安全评估?

《办法》第七条规定，省级网信部门接受来自数据

处理者的申报材料，申报材料齐全的，报送给国家网信部门。第十条规定，国家网信部门将在受理申报后，组织国务院有关部门、省级网信部门、专门机构进行评估。从实务角度来看，出境安全评估可能与现存相关审批制度相竞合。如在出口管制领域，企业涉及美国实体清单移除程序时需向商务部申报批准。

11. 哪些情形会触发重新申报评估?

根据《办法》第十四条，触发重新申报评估的情形包括如下。

（1）评估有效期（2年）届满；

（2）评估有效期内，①出境活动事实变化：包括出境活动本身的目的、方式、范围、类型及接收方的使用、存储等发生变化；或②境外环境变化：主要指数据接收方所在国家/地区数据安全保护政策法规或网络安全环境发生变化导致可能影响数据安全；③或出境双方变化：包括出境双方的变更、实际控制权变化及双方的合同变更导致可能影响数据安全。

12. 评估申报需要提交具体的数据清单吗? 如何保护企业的保密信息?

在申报安全评估前，企业应已完成内部的安全自评估，对拟出境数据的类型、影响程度（含对个人信息主体的影响、对企业的影响、对社会公共利益及国家安全的影响）作出了初步的判断，形成了数据清单。但是结合实务经验，该等清单的具体程度可能会根据数据敏感性和出境活动的敏感性有所区别，若企业仅提供笼统的数据清单进行申报，国家网信部门可能会要求企业进一步补充信息以进行具体评估。

针对企业的保密信息保护，一方面，企业可在自评估时，在不影响业务实际开展的前提下对相关拟出境数据进行处理（如采取掩码、遮盖措施等），将已处理后的数据递交评估、向国家网信部门说明采取的预处理方式。另一方面，《办法》第十五条明确规定，参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据将依法予以保密，不得泄漏或非法向他人提供。

13.《办法》生效前已经传输出境的数据该如何处理?

《办法》规定了6个月的过渡期，要求在《办法》实施前已经开展的数据出境活动，不符合《办法》规定的，应当在《办法》施行之日起6个月内完成整改。基于此，我们理解如下，

（1）对于已经完成传输、且数据接收方已经删除或匿名化处理数据的数据出境活动，《办法》不溯及既往。

（2）对于已经完成传输、但数据接收方仍继续在存储或处理数据的数据出境活动：由于数据处理活动是一个连续的行为，数据接收方的后续处理行为仍可能对国家安全、社会安全及个人权益等产生影响，我们倾向于认为《办法》适用于此种情形。

（3）对于正在进行中的数据出境活动：在过渡期内，企业因业务需要需进行数据跨境传输的，仍可继续进行，但应同时完成对现有数据出境行为的风险自评估，若触发数据出境安全评估申报的，应当在过渡期内完成安全评估。

14. 监管机构如何进行执法?

根据《办法》第十六条、第十七条，国家网信部门可以采取主动检查与接受举报监督的方式，核实企业出境活动与申报评估的情况是否一致、是否符合数据出境安全管理要求。一旦发现不符合数据出境安全管理要求的，国家网信部门可以书面通知企业停止数据出境活动。企业违反《办法》规定进行数据出境活动的，将面临《网络安全法》《数据安全法》《个保法》等法律法规规定的处罚。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

规划快一步

奇安信 | BEIJING 2022

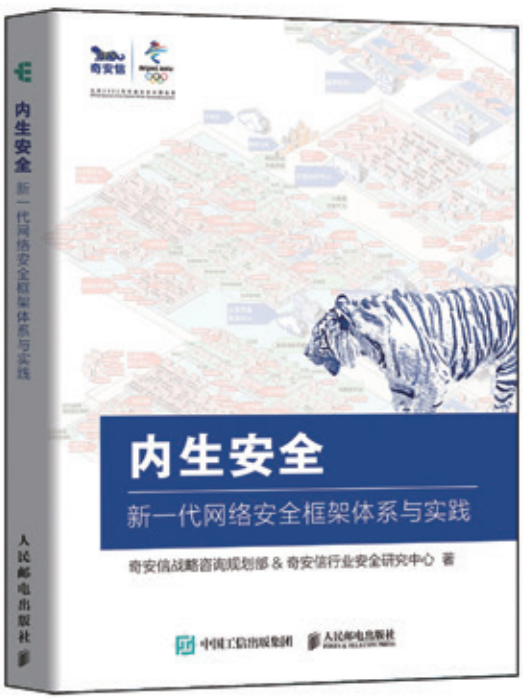
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

实战攻防演习：70% 的防守队没做好这些事导致“未战先输”

一年一度、如火如荼的网络安全攻防演习已经拉开帷幕。在攻防领域流传着很多金句，如“未知攻、焉知防”、“说一百遍不如打一遍”“以攻促防”“网络安全的本质在对抗”等。它们虽然表述不同，但核心思想是一致的：即防守队非常需要攻击队视角，从攻击者角度去站位思考，分析总结攻方会采取的手段和步骤，来反思自身的安全体系、防护弱点，达到“知己知彼、百战不殆”。

情报侦察历来都是决定战争胜负的一个重要的因素。从历年数百场攻防演习来看，经验老道的攻击队，并不是上来就工具齐上、招数使尽，而是先进行最重要的一项工作，就是侦察敌情。

侦察 攻击前的第一步

有一部很知名的老电影叫《渡江侦察记》，讲述渡江战役前夕，解放军派侦察班先遣小队，渡江去侦察敌情，并获得一份江防工事图，探明敌人江防部署。总攻开始后，解放军万帆齐发、大炮雷鸣，把敌人沿江工事精准摧毁，保障百万雄师顺利渡江，取得全面胜利。这部电影将侦察的重要性体现的淋漓尽致。

同样，有一部叫《斯巴达 300 勇士》的国外电影，从守方角度，体现了对忽视侦察导致的后果。斯巴达王列奥尼达率领 300 勇士，将波斯数十万大军堵在了温泉关，让对方寸步难行、伤亡惨重。然而，列奥尼达没有防范身后的一条小路，最终被一个叛徒引导波斯军抄小路，绕道进攻到奥尼达的后方薄弱环节，导致 300 勇士腹背受敌、血染温泉关。

在实战攻防演习中，作为攻击活动的初始环节，攻击者会通过各种手段，搜集目标信息，并选择薄弱点，如窃取登录凭证、扫描高危端口等，将其作为主

攻方向。具体包括，通过各种途径收集目标主机的信息，主要利用的是搜索引擎和扫描技术。通过外围信息收集和多种扫描技术，可以获得目标的 IP 地址、端口、操作系统版本、每个端口运行的服务、存在的漏洞等攻击必需信息等。

从攻击者的视角，侦察获得的信息越全面，找到薄弱点、突破口的概率就越高。因此，作为防守队，第一步需要做的事情，不是急迫布防，安装各种威胁检测、边界安全等产品，而是不要让敌人侦察到攻击的突破口，让他们无隙可乘。

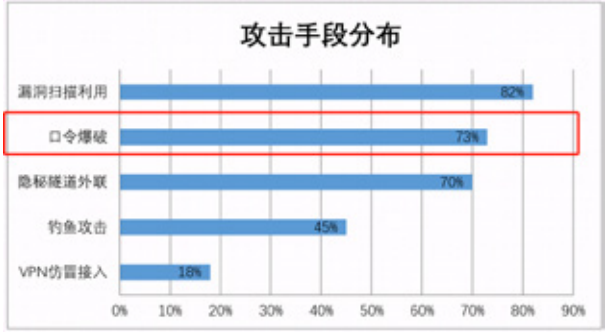
防守队痛点：未知资产暴露在外 弱口令无处不在

对于防守队而言，第一个痛点是资产繁多、难以管理，尤其是很多暴露在外的未知资产，一旦被攻方侦察到，失陷基本只是时间问题。

参加实战攻防演习的政企机构，绝大多数信息化、数字化程度都很高，对外开放的业务应用非常广泛，导致暴露在整个互联网上的服务器、设备的端口、协议、应用等非常庞杂和繁多。尤其是为因内部管理流程不完善等原因，导致很多未知资产暴露在外。这些未知资产，对于经验丰富的攻击队而言，可以用常规扫描工具轻松侦察到。攻方演习一旦开始，这些未纳入统一管理的未知资产，很容易成为率先被攻破的目标。

第二个痛点，屡禁不止的弱口令，防守虚弱的特权账号等，让攻击者屡试不爽。

弱口令是指账号口令复杂度策略配置较低，或容易被攻击者获取的口令，通常有简单口令、默认口令、空口令、规律性口令、社会工程学弱口令等。由于其口令强度过弱，容易被攻破，堪称每年实战攻防演习的十大安全漏洞之首。而实战中通过弱口令获得权限的情况占比更是高达 70% 以上。



同时，因涉及到攻击者的最终利益，特权账号往往是攻击者瞄准的重点攻击目标。特权账号由于其分布广、数量多的特点造成特权账号梳理难，组织管理员无法全面掌握特权账号的动态情况。加上僵尸账号、幽灵账号、后门账号、弱口令账号、长期未改密账号等风险账号广泛存在，且比较隐蔽，给系统资产带来很大的安全隐患。

防守方破解之道：做好资产测绘 严控账号风险

让众多未知资产暴露在互联网等公开区域，无异于给攻击队若干不设防的攻击目标，演习中会被处处打穿。为此，奇安信实战攻防专家建议，防守队首先要做的第一件事情，就是收缩暴露面，通过技术手段实现对旗下

各类资产的统一管理，才能有针对性的防护。

目前，奇安信推出的网络空间测绘鹰图平台，作为实战攻防前的互联网空间“侦察机”，将虚拟的网络空间、地理空间、社会空间相结合，可以探测到域名、服务器、网站、数据库、应用软件、网站服务组件、网站框架等各类互联网资产。鹰图平台作为侦查工具，辅助服务人员帮助客户发现未知资产和风险资产，从而形成互联网资产探测和风险预警服务，为后续的安全加固、防护增强提供支撑，防止在攻防中被攻击者劫持利用，减少防守丢分。

图：奇安信网络空间测绘鹰图平台

鹰图平台的第一个优势在于拥有域名海量资产。 在奇安信技术研究院的支持下，鹰图平台收集了海量域名数据资产。截至 5 月底，鹰图平台的资产总数 103 亿 +，独立 IP 数 5.6 亿 +，域名资产数 38 亿 +，ICP 备案资产数 600 万 +。每日资产更新量与 IP 总数更新量均在千万级别，已远超同行。

第二个优势是查看便捷，可帮助客户快速掌握资产暴露面全貌。客户在鹰图平台上，可以从攻击者视角出发，清晰、便捷、全面地查看企业暴露在互联网上的资产概况、资产分类、问题资产等资产全貌，还可以查看暴露 IP 详情、证书详情等。

第三个优势是速度更快，资产更新追求与业务同步。鹰图平台基于“零拷贝”发包技术，结合“无状态扫描”技术，可帮助客户快速扫描到网络存活资产，缩短资产更新与业务同步的时间差。鹰图平台扫描全端口，目前国内高频端口最快 4 天更新，海外高频端口最快 10 天更新。避免业务上线很久、资产还没梳理出来的“空窗期”。

防守队做的第二件事情，是定期修改弱口令，关闭高危端口，销毁闲置的虚拟机等。

随着资产日益增加，应用系统疯狂增长，应用系统类型日益复杂，对特权账号管理要求越来越高，特权账号口令的管理成为新的挑战。对此，奇安信推出了特权账号管理系统（特权卫士即 PAM），它以保障特权账号安全为核心，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，帮助客户提升账号安全的主动防御能力，降低因账号口令泄漏或被非法利用而造成的防守目标失陷问题。

围绕实战攻防演习前，奇安信为客户提供了部署和使用特权卫士的三步流程：

客户提前部署特权卫士，第一步是录入特权账号，实施账号扫描，通过收集客户资产信息，每台资产录入

图：鹰图平台监管大屏——全国资产数据全景图

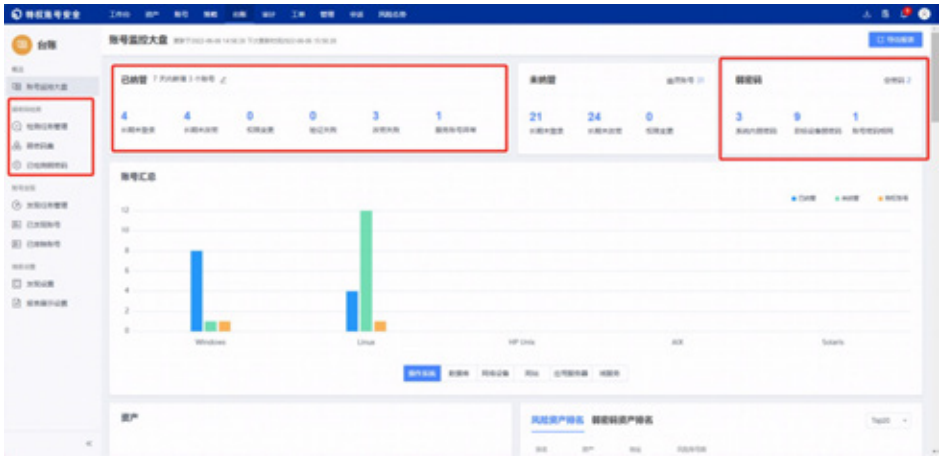
图：账号风险态势视图

最关键的特权账号（Root\Admin 等类型）存储在 PAM 密码保险箱之中；实施账号扫描，发现幽灵账号，杜绝从外部窃取账号口令。

第二步是风险台账梳理，专项整治弱口令。具体通过账号发现数据，梳理风险账号台账；录入企业内部专属的弱密码集合，实施系统弱密码扫描专项，并且一键改密，防止攻击方利用窃取到的口令实施内网横向移动。

第三步为标准管理策略，动态分配权限。通过账号改密和统一策略管理，回收账号权限，解决权限的滥用；无缝联动奇安信堡垒机，闭环账号全生命周期管理，杜绝利用账号的违规操作。

备战实战攻防 奇安信在行动



图：风险账号台账与弱密码检测专项

目前，奇安信安服团队已经为 2022 年实战攻防演习启动相关工作，在收敛暴露面方面，主要通过奇安信网络空间测绘鹰图平台，对客户侧产品对外暴露控制台等情况进行排查并通知进行收敛。而在保护特权账号、控制弱口令风险方面，奇安信安服团队联合数据安全团队，启动了账号口令专项检测行动，在实战攻防演习之前，守护好客户数据资产的账号大门。安

32.6 万员工、17 万终端……国家能源集团如何实现终端安全的“数字化运营”？

作者 研究员 张少波

32.6 万名员工，17 万台终端，分布于全国各地，乃至全球海外，这样超大规模的集团型组织，如何应对各种木马、病毒及 APT 攻击等新型攻击？如何对终端安全进行数字化的效果评估？如何构建一体化的闭环整体防护体系？如何实现全局整体的有效管控？……

面对这些问题，国家能源集团在历时 8 年的网络安全建设中，探索出一条“体系化防御、数字化运营”的终端安全运营之道。

从 8 万到 17 万的跃迁 终端安全运营问题凸显

国家能源集团，全称为国家能源投资集团有限责任公司，是由中国国电集团公司和神华集团有限责任公司联合重组而成的中央骨干能源企业，是全球规模最大的煤炭生产公司、火力发电公司、风力发电公司和煤制油煤化工公司。在国家能源集团的数字化过程中，终端作为必不可少的 IT 基础设施，是数据和应用的重要载体，更是攻防对抗的最后一道防线，其安全建设成为重中之重。

“从最初的时候，我们就秉承了体系化防御的理念，坚信网络安全一定不能靠单一的产品来解决问题，而是一个纵深防御的体系。” 国家能源信息技术有限公司网络与信息安全中心部门总经理韩鹏军这样表示。

据韩鹏军回忆，在 2014 年以前，集团终端侧均为各单位自行建设和管理，随着数字化转型的浪潮，这种单兵作战、事后补救的分散被动防御，无法应对各种木马、病毒、及 APT 攻击等新型的攻击手段，体系化防御势在必行。2014 年，集团通过天擎系统完成了 8 万多终端的统一管理。此后，陆续上线的 NGSOC(态势感知与安全运营平台)、VPN、天眼及其他的防护手段，都基于体系化防御理念。

2017 年，随着神华集团和国电集团的合并，国家能源集团正式挂牌成立，而终端规模也从近 9 万激增到 16~17 万的规模。韩鹏军表示，随着规模的激增，集团终端安全在日常运维、重要节日保障及攻防演练期间，陆续发现了很多运营方面的困扰与不足，具体表现在以下几个方面：

首先是终端资产难以掌控。由于集团规模庞大，终端资产繁多，不了解实际网内终端数量，无法确定终端防护范围；终端安装率提高缓慢，各单位缺少专门的终端安全运营，资产台账难以及时更新。

其次是数据利用相对低效。由于终端安全数据繁多，大量的终端行为数据，难以快速进行有价值、高效的安全分析；杂乱的数据往往无法直接成为管理办法制订及修改的依据。

第三是安全基线无法统一。具体表现为终端用户业务行为差异，终端安全基线无法统一，缺少判定安全基

图：终端安全建设的“四步走”

线策略的实用性方法。

最后是高阶病毒防不胜防。随着高级威胁、勒索等病毒花样繁多，在高阶对抗的新形势下，对于很多灰色文件无法有效判定，下属单位安全能力相对薄弱，无法有效处置。

这些问题归纳起来，侧面说明，终端安全防线并不是简单的安装部署就能永久生效，进化的威胁、管理的疏漏、失调的策略等，都可能导致终端安全产品失效，使得终端无法获得持续有效的保护，重新建、轻运营的思维亟待扭转。

终端安全四步走 真正实现可视、可管、可量化

回顾终端安全的建设历程，国家能源信息技术有限公司网络与信息安全中心部门副总经理曹慧划分了四个阶段：第一阶段是 2014 年开始的基础平台建设期，核心是启动防病毒项目建设，并建立考核体系；第二阶段是 2016 年完成的全集团覆盖，推动各子公司安全管理水平达到预期水平；第三阶段是 2018 年启动的平台数据深化应用，旨在建立数据分析平台，对信息化决策提供数据支撑；第四阶段是 2019 年至今，持续的终端安全深化运营，为集团信息化的精细化管理提供抓手。

在建设思路方面，根据集团提出的“统一基线策略、分级管理、分级授权”终端安全管理建设模式，采用“大统一”式架构，采用模块分离、集中部署的方式，集群统一部署于集团总部，各级单位终端通过集团广域网连接到系统管理控制中心，接受集团统一管理。

“大统一”式架构的优点显而易见，其适用于集团大型 / 复杂 / 跨广域网环境的用户，同时统一集中化管理模式，运维管理更高效；尤其是全网终端统一的安全策略防护，更高效地提升全网终端防护水平；而整体项目工程周期短，见效更快，维护投入更低。

曹慧表示，终端安全管理运营平台建设完成后，目前已经实现了可视化、可管控和可量化三大目标。

在可视化方面，通过搭建终端安全综合展示平台，可以多维度进行终端信息展示，全面掌控终端安全态势情况，尤其是多层次的安全态势视角，为领导决策指挥提供量化数据支撑。在可管控方面，通过与安全管理工作平台整合，实现告警监控与处置的全生命周期管理。而在

图：国家能源集团终端安全概况

可量化方面，通过安全指标来量化当前终端用户面临的威胁及自身的安全建设情况。

通过可视化、可管控和可量化，分别满足了决策者、管理者、运营者等不同层级使用者的需求。决策者可以通过平台了解全局终端安全态势及终端安全建设工作，帮助更快做出安全决策。管理者可以通过平台提高终端安全运营工作的效率，梳理运营流程。运营者则可通过平台进行安全监控并获取安全事件处置的佐证。

当然，对于 32 万多员工的超大集团型企业而言，终端安全运营的模式探索之路曲折而艰辛，绝非一朝一夕就能达到目标，为此，曹慧总结了四方面的经验：

第一是充分整合已有平台的安全能力，发挥更大价值。“很多单位在使用安全防护软件时，仅使用了平台推荐的功能。但我们的思路是尽可能挖掘平台深层的能力，尽可能用全、用到位，充分发挥出系统应有的价值。

第二是建立安全事件通报机制，持续提升执行效率。

图：病毒治理监测视图

由于集团的下属单位安全能力薄弱，很多攻击事件无法及时研判和有效处置，通过建立安全事件通报机制，定义终端安全事件规则，实现安全事件协同通报处置，持续提升终端安全运营的执行效率。

第三是逐步细化考核评价指标，让安全效果可量化。在过去，终端安全的效果多是感性描述，很难进行数字化考核。凭借终端运营平台持续的数据分析，集团制定了终端安全考核制度，通过技术手段对全集团终端安全情况进行评价，结合集团管理要求逐步细化调整考核评价指标，让整个安全效果可量化、可考核。

图：数据应用及分析视图

第四是深化终端安全数据处理，实现高效利用。终端安全运营中会产生海量数据，如果不能将其充分收集利用，其价值就无法被发挥出来。“我们充分提升了终端数据分析效能，增加了多个维度和分析，对于平台所采集的多维度终端数据进行高效利用。”

打造平台化底座 实现从安全到管理的跃迁

“始于安全，不止安全”，这是国家能源信息技术有限公司网络与信息安全中心安全运维经理钱隆对于终端运营最深刻的感受。“经过这么多年对天擎不断的使用、不断的运营，我们发现它不仅仅是防病毒，安全管理是其更大的功能，完全可以承担平台化底座的角色。”

第一个典型场景是软件正版化。过去集团经常头疼的事情是：第一，不知道所有的计算机都装了什么软件？第二，安装了的这些软件哪些是正版的、哪些是盗版的。依托于“天擎”的软件管家，这些信息可以一目了然。

另一个典型场景是整改违规互联网出口。依靠传统手段，很难发现隐蔽的违规互联网访问，通过天擎加入了一个定制开发功能，可以让终端不断地检测互联网出口 IP，并把这个 IP 信息报给“天擎”管理控制台，“天擎”上面录入了合规出口的 IP 地址来进行比对，这样一来，违规互联网出口问题迎刃而解。

“终端安全管理具有得天独厚的优势，因为它是可以管到最末端的一个环节的。不仅上面出现的这些安全风险可以第一时间得知和处理，更重要的是，这 17 万台终端散落的有价值信息，可以第一手获取，从而对信息化管理提供强大的支撑。”钱隆此总结到。

终端安全通常是企业最先部署的安全产品，然而也容易让很多客户对其价值的理解，停留在防病毒等基础层面。显然，国家能源集团通过在“数字化运营、体系化防御”方面的实践探索，进一步挖掘了终端安全在管理和运营层面的深层价值，使其成为数字化建设中不可或缺的平台化底座，这也是该项目最大的标杆意义所在。安

审时度势 谋定而快动

——走进奇安信集团副总裁、创新 BG 负责人孔德亮

作者 公关部 张雪丹

考究的西服，合身的剪裁，奇安信副总裁、创新 BG 负责人孔德亮浑身散发着精干的商务范儿。三年前，他还是一个穿着随意、休闲范儿的 IT 青年。

对不了解孔德亮的人来说，孔德亮像换了一个人，从幕后的技术牛人，变成了台前的带领工业互联网安全事业部和创新 BG、拿下了一个又一个优异业绩的“榜一大哥”。

而了解孔德亮的人知道，孔德亮一直没有变，一直在做自己。

能拼肯干 主动选择挑战

爱挑战、技术好、能拼、肯干是孔德亮留给大家的第一印象。

2010 年，27 岁的孔德亮还在上一家公司一线做技术，参与一款拥有 1500 万用户产品的技术支撑工作。一天晚上，这款产品出现了问题，如果不能妥善解决，将造成客户数据丢失的严重后果。但恰巧当时负责这款产品的领导、技术主管等全都出差不在京，于是，级别尚低的孔德亮成了“前锋”。

从晚上 8 点开始，孔德亮就在埋头处理。而当时的老板，就站在孔德亮的工位后面来回踱步，等待着这个小伙子能给出一个令人满意的解决方案。“刚开始的时候，我有点不自在。我想，不就是个 BUG 吗？至于这么大的领导亲自盯着我这个小兵干活儿吗？估计也是表示下重视，再晚点，领导应该就会走了吧？”

然而，时间一分一秒过去，孔德亮身后的脚步却始终都在，成为一种督促也是一种鼓励。

忙到凌晨 5 点的时候，孔德亮觉得问题应该基本解决了，只待敲一下回车，等待最终结果，而老板却谨慎地问他，你要不要先去洗把脸，精神精神，毕竟这是事关客户资料的大事。

次日清晨 8 点，孔德亮挑战自我成功，产品问题得以最终解决，危机解除。老板对他简单嘱咐了几句就离开了，但在之后的多个场合里，老板再提起这个攻坚的夜晚，都会表示公司又收获了一个好苗子。

时至今日，再回看当年的那个“毛头小子”，孔德亮觉得，其实取得宝贵收获的是自己。“那天晚上，我从老板身上第一次真正意识到‘客户至上’，也对做技术、做产品有了更深的认识。”

凭借刻苦、用心和不断应对新挑战，孔德亮用了不

到 10 年的时间，从技术岗位的“大头兵”，一步步晋升到最高级，成为这家公司里技术级别跨度最大的员工，负责多个技术平台的管理工作。

如果说这个阶段的应对挑战，对孔德亮来说还多少有些顺势而为，拾级而上的意味，2021 年主动转型，入职奇安信，则是孔德亮主动给自己发起的一次重要挑战。

“技术工作已经做了十几年，我想做一些不一样的事情。我不希望自己的跳槽只是单纯带着上一家的经验，去新公司进行‘填坑’和升级，而是希望可以把原来的技术基础和新公司的业务进行结合，去做更有挑战、也更有想象空间的事情。”

迎难而上 谋定后动

这件更有挑战的事，最初就是接手奇安信的工业互联网业务线。

在一些人眼中，这算不上一个明智的选择，因为当时工业互联网部门在集团内的业绩并不好，很难做出成绩；在另一些人眼中，这个选择很明智，因为只要稍微有点进步，就可以算是小有成绩。

孔德亮其实没有去想这么多，他只是看好工业作为国家在世界范围竞争的重要实力支撑，工业互联网已经进入关键发展期，工业互联网安全建设也必须要跟上；2021 年上半年，《工业互联网创新发展行动计划（2021—2023 年）》《工业互联网企业网络安全分类分级管理指南（试行）》《工业互联网标识管理办法》《关键信息基础设施安全保护条例》等相关法律法规发布，政策导向也十分明确。

工业互联网安全业务的崛起似乎万事俱备，但“东风”要从何处来借呢?

入职后的很长一段时间，孔德亮每天 5 点起床，6 点半到公司，把自己关在办公室里，开始认真梳理内部情况和外部市场。研发方面，集团一直重金投入；技术方面，多年来奇安信早已打下扎实的基础；市场方面，工业互联网发展正处在创新活跃期、战略窗口期和关键

发展期；销售方面，遍布全国的销售团队，能力也并不弱。

“有产品也有市场需求，那问题究竟出在哪里？”

就在此期间，美国最大的天然气和柴油运输管道公司 Colonial 因遭受网络攻击而暂时停止运营，甚至美国交通部联邦汽车运输安全管理局也因此宣布多个州进入紧急状态。

坐在办公室里的孔德亮，密切关注着这一事件。虽然发起攻击的手法并不算高明，但攻击的影响却极为广泛，工业基础设施安全成为全球共同关注的热门话题。

孔德亮再次坚信自己的选择没错。

2 个月后，孔德亮开始“走出去”，他认为，解决问题的办法应该在市场、在客户侧。他开始频繁出差、见客户，聊环境、聊政策、聊需求，天南海北的飞，硬是在很短的时间内就把经济舱飞出了金卡。

在深入市场和客户后，孔德亮发现，当前的“困境”是因为技术、研发、销售和客户之间的通路没有形成。他提出，要把公司里的技术积累形成客户需要的解决方案，去真正解决客户的工业安全需求。

通路形成，落地执行立见成效。2021 年，连续三年业绩倒数的工业互联网安全事业部做到了集团业绩第一名，团队士气也得到了前所未有的高涨。而在 2021 年底进行业绩汇报时，孔德亮主动向集团提出了 2022 年工业互联网安全业绩翻倍的年度目标。

孔德亮给工业互联网业务线 2022 年的规划是，打破当前工业安全发展套用常规安全产品的发展瓶颈，通

过深入业务场景，做真正的场景化、解决客户问题的工业安全产品。“石油石化和电力的场景是不一样的，电力和燃气是不一样的，和智能制造更是完全不同。未来两年，这将是工业互联网业务需要去深入挖掘和开发的关键。”

充当“纽带” 形成合力

工业互联网业务线的发展走上轨道，但孔德亮要应对的挑战并不止于此。

2022 年一开年，孔德亮就被任命为创新 BG 负责人。这是奇安信集团内团队人数最多的 BG，由数据安全子公司、工业互联网安全事业部、身份安全事业部、网络探针事业部、代码安全事业部、盘古事业部及反金融犯罪产品部七个事业部组成，涵盖网络安全主流新兴领域。

孔德亮很清楚，创新就意味着高投入、高期待和高风险，也可能创下更高的成就。“既然要做，那便做掌控局面的人，去拓展更好的成绩，一路赢下去，输了也不要给自己找借口。”

孔德亮对将要带领的团队进行了认真的梳理和分析。分散的业务结构和庞大的人员团队，注定不能单纯用级别来进行压制管理；而分散的多个产品方向也很难有一个人可以用专业性来征服所有人。

因此，他给自己的定位是“纽带”：以“服务”的状态，来拉通团队内的流程，并建立互信。同时，结合整个创新 BG 相对“分散”的特点，孔德亮划出了抓重点业务和重点运作模式两个方向，来让整个 BG 形成合力。

数据安全毫无疑问是重点业务。在带领工业互联网

业务线大踏步前进的同时，孔德亮也注意到了数据安全这一重点领域，工业互联网发展过程中，也提出了大量数据安全服务的需求。孔德亮认为，数据安全比网络安全更复杂。“所有的网络安全问题，可能最终都是为了解决数据安全。”

确认重点后，孔德亮就拉着团队一起，对产品和市场需求进行梳理：客户的数据安全防护需求是必然趋势，但又确实很难要求所有企业都大手笔投入、一步到位。那就针对已有产品做好基础的安全防护，先保证数据别丢；再做数据的分类分级治理，打好基础；之后再考虑做精细化的数据升级防护，以及更丰富的场景应用。

然而数据安全是一项复杂的系统工程，数据应用的全生命周期过程中的每个环节，都有着不同的安全技术需求及合规需求。创新 BG 下多产线团队便成为优势。

发动多产线各部门，针对当前政企机构的数据安全“短板”，创新 BG 很快推出了保障数据安全的“五件套”，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，帮助企业兼顾业务发展和安全合规。

运作模式方面，孔德亮认为应该充分发挥创新 BG 遍布全国的优势，形成合力。在接手创新 BG 前，工业互联网安全事业部就有遍布全国的行销人员，再加上在广东的数据安全子公司、在上海的盘古实验室、在成都的零信任团队，一旦拉通这些团队，将会形成 1+1 > 2 的效果。

“销售作为最接近客户的人，是最了解客户需求的人。”以销售人员为“触手”，深入了解客户应用场景和痛点需求，及时反馈给产线和研发团队，才能更高效地推进市场化产品研发，形成良性循环。

主动向前推进，向后传递。用产品思维做技术，用销售思维做产品，用客户思维做销售。孔德亮不信奉什么一定之规，而是审时度势，灵活地调整着思路和方向。

思路明确后，孔德亮再次开启了集中的“空中飞人”模式。这一次，他的行李箱里还带上了大量的宣传折页。一方面，为一线销售送上卖货“神器”；另一方面，直接面对客户，帮助客户理清思路，把复杂的数据安全建设需求进行拆解，并给出相应解决方案。数据安全的业绩就这么有声有色地做起来了。

2022 年上半年，爱拼爱赢的孔德亮又一次取得了漂亮的成绩。但他却说，不要过分看重个人的贡献，正确的选择和一个适当的平台更为重要。

在互联网崛起的时代，他选择了技术方向，让自己站在了一个相对高的起点；选择入职奇安信，勇敢迈出了自己转型的一大步；审时度势，看中工业互联网和数据安全的发展趋势，把握住公司和行业的重点方向，才有了团队取得的一个又一个成绩。

孔德亮非常喜欢一句励志名言：未来就是你站在茫茫大海的这一边，遥望着海的那一边，充满好奇心，憧憬着对海那边的向往，正是对未知的不了解与向往，所以才有了去追逐未来的勇气。

未来，孔德亮和创新 BG 团队希望成为这个行业的创新者。在这个变化已经成为生活本身的时代，他们愿意去拥抱变化，秉承“探索精神”的理念，持续优化产品体验、提升技术能力、完善服务体系，为社会提供更可被信赖的安全产品，为客户带来更多的惊喜。

“因为相信，所以看见，让我们携手共同创造更美好的未来！”安

▲ 蜀山之王的日落金山，可以给观众带来好运

▼ 魔鬼城的日落

▲ 2021年第一场雪天坛皇穹宇

作者 终端 BG 国产化事业部 王洪飞

▲ 颐和园冬至时的金光穿洞

▼ 2021 年第一场雪天坛祈年殿

金秋下的喀纳斯河

一场“他逃、他追，他插翅难飞”的博弈大戏

作者 公关部 王梦琪

在攻防领域，“未知攻焉知防”“说一百遍不如打一遍”等金句始终广为流传，其本质上都是要求防守方需要具备攻击视角，从攻击者角度换位思考，分析总结攻击方在各个阶段可能会采取的方式，才能守好防线。今天，我们就来讲一下攻击者的核心一击——“投毒”，即目标植入。在这一阶段，从攻击者的视角来看防守，无非就是一场“他逃、他追，他插翅难飞”的博弈大戏。

江湖高手都是怎样成功投毒的?

在古龙武侠小说《多情剑客无情剑》中，有这样一位用毒高手，名为五毒童子，苗疆极乐峒峒主，擅长下毒，身形矮小如幼童，绝招为“极乐虫”与五毒水晶。五毒童子的用毒功夫可谓是出神入化，已经达到登峰造极的程度，可借助一切动植物为媒介产生毒杀人，武林中人无不闻风丧胆。在追杀主人公李寻欢的过程中，曾言到：“到今夜为止，死在我手上的人已有三百九十二个，非但从来没有一人见到过我，根本连我的影子都看不到。”

这一幕中，李寻欢被误认为是梅花盗，田七和心眉大师押送李寻欢前往少林寺。五毒童子为给徒弟报仇，在半路多次截杀李寻欢。第一次，李寻欢打败另一个追杀者伊哭后，一行人在饭馆吃饭，李寻欢刚夹了块红烧豆腐送到嘴旁，就意识到菜中有毒，果不其然，邻桌四个和尚已被毒死。第二次，李寻欢等人不敢吃喝，田七看到车夫吃馍喝汤后试图吃车夫的馍，李寻欢仍说有毒，田七掰了块馍给路边的狗吃，狗被毒死了。第三次，田七看中了大街上穷孩子碗里的饽饽，认为五毒童子不会恰好选中这个孩子下毒，于是放心的吃饽饽，李寻欢仍坚持不吃，结果田七和心眉大师全都中了剧毒。

整个过程中，李寻欢等人在明处，五毒童子潜藏在暗处，伺机而动。在被李寻欢杀死之前，五毒童子的所向披靡在于其高深的用毒水平，五毒童子会在什么时候下毒？毒药下在了哪里？用的又是什么毒？是否有药可解？这里面的两个关键点就是未知与隐匿，没有人能勘破的下毒手段和无人可解的剧毒，算计好了天时地利与众人的心理活动。

同样，在实战攻防演习中攻击者进行目标植入的阶段，也需要像五毒童子一样，思考怎样才能不被防守方发现，成功将攻击武器植入目标内部。通常情况下，攻击者基于白利用、高级后门、加壳、沙箱逃逸等多种技术方式，在目标机器上安装恶意软件、执行攻击代码，并且实现持久化利用，逃避安全软件的查杀。

攻击者的“秘密武器”：0day、无文件攻击与高级后门

荆轲刺秦王式的图穷匕见并不是一个好的选择。早期的实战攻防演习聚焦内网边界的攻击，近几年则更流行供应链攻击、社工钓鱼等手段。攻击者的攻击手法五花八门，攻击样本多种多样，防守方的查杀水平也水涨船高。大多数情况下，针对攻击行为，现有的查杀防护系统可以对比恶意软件特征库快速自行处置，但仍有个别极难被发现的“秘密武器”，如 0day 漏洞攻击、无文件攻击和高级后门等。

顺应上文的说法，五毒童子下毒的高深之处关键在于未知与隐匿，那么 0day 漏洞恰好象征着未知，无需介质的无文件攻击和高级后门则代表着隐匿，这类攻击也是近年来攻击者最爱用的攻击手段。

从攻击者视角来看，0day 漏洞攻击成功的关键在于穿透现有基于规则的防护技术，具有极强的突发性和破坏性。即使防守方在发现攻击后意识到了 0day 漏洞的存在，但仍然无法立即修复漏洞，多数情况下只能被迫关停服务器或者系统，等待厂商发布漏洞补丁。

另一种无文件攻击，其中，最常用的一种手段“内存马”，其历史可以追溯到十几年前。这种古老的攻击手段通过将木马注入到系统进程和删除自身进程的方式，来躲避杀毒软件的查杀和实现自身的隐藏。删除自身并且在内存中驻留隐藏，意味着内存马具有较强的隐蔽性，增加了检测难度。

还有一种是指令劫持类高级后门。此前，奇安盘古实验室发布报告，发现美国国家安全局的黑客组织“方程式”利用顶级后门“电幕行动（Bvp47）”，对包括中国在内的 45 个国家开展长达十几年的监控，再次证明类似“双脉冲星、鬼影变种”等这类高级后门绝非个例。它们普遍通过更改原本正常的指令控制流，进行额外的恶意逻辑判断或执行，从而实现攻击者的恶意目的。因此，当安全软件读取文件中的代码进行匹配时，攻击者就可以将更改过的、与内存中一致的数据返回给调用者，让其认为两者是一致的，并不存在问题，从而绕过安全检测，实现隐匿效果。

隐蔽性强、种类多、范围广……这些攻击手段都让防守队如临大敌。

防守有道：新一代安全软件让威胁无所遁形

攻击者利用各种恶意软件发起攻击，来达到后续破坏系统、盗取数据或横向渗透等目的，常规的杀毒防护软件在面对未知且隐蔽性强的攻击时很难识别出来，对此，奇安信安全专家建议，防守方应尽快部署新一代安全软件，尤其是加强针对“免杀”“高级后门”“无文件恶意软件”的查杀能力。

针对服务器侧的恶意攻击，服务器安全管理系统（椒图）基于服务器轻量级 Agent，能有效保护服务器操作系统及应用，通过资产清点、基线检查、漏洞检测、虚拟补丁、应用防护（RASP、IN-APP WAF）、系统加固、Webshell& 病毒查杀、攻击溯源等功能，有效抵御黑客攻击和恶意代码，实现资产发现 - 漏洞检测 - 漏洞利用防护的闭环管理，帮助防守方从战前准备、攻防对抗、回溯分析三个阶段构建服务器端防护体系。 在攻防对抗阶段，针对各类恶意软件攻击，尤其是 0day 漏洞攻击和无文件攻击等，椒图聚焦服务内部的持续监测与响应，这也是其核心优势所在。

在实战攻防演习中，终端就是攻防对抗的“着陆点”、双方必争之地。防守方可选择奇安信天擎终端安全管理

系统（简称“天擎”），基于奇安信全新的“川陀”终端安全平台构建，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，充分满足防守方从备战到实战不同阶段的差异化防守需求。

依托奇安信深厚的攻防技术及安全大数据积累，自主研发的奇安信云安全引擎（QCE）、猫头鹰（QOWL）、海狮人工智能（QDE）、六合引擎（DLHE）及天狗（QTVP）等多个主动防御引擎和高级威胁防御引擎，再结合奇安信强大的攻防研究能力和丰富的规则库储备及生产能力，奇安信天擎可提供强大的持续监测、响应能力，实现对可疑行为、未知高级威胁的高效检测、准确定位、完整溯源，为终端的安全运行提供有力保障。

针对 0day 漏洞问题和高级后门的问题，奇安信历时四年打造了全新一代安全技术“天狗”，并推出了领先业界的产品——奇安信天狗安全防护平台。基于内存指令执行序列进行安全检测的技术，配合“非白即黑”的安全策略，能够有效解决 0day 漏洞攻击问题。值得一提的是，针对高级后门，“天狗”还创新使用了 CPU 硬件能力，实现了对全控制流进行检测。利用该创新技术可以发现各类公开或未公开的指令劫持类高级后门，从而有效保障安全产品的能力不会被这些后门影响从而失去应有的效果，让安全检测结果可信。安

奇安信 | BEIJING 2022

北京2022年冬奥会官方网络安全赞助商

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

齐向东受邀参加全国政协“深入实施新时代人才强国战略”专题协商会

7 月 19 日，全国政协在京召开“深入实施新时代人才强国战略”专题协商会，中共中央政治局常委、全国政协主席汪洋，中共中央政治局委员、中组部部长陈希出席并讲话。北京市政协委员、奇安信集团董事长齐向东受邀参加会议并发言，就“加快培养面向世界科技前沿和国家重大需求的创新人才”角度给出建议。

齐向东建议，重大前沿技术研发工程需要围绕龙头企业来开展，鼓励龙头企业针对“卡脖子”难题，通过承担国家重大前沿技术研发工程，培养创新技术人才；打通企业和高校两个蓄才池，在国家重大需求领域，联合培养能够解决复杂问题的卓越工程师；选取重点产业开展育才引才试点，国企、民企一视同仁，打造更优的软环境。

奇安信与吉大正元达成战略合作 联合助力网络安全产业生态发展

7 月 20 日，奇安信集团与吉大正元签署战略合作协议。双方将重点围绕密码技术应用、密评、浏览器、车联网等多个产品技术、解决方案及市场等多个领域进一步深化合作，共同携手推出全方位解决方案，推动网络安全整体架构的进化，夯实数字经济的安全底座。

打造产学合作新标杆 奇安信与北京交通大学达成合作

7 月 11 日，奇安信与北京交通大学合作协议签约仪式在奇安信安全中心举行。双方将在技术创新合作、产学研合作、行业应用推广、人才交流培养等方面进行深入合作。针对网络威胁检测及态势感知技术等前沿及行业应用进行探索和研究，推进信息安全技术及密码技术领域合作，并积极尝试成果转化，促进核心技术产品化。同时筹划建设联合实习实践基地，鼓励基于网络安全生态的教学课程体系建设，实现基础课程到实训教学到场景实战的贯通。

盘石司法鉴定所首批获评司法鉴定机构诚信等级 A 级

近日，奇安信旗下盘石软件（上海）有限公司计算机司法鉴定所，通过司法鉴定机构自查自评、上海市闵行区司法局初评、上海市司法局综合评估并公示等流程，在司法鉴定机构诚信等级评级中荣获诚信评估 A 等级，为第一批 13 家获得 A 等级评级的鉴定所之一。

作为上海第一家通过 CNAS 认证认可的民营计算机类司法鉴定机构，盘石司法鉴定所于 2007 年获得上海市司法局颁发的“司法鉴定许可证”，已协助相关执法部门破获数千起涉及电子证据的案件，处于上海同类机构先锋的位置，为多起轰动全国的案件提供了专业的司法鉴定服务。

奇安信司法鉴定业务负责人段继平表示，盘石司法鉴定所是目前国内少数能够通过自主研发软件进行取证与分析的电子数据司法鉴定机构，具有独立的实验室场所，其中包括：案件受理区、数据恢复区、手机取证区、计算机取证区、屏蔽室、无尘工作间和物证室，并配备多种国内外先进的技术设备检验及辅助设备。


◆机构名称：盘石软件（上海）有限公司计算机司法鉴定所　　诚信评估等级：A
机构住所：上海市闵行区合川路 2555 号 3 幢 4 层
办公场所：上海市闵行区合川路 2555 号 3 幢 4 层
法定代表人：李　毅
机构负责人：李　毅
电　话：（021）52658848　　传　真：（021）52809766
邮　编：201103　　电子邮箱：liyi@pansafe.com
许可证号/统一社会信用代码：91310107736681367B
业务范围：电子数据鉴定
能力验证情况：电子数据提取与分析（电子数据存在性鉴定）、电子数据功能性鉴定项目。评价结果为满意。

奇安信中标深圳市龙华区政务网络安全智能感知项目

近日，深圳交易集团有限公司龙华分公司发布公告，奇安信网神信息技术（北京）股份有限公司独家中标深圳市龙华区政务服务数据管理局龙华区政务网络安全智能感知项目，中标金额为 1450 万。

该项目旨在“智慧龙华”已有安全成果的基础上，利用大数据、人工智能等信息化技术，完成智能化感知改造，全面提升网络安全风险感知的精准度和覆盖面，构建全方位一体化、动态化的纵深领域防御体系，配合完成市区网络安全应急处置联动机制体制建设，进一步夯实网络安全保障体系，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力，为智慧龙华的建设保驾护航。


[公开招标]深圳市龙华区政务服务数据管理局龙华区政务网络安全智能感知项目成交公告

深圳交易集团有限公司龙华分公司
中标（成交）结果公告

一、项目编号：LHJC2022000092
二、项目名称：深圳市龙华区政务服务数据管理局龙华区政务网络安全智能感知项目
四、中标（成交）信息
供应商名称：奇安信网神信息技术（北京）股份有限公司
供应商地址：北京市西城区西直门外南路26号院1号楼5层
中标（成交）金额：14,500,000.00元
五、主要标的信息

名称	服务范围	服务要求	服务时间	服务标准
深圳市龙华区政务服务数据管理局龙华区政务网络安全智能感知项目	深圳市龙华区	详见招标文件	详见招标文件	详见招标文件

《数据出境安全评估办法》公布 奇安信与普华永道达成战略合作

7 月 7 日，奇安信与普华永道举行战略合作签约仪式。双方将充分发挥各自优势，围绕国际化战略布局、打造网络安全产品和专业安全服务能力的联合解决方案、

推进全产业数字化网络安全咨询服务开拓三个方向展开深入合作，推动全产业数字化网络安全咨询服务，加速国内网络安全产业布局海外市场，共同守护数据跨境安全流动。

2017 年 9 月，普华永道中国成立了普华永道“一带一路”全景平台，与奇安信的战略合作，也将依托该平台，充分发挥双方资源优势和能力优势，共同拓展国内外信息安全市场。

奇安信加入网络安全学生创新资助计划

在中央网信办指导下，由中国网络空间安全协会、中国互联网发展基金会支持，奇安信集团与西安电子科技大学、北京航空航天大学、山东大学、东南大学、四川大学等高校的一流网络安全学院，围绕网络安全人才培养、共建网络安全教学及科研实践基地、网络安全技术研究合作等方面进行深入合作，加入网络安全学院学生创新计划，共同培育网络安全人才基础性创新能力。

“奇安信作为网络安全行业领军企业，有责任、有义务参与其中，探索人才培养创新机制。”齐向东介绍，秉承以人为核心的安全运营服务，奇安信已形成了包括研究型人才培养、应用型人才培养、继续教育、特殊人才培养、国家安全意识教育等方面的完整解决方案。

超八成数据被盗涉及人为因素 齐向东建议企业做好“三防”

2022 年全国工商联主席高端峰会暨全国优强民营企业助推黑龙江高质量发展大会上，北京工商联副主席、奇安信集团董事长齐向东发表“企业数据要‘三防’：防违法、防盗窃、防勒索”主题演讲，他指出，企业数据违法将面临巨额罚款，需加快建立自证清白的技术体系，以内生安全守护企业数据安全。

奇安信牵头“电信和互联网行业数据安全人才强基计划”产业促进工作

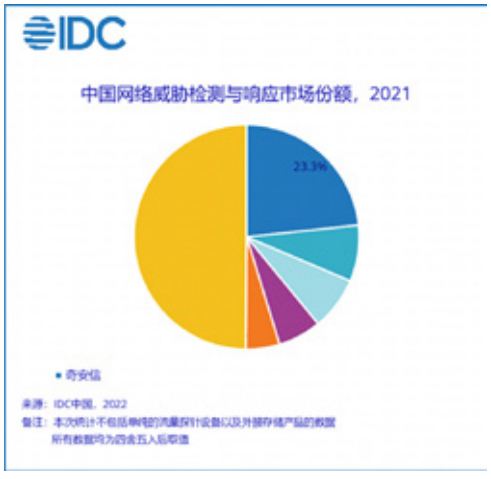
7 月 1 日，中国互联网协会联合中国信息通信研究院牵头开展的“电信和互联网行业数据安全人才强基计划”首次工作会议上，奇安信集团作为唯一一家网络安全企业，与中国电信、中国移动、中国联通三大运营商一起担任牵头单位，负责推进数据安全人才强基计划工作。

作为产业促进组牵头单位，奇安信围绕项目组“建设数据安全人才培养长效保障机制”职责，梳理了产业促进组的六项重点工作任务：数据安全人才现状调研、数据安全人才交流、拓展市场活动平台、促进数据安全产教融合、促进数据安全相关成果形成行业标准、为人才培养与产业发展搭建良性互动平台，并细化为 17 项具体工作举措。

荣誉墙

奇安信持续领先网络威胁检测与响应市场

近日，IT 市场研究和咨询公司 IDC 发布针对中国 NDR 产品的《中国网络威胁检测与响应市场份额，2021：实战效果显著，市场需求明确》报告，数据表明，中国网络威胁检测与响应市场在 2021 年实现了 36.6% 的同比增长，规模达 3.1 亿美元。其中，奇安信作为该市场的主要玩家，凭借其在政府、金融、运营商、公共事业、医疗等重点行业的广泛覆盖，以及奇安信网神威胁监测与分析系统（简称：天眼）在市场上的良好口碑，最终以 23.3% 的市场份额排名第一。



奇安信入选首批数据安全产业系列工作组成员单位

近日，中国计算机行业协会数据安全专业委员会公布首批数据安全产业专家委员会成员和系列工作组成员单位名单。奇安信集团董事长齐向东为数据安全产业专家委员会常务委员，奇安信集团副总裁韩永刚为委员，奇安信集团成为数据安全产业标准工作组、数据安全产业能力评价工作组、数据安全产业人才培养工作组、数据安全产业研究工作组 4 个系列工作组成员单位。

齐向东表示，奇安信将积极参与数专委分配工作，主动履行工作组的各项职责，推动建设数据安全产业创新体系，实现我国数据安全产业高质量发展。

附件 1：

首批数据安全产业专家委员会和系列工作组成员单位名单

1. 数据安全产业专家委员会（按姓氏笔画排序）

主 任 委 员：郑建华　　中国科学院院士

副 主 任 委 员：

刘文强　　中国电子信息产业发展研究院党委书记、副院长

李京春　　中国网络安全审查技术与认证中心首席专家

陈兴荣　　四川大学网络空间安全学院院长、教授

陈　鑫　　中国电子科技网络信息安全有限公司董事长

郝志强　　国家工业信息安全发展研究中心副主任

魏　亮　　中国信息通信研究院副院长

常 务 委 员：

于程水　　中铁建发展集团有限公司党委委员、副总经理

左晓栋　　中国科学技术大学网络空间安全学院教授

伍爱群　　上海航天信息科技研究院院长

仲　悦　　成都卫士通信息产业股份有限公司总经理

刘海峰　　北京市政务信息安全保障中心主任

刘琪煜　　国家信息技术安全研究中心副主任

齐向东　　奇安信科技集团股份有限公司董事长

安　晖　　中国电子信息产业发展研究院副总工程师

孙景锋　　中国联合网络通信有限公司数字化部（信息安全部）总经理

赛迪发布中国特权账号市场报告 奇安信位列重点头部厂商

近日，赛迪首次正式发布《中国特权账号管理平台市场研究报告（2022）》，《报告》指出，当前我国各类企业对于特权账号管理类产品的需求度相对较高，市场规模持续保持持续增长趋势。其中，奇安信被列为特权账号领域重点头部厂商之一。

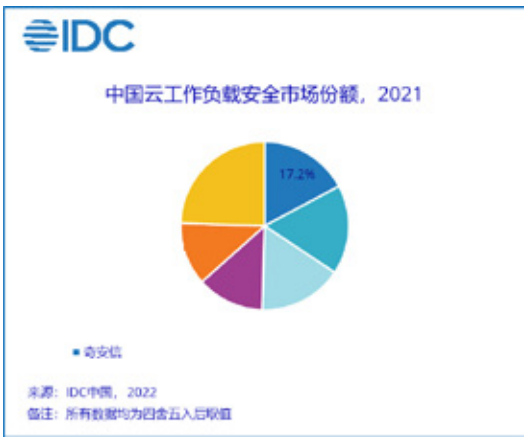
在国内特权账号管理平台产品市场的重点厂商中，奇安信凭借其在网络安全领域的综合实力，以及在特权账号管理产品上强大的产品实力，处于重点厂商中的头部地位。其产品在功能方面以其改密的准确度、账号存储安全性、风险账号发现及其呈现维度和方式，特别是弱密码检测；融合奇安信数据安全能力推出的特权卫士解决方案深入匹配客户需求。另外，推出的特权账号风险检测工具和账号口令安全检测服务，更具备实战防守意义，充分匹配《报告》中攻防演练场景中特权账号管理偏向工具化与服务化的市场趋势。

规模和增速双爆发！奇安信云工作负载市场份额位居第一

IT 市场研究和咨询公司 IDC 发布《中国云工作负载安全市场份额，2021：云原生与安全左移驱动技术持续创新》，针对 2021 年中国云工作负载安全市场的规模、增长速度、主要玩家、市场与技术的发展趋势等内容进行了详细研究。

《报告》数据显示，中国云工作负载安全市场在 2021 年实现了规模和增速的双爆发，市场规模达到 2.8 亿美元，同比增长 57.9%。其中，奇安信以 17.2% 的市场份额位列第一，彰显了在云工作负载安全领域的实力。

这也是今年继终端安全、AIRO、咨询服务领域之后奇安信集团拿下的第四个中国市场份额第一，标志着产品及实力再获市场和权威机构认可。



奇安信车联网安全网络靶场荣获中国智能网联汽车技术创新成果奖

在中国汽车工程研究院、中国汽车信息化推进产业联盟、重庆市招商投资促进局、北京中汽智联科技有限公司共同主办的 2022 中国智能网联汽车创新成果大会上，奇安信集团“车联网安全网络靶场”荣获中国智能网联汽车创新成果奖。

面对复杂的应用环境，车联网安全能力需要在实战中进行检验。奇安信集团自主研发的车联网安全网络靶场，以车联网系统中各种安全威胁和防护问题为研究对象，依托于提供的演练环境及靶场功能，构建风险评估系统和产品测试系统，可提供安全评估和产品测试能力。

两案例入选信通院 2022 安全守卫者计划优秀案例

近日，中国信息通信研究院公布了 2022 安全守卫者计划。凭借在软件供应链安全的丰富实践和技术积累，奇安信申报的“基于 DevOps 的供应链安全实践”和“开源软件安全治理体系”获 2022 安全守卫者计划优秀案例。

中国信通院还公布了“业务安全推进计划”成员单位，奇安信集团入选为首批成员单位。

奇安信零信任入选工信部信息技术应用创新典型解决方案

在 2022 新一代信息技术融合应用创新云峰会上，奇安信提报的“奇安信零信任身份安全解决方案”，入选了 2021 信息技术应用创新典型解决方案。

为了打造安全可信框架下的中国特色零信任解决方案，作为国内零信任身份安全的首倡者，奇安信于 2018 年率先将零信任安全理念及技术系统介绍到国内。经过持续的技术研究和产品迭代研制，并契合“十四五”数字化转型需求，奇安信已打造出国内一流、国际领先的基于 PKS 的零信任动态授信体系化产品，支持模块化构建零信任动态授信平台。

同时，方案结合应用场景，模块化、体系化地实施零信任访问控制与身份安全大数据服务，所采用产品均具有国产自主知识产权，并广泛应用于党政、金融、通信、能源等领域，在传统办公访问场景及云计算、大数据中心、物联网等新 IT 场景下实施整体、主动、持续的安全防护，保障国家关键基础设施重要信息系统的信息安全。

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