

网安26号院

S E C U R I T Y I N S I D E R



解读

2020

安全态势

首家银行系金融科技子公司

兴业数金 系兴业银行集团旗下金融科技子公司，成立于2015年12月。面向集团，作为集团高科技内核和创新孵化器，全面负责兴业银行集团科技研发和数字化创新工作。对外，兴业数金致力于运用云计算、人工智能、开放API、流程机器人等前沿科技，为商业银行数字化转型提供解决方案，输出科技产品与服务。



更多业务交流与咨询，可联系寿先生：13774399844，欢迎垂询。

阴霾中的光明和希望

当你拿到这本小刊的时候，可能已是节后，我们正踌躇满志、着手新一年的工作。

岁末年初，网络安全行业有回顾与展望的传统。

2020年，网安人经历了少有的阴霾时光。疫情肆虐之际，也是网络攻击组织狂欢之时。从保障健康的医疗机构，到保障生产生活的关键基础设施，都成为攻击者肆意攻击的目标。黑客组织丝毫没有放松攻击的步伐：窃密、破坏、勒索，惊人的网络安全事件频频出现。全球网络攻击数量、漏洞数量、数据泄露数量创下新高。在严峻的安全形势面前，任何机构的丝毫麻痹与轻视，都可能令自己成为下一个受害者。

在挑战面前，我们选择守望相助。为保障疫情防控一线单位的网络安全，包括奇安信在内的网络安全企业纷纷援手。其中，奇安信发起了网络安全行业迄今为止最大规模的捐赠行动，向全国19个省、市、自治区，100多家医院（包括火神山、雷神山）和疾控等疫情防控一线单位捐赠了专业设备和服务，累计达成产品和服务捐赠意向金额达数千万元。奇安信还利用大数据技术和工具，绘制疫情态势感知图，快速切断感染途径，为打赢疫情防控阻击战提供技术保障。就我国而言，疫情期间没有发生灾难性的网络安全事故，这在一定程度上体现了我国抵御网络攻击的基本能力已初步形成，更展示出了我们安全人在疫情期间的担当与守望相助。

阴霾中更看到光明与希望。在安全风险面前，我们选择了拥抱创新与变化。2020年疫情加速数字化转型，也进一步推动了网络安全技术的创新。内生安全框架发布、零信任方案逐步落地、实战化能力强化、敏感数据防护技术等创新成为2020年的亮点。政府和企业客户日益认识到网络安全的重要性，更加主动接受新型的产品和服务。上市的网络安全公司披露的报告显示，第三季度财务收入增幅平均超过35%，其中奇安信增速最快，达到了89%。

2020年，安全人同舟共济、携手战“疫”，共同应对网络安全行业的挑战。2021年，面对不确定的未来，网络威胁仍是最确定的安全风险，各行各业的安全人更应该携手创造网络安全的新未来。

总编辑

李建平

2021年2月1日

安全态势

P4-P5 事件篇

- 新西兰央行大量敏感数据泄露：因第三方托管服务被黑
- 惊险一刻：刚果国家顶级域名险遭黑客控制
- 遭暗网贩卖，Nitro PDF 服务 7700 万用户数据全部泄露
- 苏格兰环保局遭勒索袭击，要瘫痪数月才能恢复



P6 漏洞篇

- Drupal 目录遍历漏洞 (CVE-2020-36193) 预警
- 国家漏洞库关于 Dnsmasq 多个缓冲区错误漏洞的通报
- Oracle WebLogic Server 远程代码执行漏洞安全风险通告
- 开源堡垒机 JumpServer 远程命令执行漏洞预警

P7-P9 政策篇

- 中国银保监会印发《监管数据安全管理办法（试行）》
- 最高检印发《人民检察院办理网络犯罪案件规定》
- 《互联网用户公众账号信息服务管理规定》修订版发布
- 从《监管数据安全管理办法》看金融数据安全保护趋势和应对策略



P10-P12 政协提案

- 建议网络安全投入占比提高至 15% 以上打造标杆项目
- 北京应构建网络安全“双能力”保障体系守护首都大安全格局

P14

月度专题

解读 2020 安全态势

奇安信安服团队、威胁情报中心、安全监测与响应中心、技术研究院、行业安全研究中心、补天漏洞响应平台及虎符智库、工业控制系统安全国家地方联合工程实验室，同时发布了 7 份网络安全 2020 年度研究报告，重磅信息披露，呈现独家观点及安全态势解析。



攻防一线

P26

不咬钩也被钓鱼？当黑客团伙盯上了供应链，千里之堤竟毁于一旦

安全之道

P30

为区域基层医疗机构 构筑“积极防御”体系

奇安信人

P34

齐向东：五五制
打造高效有战斗力的组织

P38 我在奇安信
一层一层叠出世界

奇安信资讯

- P44 | 奇安信荣获第三届进博会“网络安全突出贡献奖”
- P44 | 奇安信双向网闸荣获中国信息安全测评中心最高级别认证
- P44 | 奇安信代码安全实验室获微软官方致谢
- P45 | 奇安信威胁情报荣获“2020 年度‘新基建’优秀解决方案”奖
- P45 | “格格病毒”潜伏十余年发威 奇安信公布病毒发作日历
- P46 | 奇安信董事长齐向东谈职场：干网络安全要甘于寂寞
- P46 | 2021 数字中国创新大赛启动 第二届“虎符网络安全赛道”升级助推数字中国建设

报告速递

P48

《安全运营中心调研分析报告》

安全意识

P51

疫情期间，防范恶意软件 / 钓鱼邮件“趁火打劫”



第 2 期

《网安 26 号院》编辑部

主办

奇安信集团

总编辑 李建平

副总编 裴智勇

安全态势主编 王彪

月度专题主编 李建平

攻防一线主编 魏开元

安全之道主编 张少波

奇安信人主编 孙丽芳

奇安信资讯主编 陈冲

报告速递主编 张文辉

安全意识主编 李建平



奇安信集团



虎符智库



安全内参

投稿邮箱 26hao@qianxin.com

联系电话 13701388557

> 事件篇**新西兰央行大量敏感数据泄露：因第三方托管服务被黑**

据 NBC News 消息，新西兰中央银行近日表示，某身份不明的攻击者已经成功入侵其内部一个数据系统，并且可能已经访问了商业及个人敏感信息。

这家位于新西兰惠灵顿的国家银行在声明中表示，遭到非法访问的是新西兰储备银行用于共享及存储敏感信息的第三方文件共享服务。

央行行长 Adrian Orr 表示，违规行为已经得到遏制。“我们正与国内外网络安全专家及其他相关机构紧密合作，对此次恶意攻击开展全面调查。” Adrian 说，“目前我们仍在确定可能遭遇泄露的敏感信息的性质与范围，其中可能包括部分商业及个人敏感信息。”

相关系统已断开网络连接并受到全面保护，直到调查完成才会重新上线。

Adrian 提到，“要筛查此次事件的全部影响，确实还需要一定时间。我们正与信息可能受到影响的系统用户进行合作。”

该银行拒绝在采访邮件中就更多细节发表进一步评论。目前尚不清楚此次违规事件的发生时间，也无法判断攻击是谁所为、文件共享服务位于哪个国家 / 地区。

过去一年以来，新西兰多个主要组织先后沦为网络攻击活动的目标。特别是新西兰证券交易所，其服务器曾在 2020 年 8 月遭 DDoS 攻击被迫关闭近一周。

奥克兰大学计算机科学教授 Dave Parry 在采访中表示，此次银行数据泄露的幕后黑手很可能是其他国家政府。Dave 总结道，“如果从类似犯罪活动的视角来看，政府机构一般不会支付勒索攻击赎金或者采取其他类似的妥协性回应，因此这类攻击大概率出自别国政府的利益诉求。”

**惊险一刻：刚果国家顶级域名险遭黑客控制**

据 portswigger.net 消息，安全研究员 Fredrik Almroth 近日发表博客称，刚果民主共和国国家顶级域名 .cd 的一个名称服务器域名忘记续费，导致被他接管了一段时间，在 2020 年底短暂获得了这个顶级域名大约 50% 的 DNS 流量控制权。Fredrik 在日常扫描中发现，.cd 的名称服务器 scpt-network.com 即将过期，他表示在过期后马上买下，避免被攻击者劫持。Fredrik 在后续联系了 .cd 的联络人，对方重新设置了新的名称服务器。

**遭暗网贩卖，Nitro PDF 服务 7700 万用户数据全部泄露**

据 BleepingComputer 消息，包含超过 7700 万条 Nitro PDF 用户记录的数据库被盗，被知名威胁者 ShinyHunters 免费公开泄漏。此次公布的这个 14GB 的泄漏数据库包含 77,159,696 条记录，其中包含用户的电子邮件地址、全名、bcrypt 哈希密码、标题、公司名称、IP 地址以及其它与系统相关的信息。Nitro 是一款可帮助创建、编辑和签署 PDF 和数字文档的应用程序，声称拥有 1 万多个商业客户和大约 180 万许可用户。

苏格兰环保局遭勒索袭击，要瘫痪数月才能恢复

据 heraldscotland.com 消息，英国苏格兰环境保护局表示，内部网络系统在 2020 年圣诞节前夜被某“组织严密的国际网络犯罪团伙”所破坏，对方提出索要赎金，被环保局拒绝。犯罪团队窃取了超 1GB 敏感数据，包括员工个人信息、监管和合作企业信息等。环保局方面称，尽管受感染系统已经隔离，但恢复工作将需要相当长的时间，完全恢复可能要半年之久。不过环保局的环境预警职能未受影响，官方已经找到继续提供服务的方法。



第四家安全公司中招！Malwarebytes 也遭 SolarWinds 黑客入侵

据 ZDNet 消息，美国网络安全公司 Malwarebytes 表示，遭到 SolarWinds 幕后黑客入侵，攻击者染指了其部分内部电子邮件。Malwarebytes 称，它并未使用 SolarWinds 的软件，攻击者利用了另一手段，窃取了拥有 Microsoft Office 365 和 Azure 环境访问特权的应用权限。在 FireEye、微软和 CrowdStrike 之后，Malwarebytes 成为第四家内部防线被 SolarWinds 黑客突破的主流网络安全供应商。



敏感财务信息遭黑客窃取，英特尔被迫提前发布财报

据新浪科技消息，英特尔表示，有黑客 1 月 21 日从该公司网站上窃取了敏感的财务信息，迫使该公司比预订计划提前发布财报。英特尔首席财务官乔治·戴维斯表示，该公司原定于周四盘后发布财报，但他们认为攻击者已经提前了解了最新财季的详细财报信息。“我们的公关新闻网站上有一张信息图被盗。”戴维斯说，“我们发现问题后立刻发布财报。”他并未披露更多详情，只是表示此次

信息泄露源自不法行为，并非该公司无意间泄露出去的。英特尔股价当天上涨逾 6%，并在交易时段最后 15 分钟突然拉升近 2%。



黑客泄露被篡改的辉瑞疫苗数据，以破坏民众对疫苗的信任

据 BleepingComputer 消息，欧洲药品管理局 1 月 15 日透露，网上流传的一些辉瑞/BioNTech 候选疫苗数据是被篡改过的，目的是为了破坏民众对新冠疫苗的信任。此前，欧洲药品管理局在去年 12 月被黑，相关的疫苗数据被泄露。12 月底，多个黑客论坛上开始流传所谓“欧洲药品管理局疫苗数据”。



德国电商 NBB 视频监控员工违反 GDPR，被顶格处罚 1040 万欧元

据 Security Affairs 消息，德国国家数据保护委员会 (LfD) 宣布，根据 GDPR 规定，对笔记本电脑和电子产品电商 NBB 视频监控员工至少两年处以 1040 万欧元罚款，这是德国目前针对 GDPR 的最高处罚。NBB 声称，安装摄像头是为了阻止和调查犯罪行为，以及跟踪仓库物流流动，对此次罚款名义表示失望。LfD 则表示，阻止盗窃有许多其它侵入性较小的措施。



艺龙酒店、东风出行等 157 款侵害用户权益，工信部公开通报

工信部近期组织第三方检测机构对手机应用软件进行检查，督促存在问题的企业进行整改。截至目前，尚有 157 款 APP 未完成整改，包括艺龙酒店、Metro 大都会、东风出行、永辉生活、芒果 TV 等，工信部要求上述 APP 应在 1 月 29 日前完成整改落实工作。

漏洞篇

Drupal 目录遍历漏洞 (CVE-2020-36193) 预警

工信部网络安全威胁信息共享平台发布漏洞预警，Drupal 发布了 Drupal 存在目录遍历漏洞的风险通告，CVE 漏洞编号: CVE-2020-36193。攻击者可利用该漏洞获取敏感信息，最严重的影响可造成远程代码执行。目前，Drupal 官方已发布最新版本修复漏洞，建议受影响用户及时升级至修复版本，做好资产自查以及预防工作，以免遭受黑客攻击。Drupal 是一套基于 PHP 语言编写的开源 CMS 系统。



国家漏洞库关于 Dnsmasq 多个缓冲区错误漏洞的通报

国家信息安全漏洞库 (CNNVD) 收到 2 个 Dnsmasq 缓冲区错误漏洞 (CNNVD-202101-1570、CVE-2020-25681) (CNNVD-202101-1569、CVE-2020-25682) 情况的报送。成功利用漏洞的攻击者，可进行内存破坏、拒绝服务等攻击，甚至可以远程执行恶意代码，最终控制目标服务器。Dnsmasq 2.83 以下版本均受漏洞影响。目前，Dnsmasq 官方已经发布了升级补丁修复了该漏洞，建议用户及时确认版本信息，尽快采取修补措施。Dnsmasq 是一款使用 C 语言编写的轻量级 DNS 转发和 DHCP、TFTP 服务器。

Oracle WebLogic Server 远程代码执行漏洞安全风险通告

奇安信 CERT 发布通告，Oracle WebLogic 产品中存在安全漏洞，漏洞编号 CVE-2021-2108，受此漏洞影响的版本包括 12.1.3.0.0，未经身份验证的攻击者可以通过 IIOP、T3 网络访问 WebLogic Server 利用此漏洞，成功利用此漏洞的攻击者可以接管当前 Oracle WebLogic Server。鉴于危害较大，建议用户及时安装更新 Oracle 官方于 2021 年 1 月发布的修复补丁。Oracle WebLogic Server 是 Oracle 旗下的适用于云环境和传统环境的应用服务中间件。



开源堡垒机 JumpServer 远程命令执行漏洞预警

工信部网络安全威胁信息共享平台发布漏洞预警，开源堡垒机 JumpServer 披露了存在远程命令执行漏洞的风险通告。攻击者可利用该漏洞执行任意命令。目前，JumpServer 官方已发布安全版本修复该漏洞，建议受影响用户及时升级至相对应安全版本，并做好资产自查以及预防工作，以免遭受黑客攻击。Jumpserver 是全球首款完全开源的堡垒机，是符合 4A 的专业运维审计系统。



2020 年工业信息安全漏洞 2138 个，环比上升 22.2%

国家工业信息安全漏洞库 (CICSVD) 发布《2020 年工业信息安全漏洞态势年度简报》报告显示，2020 年共收录工业信息安全漏洞 2138 个，环比上升 22.2%。其中，通用型漏洞 2045 个，事件型漏洞 93 个，涉及 335 家厂商，国外厂商占比 66.2%，我国厂商占比 33.8%。在收录的通用型漏洞中，超危漏洞 379 个，高危漏洞 899 个，高危及以上漏洞占比 62.5%。

政策篇



中国银保监会印发《监管数据安全管理办法（试行）》

中国银保监会印发《监管数据安全管理办法（试行）》，加强监管数据安全，防范监管数据安全风险。《办法》提出，银保监会建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。在监管数据活动生命周期中，要始终处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。银保监会统计信息部门负责统筹监管数据安全管理工作，银保监会各业务部门负责本部门监管数据安全管理工作。



最高检印发《人民检察院办理网络犯罪案件规定》

最高人民检察院发布《人民检察院办理网络犯罪案件规定》，要求人民检察院办理网络犯罪案件应当加强全链条惩治，坚持惩治犯罪与预防犯罪并举。人民检察院应当加强对电子数据收集、提取、保全、固定等的审查，充分运用同一电子数据往往具有的多元关联证明作用，综合运用电子数据与其他证据，准确认定案件事实。



《互联网用户公众账号信息服务管理规定》修订版发布

国家互联网信息办公室发布新修订的《互联网用户公众账号信息服务管理规定》，将在2021年2月22日施行。《规定》旨在进一步加强互联网用户公众账号的依法监管，促进公众账号信息服务健康有序发展。《规定》要求，公众账号信息服务平台应当履行信息内容和公众账号管理主体责任，设置内容安全负责人岗位，建立健全并严格落实信息内容安全、网络安全、数据安全、个人信息保护等管理制度。上线具有舆论属性或者社会动员能力的新技术新应用新功能，应当按照有关规定进行安全评估。



《区块链信息服务安全规范》等4项国家标准公开征求意见

全国信息安全标准化技术委员会发布公告，《信息安全技术 区块链信息服务安全规范》、《信息安全技术 公共域名服务系统安全要求》、《信息安全技术 信息安全事件分类分级指南》、《信息安全技术 信息安全管理体系 指南》4项国家标准现已形成标准征求意见稿，面向社会公开征求意见，反馈截止日期3月22日。



美国商务部发布《确保信息和通信技术及服务供应链安全》公开征集意见

综合消息，美国商务部发布《确保信息和通信技术及服务供应链安全》的最新规则，旨在落实特朗普政府第13873号总统令《确保信息和通信技术及服务供应链安全的总统令》（2019年5月15日发布）中列明的相关要求，建立并完善“用于识别、评估和处理美国人与外国人之间涉及设计、开发、制造或提供信息和通信技术或服务的某些交易（包括交易类别）”的流程和程序。该规则目前面向公众征集意见，计划于2021年3月22日生效。



美网络安全与基础设施安全局发布加强云服务安全配置建议

据fedscoop消息，美国网络安全与基础设施安全局（CISA）1月15日发布分析报告，介绍了近期处置的网络攻击成功案例，并给出使用云服务组织的安全实践。报告称，攻击者正在使用网络钓鱼、暴力登录、cookie传递等方式来利用受害者云服务配置中的不良卫生习惯，一旦进入系统，将进行设置自动转发邮件、搜索敏感关键字、隐藏安全警告邮件等行为。CISA为相关组织提供了21条加强云安全的建议，包括建立正常网络活动的基准、检查员工的邮件转发规则、使用多因素认证等。

美国公路安全局发布2020版《现代车辆的网络安全最佳实践》公开征求意见

据Nextgov消息，美国国家公路交通安全局（NHTSA）1月12日在联邦公报上公布《现代车辆的网络安全最佳实践》的自愿性指南，向业界征集意见。公路安全局在2016年发布首份《最佳实践》，这次2020修订版更新了OTA更新、加密方法、渗透测试和诊断等方面的内容，建议在整个软件供应链以及开发、实施和更新软件系统等整个生命周期纳入网络安全考量，呼吁汽车制造商实行软件物料清单制度等。《最佳实践》指出，现代车辆引入了大量网络连接和电子设备，为恶意黑客提供了更多危害其安全的机会。





从《监管数据安全管理办法》看金融数据安全保护趋势和应对策略

● 作者 数据安全子公司 姚磊
银行事业部 陈骏

近日，银保监会发布《监管数据安全管理办法（试行）》（简称《办法》），共7章34条，对监管数据全生命周期的安全管理提出了全面要求。本文对如何在监管数据的访问、使用等动态流转环节符合《办法》中的要求，进行解读和建议。

金融业是数据密集型产业，对数据的依赖程度较高，金融大数据的广泛应用更是促进了数据资源的爆发式增长，也引发了内部泄密、个人隐私保护、数据鸿沟等安全问题。近年来我国的金融管理部门、行业协会以及广大的从业机构在个人金融信息保护的制度建设和实践上做了大量的工作，法律规范不断完善，技术标准加速出台，行政监管持续发力，行业实现有序推进。但同时也要清醒地看到，在数字化时代下，金融数据安全在立法、监管、自律等方面依然有一些亟待解决的问题。

从权威机构的调研报告不难看出，金融行业数据保护依然存在薄弱环节。Forrester 调研报告指出，80%的数据泄漏都与特权账户凭证被窃取有关。相关数据也显示，数据泄露及贩卖也从单纯的交易数据演变到交易数据访问权限。如倒卖银行访问权限：黑市上有很多银行访问权限的倒卖活动，有的价格还很优惠，卖家号称可以提供对全球各家银行的远程访问。

《办法》提出，银保监会建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。在监管数据活动生命周期中，要始终处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。

金融行业的数据安全应该是在金融数据安全分级的基础上，建立金融数据全生命周期安全保护框架。明确金融数据风险防控及数据资产保护措施，保护金融数据在采集、传输、存储、处理、交换、销毁等各个环节的安全性，是金融监管机构实施准确、高效的数据安全管理的基础。

《办法》颁布后，如何在最短时间内做到性价比最好的数据安全防护和符合监管的要求，是每个相关金融机构需要思考的问题。我们认为做好监管数据的特权访问安全是短期内最行之有效的方法之一。具体建议思路如下：

1、使用多因素认证等方式对操作用户的身份鉴别，对业务系统、IT系统的特权账号进行加固，如定期轮换口令（此处说明，大部分用户会使用两个或多个高强度口令进行周期性轮换，基本上可以认定此种方式无任何安全作用，建议使用一些技术手段保障口令的安全性）；对存储在本地的特权账号或系统中的“硬编码”（如Web向数据库建立连接用的用户名密码）要及时消除。

2、数据使用必须遵循国家相关法律规定和行业安全规范，对数据的使用有明确的权限授权管理。数据访问权限严格控制最小化，并对过程进行全程细粒度的审计记录。如通过数据的细粒度权限访问控制技术对管理员、第三方运维人员以及临时运维人员进行有效的身份管理、运维权限控制、运维操作细粒度权限控制，同时支持对运维操作行为的安全审计，依据数据敏感等级及访问者角色实现数据动态脱敏，防止越权操作以及利用合法权限的数据窃取行为，实现数据操作权限最小化。

3、建立针对数据流动的监控，统计数据的访问、使用、流动行为，建立风险识别模型，预警、发现潜在的数据泄露、滥用行为，并提供数据风险的溯源分析能力。

数据，作为宝贵的资源具有双面性，既是动力，又是武器。特权访问安全将成为用户数据安全保护和企业发挥数据价值之间，最重要的那道把关者。如何找到安全最大化，效率较大化，弊端最小化的最优解将是我们一直致力探索的方向。安



政协提案

建议网络安全投入占比提高至 15% 以上
打造标杆项目

北京市政协委员 齐向东



十九届五中全会宣布，我国已经进入新发展阶段。新发展阶段是数字技术革命的加速期，网络安全是数字时代的底板工程，没有网络安全，数字技术的作用会大打折扣。想要加速实现第二个百年奋斗目标，亟需进一步加大网络安全投入，推动网络安全产业发展壮大。

目前，我国网络安全产业和西方发达国家相比，还有较大差距。为此，建议在北京市的重大信息化项目和关键信息基础设施中，将网络安全的占比提高至 15%，探索出具有示范效应的北京模式，推向全国市场，为我国网络空间安全筑牢底板。

一、我国和美国网络安全投入相差 10 倍，网络安全产业发展的速度跟不上数字化发展的需求

美国联邦政府一直高度重视网络安全投入。根据美国白宫公布的 2021 财年预算，IT 总预算为 922 亿美元，

网络安全领域总预算为 188 亿美元，和 2020 财年相比，高出了 14 亿美元。

从网络安全预算占 IT 预算比重来看，美国政府在 IT 上每投入 10 块钱，就有 2 块钱花在安全上。2021 财年美国政府的网络安全预算占 IT 预算的比重是 20.4%，国土安全部、司法部的这一比重更高，分别为 35.7% 和 28.5%（详情参见附表）。

事实上，美国政府在网络安全上的实际花费往往还要高于公布的预算。2020 财年美国联邦政府申请的网络安全预算是 174 亿美元，但实际支出 184 亿美元，折合人民币近 1300 亿。而我国 2019 年的网络安全产业总规模为 600 亿元，就是说，仅美国政府这一家大客户采购的额度就等于我国产业规模的 2 倍。

目前，我国网络安全投入占信息化的比重，和美国相差 10 倍以上，低于世界平均水平。IDC 统计数据显示，我国网络安全市场占信息市场的比重为 1.87%，和美国政府 20.4% 的比重相差十倍，同时也低于全球 3.74% 的平均水平，无法满足数字化发展的需求。

二、在重大信息化项目和关键信息基础设施中，将网络安全的投入占比提高至 15%，打造标杆项目，为全国提供示范模板

北京是全国科技创新中心，具备引领我国网络安全产业发展的最好条件。为此，建议充分发挥北京市在人才、技术、资本等方面的优势，把北京模式推向全国市场，为数字经济发展提供坚实的网络安全保障。具体建议如下：

（一）对网络安全预算占比提出强制要求，重大信息化项目和关键信息基础设施不低于 15%。建议由重点单位作为责任主体，市政府指导支撑，在 5G、工业互联网、智能制造等重点信息化项目建设中，明确提出网络安全预算比例不能低于 15%。同时，定期进行实战化演练，

监督检查各重点单位的建设与运行效果。

(二)加快推进信创工程,逐步降低供应链断供风险。建议北京市在需求侧,特别是重要单位,加快推进信创发展,以及密码应用和涉密系统保密工作,并在供给侧推动信创产业链发展,实现核心信息化与网络安全技术自主可控。

(三)建立骨干网络安全企业名录,及时解决他们在业务高速发展中遇到的难题,引导支持产业发展壮大。根据赛迪、信通院、IDC 等中外研究机构预测,未来十年网络安全产业会保持 25% 以上的增长。骨干网络安全企业,增长更快,达到 30% 以上,就是 3 年翻一番,10 年就能增长 8 到 10 倍。

目前,北京在网络安全产业规模上具有领先地位,其他省市也呈现加速追赶之势。北京必须保证比其他地区更快的增速,才能巩固已有优势,确保第一的地位。建议对骨干企业进行贴身帮扶,统筹整合分散在政府各部门的创新扶持资金,加大向骨干企业的倾斜力度,加

快形成一批创新能力突出的大公司,形成规模效应,推动产业发展。安

附表: 2021 财年美国网络安全预算占 IT 预算百分比(单位: 美元)

机构	网络安全预算	IT 预算	百分比
国防部	98.46 亿	388.15 亿	25.4%
国土安全部	26.04 亿	72.98 亿	35.7%
司法部	9.29 亿	32.65 亿	28.5%
财政部	6.89 亿	51.07 亿	13.5%
能源部	6.66 亿	28.47 亿	23.4%
卫生和公众服务部	5.19 亿	64.22 亿	8.1%
国务院	4.89 亿	26.34 亿	18.6%
退伍军人事务部	4.60 亿	77.61 亿	5.9%
商务部	3.78 亿	26.34 亿	14.4%
农业部	2.30 亿	23.72 亿	9.7%





政协提案

北京应构建网络安全“双能力”保障体系
守护首都大安全格局

北京市政协委员 齐向东

2021是十四五开局之年，习总书记强调，要抓住和用好我国发展的重要战略机遇期，把国家安全贯穿到党和国家工作各方面全过程，同经济社会发展一起谋划、一起部署，坚持系统思维，构建大安全格局。

当前，针对重要部门和关键信息基础设施的网络攻击层出不穷，重大事件和国家级活动期间网络攻击异常活跃。建议北京市构建系统完整、科学规范、运行有效的“双能力”保障体系，加快实现大安全格局。

一、供应链攻击、勒索攻击、国家级黑客等安全威胁日益频繁，对国家和首都的安全稳定运行带来了严峻挑战。

疫情的爆发加深了人们对数字化的依赖，但也让网络攻击面扩大，针对国家重要机构和重点行业的网络攻击激增，严重威胁国家社会的安全稳定。

（一）供应链成安全短板，是威胁网络安全的主要攻击手段。2020年12月，震动全美国的供应链攻击被曝光。奇安信CERT追踪分析发现，发动攻击的是一个数百人的组织，通过攻陷网络监控软件商“太阳风”，渗透了200多个重要系统，美国关键政府部门、企业大面积沦陷。

（二）勒索攻击活跃，关键信息基础设施成为重灾区。统计数据显示，勒索攻击约占2020年攻击事件数量的1/3。过去，勒索攻击主要为获取经济利益；现在，勒索攻击主要以关键信息基础设施为目标，严重影响社会国家的安全稳定。

（三）国家级黑客攻击日益频繁，组织性强，目的明确，是攻击政府机构的主要力量。2020年4月，我国国家安全部披露多起境外黑客窃密事件，黑客利用新型肺炎疫情相关热词发起攻击。疫情爆发后十天内，奇安信就成功拦截了针对疫情防控相关单位的CC攻击超过3亿次，Web应用攻击超过150万次。

疫情以来，我国未发生灾难性网络安全事故，体现

了我国抵御网络攻击的基本能力已初步形成。但随着数字化加速演进，网络攻击频率将更高、烈度更大，全面提高网络安全体系防御能力迫在眉睫。

二、坚持系统思维构建大安全格局，建立以“重点单位防御体系”和“网络空间监管与网空对抗体系”为核心的“双能力”保障体系。

为加快构建大安全格局，筑牢我国网络空间安全底板，建议北京市运用系统性思维，打造“重点单位防御体系”和“网络空间监管与网空对抗体系”为核心的“双能力”保障体系。

（一）“重点单位防御体系”主要是针对北京市的政企要害部门和关键信息基础设施，是北京市防御体系中的重点环节。重要单位的防御能力，是必须坚守的战略底线。建议由重点单位作为责任主体，市政府指导支撑，对重点单位进行规划指引、建设督促、实战运行监督，并通过政策对组织、机制、预算保障提出要求。同时，加快推进自主可控技术产品替代，推动教育、医疗、金融等重点行业网络安全运营中心建设。

（二）“网络空间监管与对抗体系”主要是针对防范重大网络安全风险，强化网络安全指挥、预警、应急和治理，实现挂图作战以及对高级威胁的诱捕和猎杀等能力。建议由北京市政府主导、重点单位参与、专业网络安全企业支撑，建立纵横交织的网络空间安全监管与网空对抗体系，加快实施打击网络犯罪、保护网空公共安全等重点工程建设，定期进行实战化演练。

（三）利用内生安全框架，实现“双能力”体系的高效协同。“双能力”体系是一个复杂的系统工程，需要在统一框架下，形成两个体系之间的支援与帮扶、反向的协同。内生安全框架是基于系统思维下的最新研发成果，能把安全能力内置到信息化环境当中，为“双能力”体系的建设发挥支撑作用，保障国家重要信息系统和关键信息基础设施的网络安全。安

“天眼+安服”创新安全运营服务

实战化攻防演习

网络安全重保

7*24小时应急响应

威胁溯源分析

奇安信 新一代网络安全领军者

奇安信融合自身的优势资源，推出了“天眼+安服”的安全运营服务。通过本地部署“天眼新一代威感知系统”检测网络中的各类安全威胁，再结合专家级的安全分析服务，有效应对高级持续性威胁（简称APT），为政企客户提供优质的安全运营服务。目前“天眼+安服”的安全运营模式已经在政府、金融、能源、教育等诸多行业当中应用，并得到了广泛认可。在未来1-2年，随着各种新型攻击的持续发生，该模式将成为政企高级威胁防护的主流。





解读 2020 安全态势

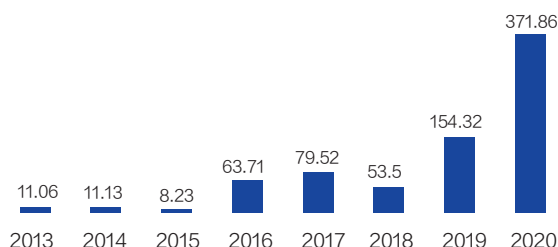
全球范围来看，2020 年网络攻击行动日趋频繁化和白热化，聚焦窃密的同时，对关键基础设施的攻击激增。与此同时，攻防博弈失衡加剧，信息系统“千疮百孔”，核心应用、网络设备和新技术的漏洞频发。在不确定的未来，安全威胁无疑是最确定的风险，唯有积极拥抱安全技术创新，才能领先攻击者，真正做到安全快一步。

1月20日，奇安信安服团队、威胁情报中心、安全监测与响应中心、技术研究院、行业安全研究中心、补天漏洞响应平台及虎符智库、工业控制系统安全国家地方联合工程实验室，同时发布了7份网络安全2020年度研究报告，多达20万字的重磅信息披露，呈现独家观点及安全态势解析。

其中包括《2020中国实战化白帽能力白皮书》、《工业互联网安全发展与实践分析报告》、《2020年度漏洞态势观察报告》、《2020年网络安全应急响应分析报告》、《2020网络安全投融资趋势报告》、《全球高级持续性威胁（APT）活动2020年报告》六大细分领域专项报告，以及预测网络安全发展态势的《2021安全前瞻报告》。

《2021安全前瞻报告》显示：2020年数据泄露事件总量达到历史新高，Risk Based Security的报告显示，2020年公开披露的全球数据泄露数量猛增141%，达到370亿条，为2019年泄露数据量的2.4倍。

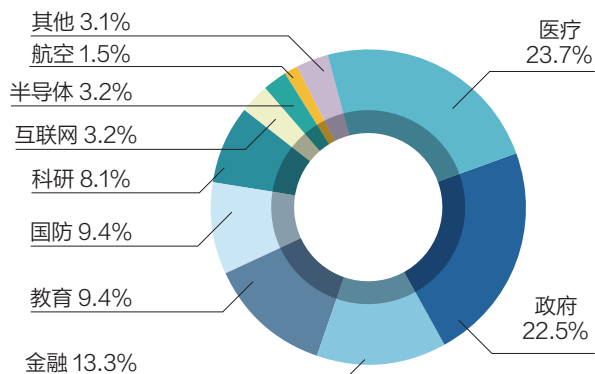
每年泄露数据量（亿）



曝光的信息系统安全漏洞也大幅增加：2020年奇安信CERT监测到漏洞信息77408条，较2019年新增3381条，其中较严重的影响或攻击成本较低的高危漏洞约占46%；勒索软件依然是主要的安全威胁，其中政府部门和医疗卫生行业遭受的网络威胁最多；与此同时，全球针对医疗行业攻击的APT事件增幅达117%，针对我国的APT攻击事件，医疗行业亦是“重点目标”，占比达23.7%。

全球范围来看，各国间的网络攻击行动日趋频繁化和白热化，聚焦窃密的同时，对关键基础设施的攻击激增，

2020年高级威胁事件涉及行业分布情况



意图造成社会混乱和持久破坏，供应链成为攻击组织的重要突破口；疫情推动数字化变革加速的同时，也对网络安全提出更高要求：远程办公突破了传统网络边界，也让黑客看到可乘之机，疫情期间个人信息泄露事件频发，也让隐私合规问题受到重视。

2021年，新冠疫情的影响仍将持续，面对更加不确定的未来，安全威胁是最确定的风险。可以预见，在2021年国家网络攻击组织将更具攻击性，影响和风险越来越大，勒索攻击的黑产模式将走向成熟，收益不菲的远程攻击将更加受黑客“青睐”。面对这样的网络安全环境，企业面临更高的隐私保护压力，实战攻防演习将成为政企用户实战化安全能力建设的重要手段，而基于安全内生理念的新一代网络安全框架将成为实现弹性网络的重要途径。

从全球漏洞态势，到应急响应分析，再到白帽人才能力，每一份报告中的案例和分析都明确表达了：网络安全没有灵丹妙药，任何放松警惕的行为将会带来不可承受的风险和责任。

在加快推进新型基础设施建设的“十四五”期间，奇安信作为网安行业领军企业，希望可以帮助政府、企业用户实现“规划快一步”、“发现快一步”、“攻防快一步”，筑牢安全底板，守好安全第一线，掌握安全主动权，让安全少走弯路。安

2020: 疫情年份网安迎来大考 安全风险加速技术创新

2020年新冠疫情肆虐，危及全球人类生命，但疫情并未使网络攻击组织停下脚步。疫情年份，全球黑客迎来狂欢年。新冠疫情对各国医疗保障能力形成考验，严峻的安全态势则对网络安全防护带来年度“大考”。

2020年国际网络攻击行动日趋频繁化和白热化，网络攻击和军事冲突成为互补的工具，物理空间的攻击引发网络空间的报复，反之亦然。

间谍窃密依然是网络攻击行动主要目的，军政机构面临泄密风险。年底曝光的供应链攻击事件“可能是历史上最重大的网络间谍行动”，以窃取疫苗相关研究成果为目标的攻击事件也大幅增加。

对关键基础设施等关系国计民生领域实施攻击，意图造成社会混乱和持久破坏的活动出现激增。这是传统情报窃取之外，国家级黑客组织的重要目标。

全球远程办公需求激增，用户和市场规模呈爆发式增长，导致全球网络攻击激增。2020年上半年，网络攻击强度和严重程度均出现飙升。针对医疗和人道主义组织的攻击尤其明显。

攻防博弈失衡加剧，信息系统“千疮百孔”。攻击组织具备更加良好的攻击能力，与此形成对照，核心应用、网络设备和新技术的漏洞频发。近两年漏洞数量不断突破新的记录。

此外，疫情期间的个人信息泄露事件依然频发。APP侵犯个人隐私问题同样是社会热点。

疫情成数字化变革的催化剂，尤其是随着我国新基建的全面加速，5G、工业互联网等数字技术得到逐步部署，增加了新的安全风险。

风险加速安全技术创新

2020年严峻的网络安全风险，加速了安全技术产品的研发创新和实践落地，从远程办公催生的“零信任”热，到个人信息保护带来的隐私保护技术，再到新基建浪潮驱动的新一代防御体系——“内生安全框架”，2020年是技术创新加速向实践转化的一年。

1、疫情之下远程访问需求激增，零信任加速标准化

为了解决远程访问中的诸多安全问题，各大厂商纷纷推出了针对远程访问场景下的零信任身份安全解决方案，信任标准化工作也加速推进。

2、内生安全框架从顶层视角构建动态综合防御体系

内生安全框架构建了适应不同业务场景网络安全整体防御能力分析模型，可以帮助用户建成面向数字化时代的一体化安全体系。

3、自动化技术推动隐私保护合规化

基于方滨兴院士提出的“数据不动程序动，数据可用不可见”的技术理念，奇安信数据安全子公司云安宝在国内率先推出更为实战落地的防水堡。防水堡在数据安全和隐私保护方面采用了创新性的数据沙箱和安全分离学习技术，可以有效实现对敏感数据的防护。

4、攻防博弈进化，第三代安全引擎破解0day漏洞难题

安全攻击防不胜防，0Day漏洞屡被曝出，现有安全体系亟需革新。2020年1月发布的第三代安全引擎“天狗”，颠覆了查漏洞打补丁的传统安全防护思路，即使不打补丁，也能有效抵御攻击。

5、实战攻防演习推动产品技术创新大量涌现

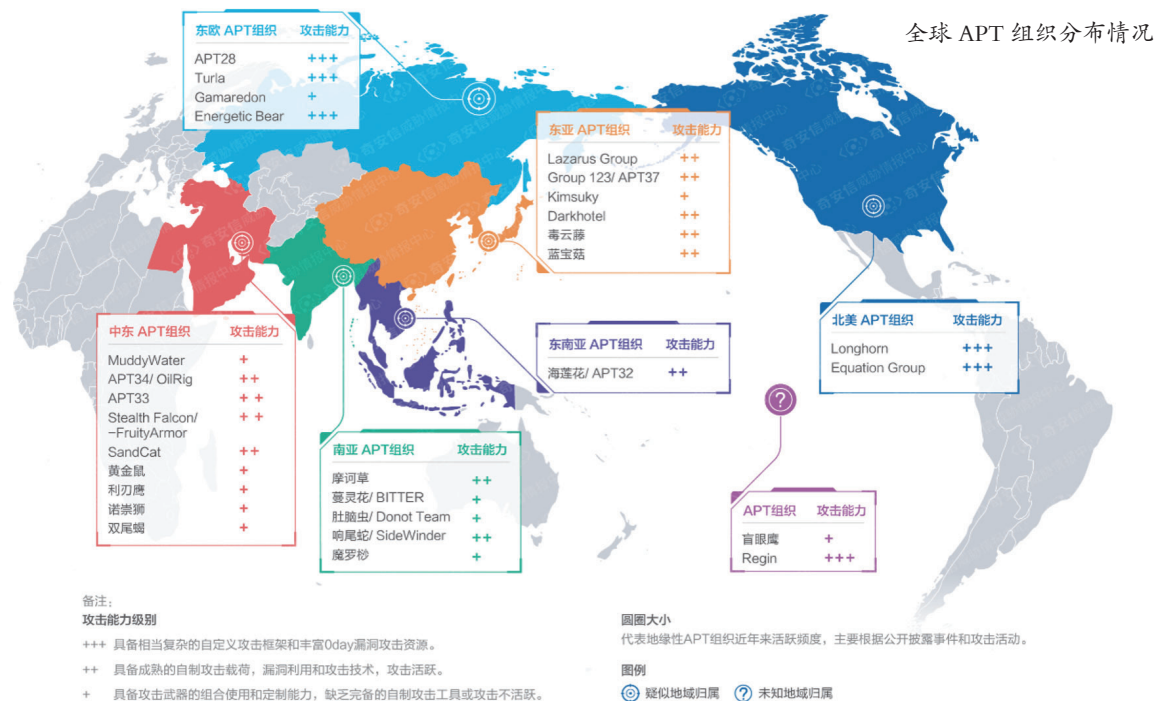
常态化的实战攻防演习成为了一种重要手段，推动大量网络安全产品技术的创新与落地实践，如漏洞管理、欺骗检测、安全编排自动化与响应（SOAR）、扩展检测与响应（XDR）等。

6、SOC/SIEM建设强化实战化能力

实战化能力建设成为安全运营平台SOC/SIEM设备重点发展方向。奇安信发布了新版态势感知与安全运营平台NGSOC、启明星辰推出泰合智能运营系统TSOC皆属此类。

7、政企机构加速上云，云原生安全重构云上安全防护体系

为了确保云上的安全防护，云原生安全作为新兴的安全理念在2020年成为热点。



APT 攻击：疫情之下愈演愈烈

2020 年，奇安信威胁情报中心收录了高级威胁类公开报告共 642 篇，涉及了 151 个命名的攻击组织或攻击行动，其中，提及率最高也是 2020 年最为活跃的几个 APT 组织分别是：Lazarus：10.3%，Kimsuky：7.8%，海莲花：5.4%，Darkhotel：4.8%，曼灵花：3.2%。

其中，医疗卫生行业史上首次超过政府、金融、国防、能源、电信等领域，成为全球 APT 活动关注的首要目标。全球 23.7% 的 APT 活动事件与医疗卫生行业相关。针对疾控与防疫机构、病毒研究机构、疫苗研发机构和其他相关的医学研究机构的高级威胁活动持续不断。

在漏洞利用方面，Oday 在野利用在 2020 年持续高发。攻击者选用的漏洞目标逐渐从 Windows 下的原生浏览器，向 Chrome、Firefox 等用户量更大的浏览器转移，甚至可用“Chrome 漏洞利用年”来总结 2020 年 APT 攻击的漏洞利用情况。

奇安信威胁情报中心发现，全球 APT 活动呈现出三大特点：

第一，疫情热点信息成 APT 活动常用诱饵，根据奇安信威胁情报中心的监测，2020 年上半年，就已经出现

了大量以各类疫情热点信息为关键词的诱饵文件，而到了 2020 年下半年以后，逐步成为了全球高级持续性威胁的攻击的普遍趋势。

第二，供应链和远程办公成为攻击切入点，从某种程度上说，属于攻击者发动的“降维打击”，往往使防守方束手无策。2020 年，供应链攻击已经成为全球 APT 活动的流行新趋势，例如 SolarWinds 事件就属于典型的供应链攻击。另一方面，新冠疫情在全球范围的蔓延，导致很多公司和机构采用了远程办公的方式，为攻击者提供重要的入口。

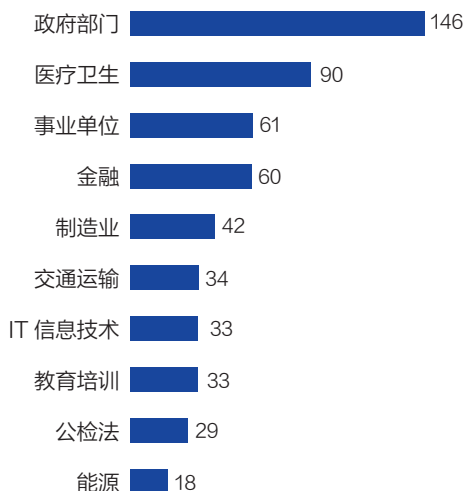
第三，定向勒索威胁成为 APT 活动新趋势，早在一两年前，定向勒索威胁的事件就已经偶有发生，2020 年以后，定向勒索攻击已经逐渐转变为一种新的流行趋势，攻击频率就一直处于持续平稳增长态势。

奇安信威胁情报中心预测，在 2021 年，APT 活动将呈现出如下六个趋势：疫苗及相关产业将会遭到持续攻击；针对中国的 APT 行动将持续加剧；远程办公的各个环节都将遭受 APT 攻击；地区冲突将引爆更激烈的网络战；网络武器库的泄露或将常态化；APT 组织可能组建基于 5G 与 IPv6 技术的物联网僵尸网络。安

应急响应： 政府、医疗卫生和事业单位是主要攻击目标

2020年，奇安信集团安服团队共接到应急服务需求660起，最多的行业TOP3分别为：政府部门行业（146起）、医疗卫生行业（90起）以及事业单位（61起），事件处置数分别占应急处置所有行业的22.1%、13.6%、9.2%。由此可见，政府部门、医疗卫生行业和事业单位的业务专网是2020年攻击者攻击的主要目标。

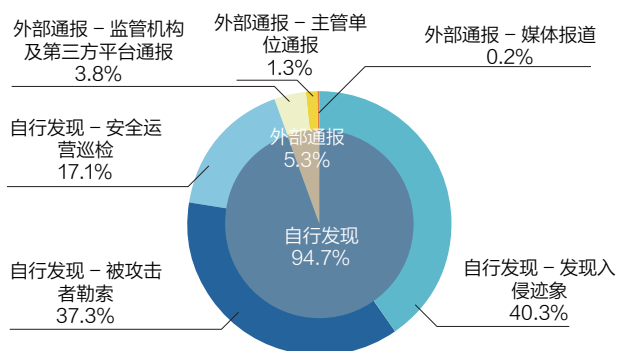
大中型政企机构应急响应行业分布 TOP10



在所有参与处置的网络安全应急响应事件中，由行业单位自行发现的安全攻击事件占94.7%，其中被攻击者勒索后发现的攻击占37.3%，另有5.3%的安全攻击事件政府机构和企业是在得到了监管机构及第三方平台的通报后，才得知自己已被攻击。

但值得关注的是，仍有77.6%的企业是在已经发生重大安全事故后才寻求应急响应的。能够通过自主巡检在重大事件发生之前及时组织的机构占比仅为17.3%。这说明，国内政企机构的日常安全运营建设水平仍有待大幅提高。特别地，有37.3%的机构是在被勒索后才寻

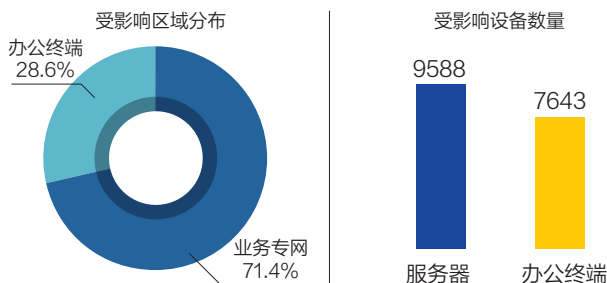
政府机构、大中型企业应急攻击事件发现分析



求应急响应，但此时补救往往为时已晚。

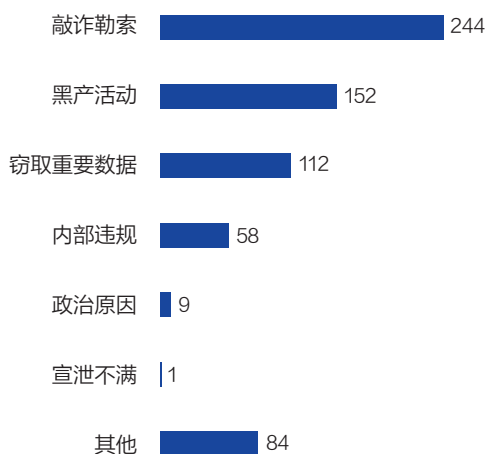
2020年应急响应事件的影响范围主要集中在业务专网，占比71.4%；其次为办公终端，占比28.6%。根据受影响区域分布对受影响设备数量进行了统计，全年失陷的设备中，9588台服务器受到影响，7643台办公终端被攻陷，如下图所示。从影响范围和受影响设备数量可以看出，大中型政企机构的业务专网、服务器为攻击者攻击的主要攻击目标。

大中型政企机构遭受攻击影响范围分布



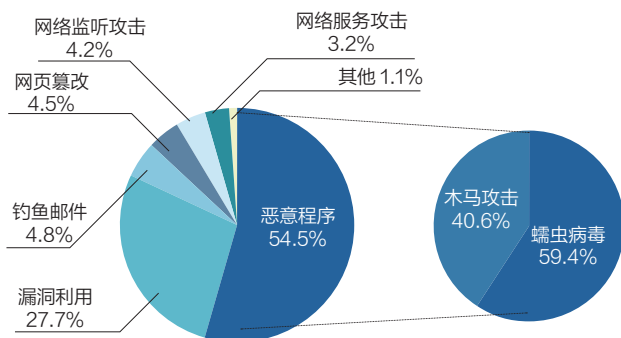
从攻击意图来看，攻击者主要为敲诈勒索、黑产活动、窃取重要数据和内部违规操作。

攻击者针对大中型政企机构的攻击意图排行



从攻击事件来看，2020 年全年大中型政企机构安全事件攻击类型，排名前三的类型分别是：恶意程序，占比 54.5%；漏洞利用，占比 27.7%；钓鱼邮件，占比 4.8%。其中，弱口令、永恒之蓝漏洞仍是大中型政企机构被攻陷的重要原因。

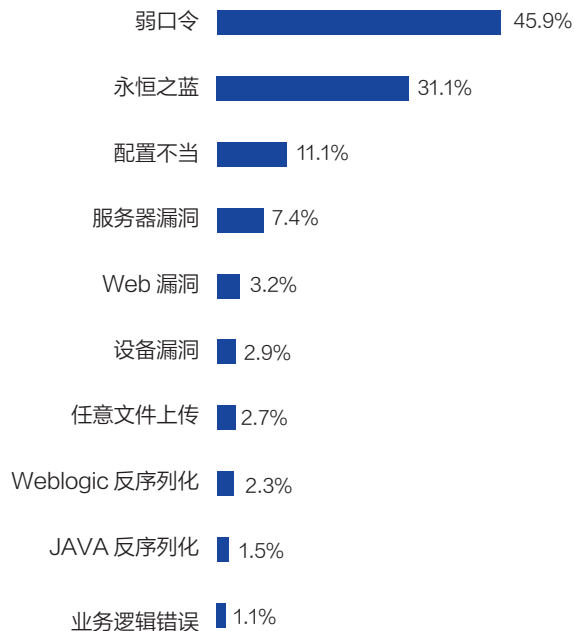
大中型政企机构遭受攻击类型统计分析



2020 年全年未发现大面积攻击事件，每月应急次数趋于平稳，说明行业专用网络或特殊网络的安全建设有明显进步。持续进行的实战攻防演习活动也是提升整个行业网络安全水平的重要原因。事实上，在过去几年间，每年都会发生数起甚至数十起大规模的网络安全事件引发的应急响应。受同一攻击者或同一病毒攻击的机构少则数家，多则数十家。这往往是由于相关企业通过某些专用或特殊网络相连，但对专网或特殊网络防护不足而引发的。

另外，奇安信安服团队认为，员工安全意识培养迫在眉睫。公网泄露敏感信息、高危端口外连、弱口令等由于安全意识淡薄而引发的内网服务器受感染导致勒索病毒蔓延、数据泄露甚至是服务器失陷事件比比皆是。安

大中型政企机构遭受攻击常见漏洞利用方式 TOP10



漏洞态势： 漏洞情报成政企安全防护重要一环

2020年，业界共提交了 CVE 漏洞 1 万 3 千余个；2020 年，国家信息安全漏洞共享平台 CNVD 收录的漏洞总数较 2019 年同比增长 24.23%。

面对如此庞大的漏洞数量，对于政企客户的网络安全防护而言，没有一劳永逸的解决方案，在攻防交替的博弈中，率先掌握漏洞情报的一方，往往更加容易占据优势地位。

1 月 20 日，由奇安信安全监测与响应中心（奇安信 CERT）、奇安信红雨滴高级威胁研究团队（天眼实验室）、奇安信技术研究院联合发布了《2020 年度漏洞态势观察报告》，报告从漏洞视角出发，梳理全年漏洞数据、分享漏洞研究成果、总结漏洞监测与响应方法论，并以此展望安全漏洞发展趋势。

2020 年度漏洞态势分析

2020 年，奇安信 CERT 共监测到漏洞信息 83692 条，经过 NOX 安全监测平台筛选后，其中 750 条漏洞信息达到奇安信 CERT 的处置标准并进行初步研判。

其中低危漏洞占比 24%，此类漏洞利用较为复杂或

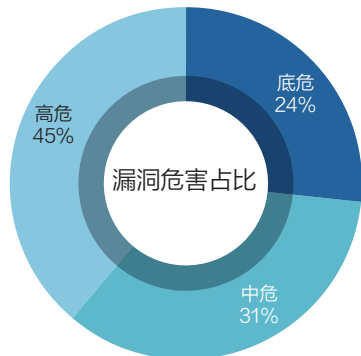
对可用性、机密性、完整性造成的影响较低；中危漏洞占比 31%，此类漏洞产生的影响介于高危漏洞与低危漏洞之间，可能需要一些复杂的配置或对漏洞成功利用的要求较高；高危漏洞占比 45%，此类漏洞极大可能造成较严重的影响或攻击成本较低。

漏洞情报成政企客户网络安全防护重要一环

面对井喷式的漏洞情报增长，奇安信 CERT 对漏洞情报进行监测与响应，从第一篇风险通告发布至今，奇安信 CERT 已经持续为企业提供免费高质量漏洞情报达 5 年之久。通过 5 年的探索，奇安信 CERT 已经建立起了有效的漏洞响应机制，并将其流程化、系统化。

近几年随着网络安全上升为国家战略，网络安全建设已经成为重中之重，每当互联网上有新的漏洞情报被暴露出时，各家单位都如临大敌，严阵以待，传统手段，都是通过网络安全公司对外发出的情报来获知，然后再升级系统、打补丁、做防御等。这种方式也逐渐显现出一些弊端，比如收到的漏洞通告，并不是自己所关注的；或者是通过邮箱方式，无法及时查看；亦或是收到的漏洞情报信息不全，无法判断如何处理。

为此，奇安信 CERT 发布的 NOX 安全监测平台向企业级用户推出了漏洞情报精准订阅功能，通过在 NOX 平台注册或升级为企业用户，可以通过订阅功能，获取你所关注的漏洞情报。在 NOX 漏洞情报订阅中，你可以根据自身的维护的资产范围，去订阅关联的漏洞情报，同时支持多种维度的订阅逻辑，比如你可以按照漏洞危害等级，漏洞类型，漏洞造成后果，漏洞的影响范围等众多维度进行订阅。漏洞情报已经成为政企客户网络安全防护重要一环。安

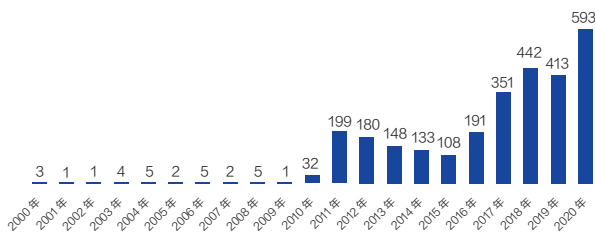


工业互联网： 漏洞数量陡然增长 安全投入明显不足

根据工业控制系统安全国家地方联合工程实验室与奇安信行业安全研究中心联合发布的《2020 工业互联网安全发展与实践分析报告》，2020 年，工业互联网安全漏洞持续高发，截止到 2020 年 12 月，CNVD 收录的与工业控制系统相关的漏洞高达 2955 个，2020 年新增的工业控制系统漏洞数量达到 593 个，较 2019 年增长了 43.6%。工业控制系统漏洞数据再创历史新高，安全漏洞数量快速增长，整体形势严峻。

2000-2020 年 CNVD 工控新增漏洞年度分布如下所示：

CNVD 历年收录工控系统漏洞数量分布



在 2020 年，CVE、NVD、中国国家信息安全漏洞共享平台（CNVD）及国家信息安全漏洞库（CNNVD）四大漏洞平台收录的工业系统安全漏洞信息共达 804 条。这些工业系统漏洞的成因多样化特征明显，技术类型多达 30 种以上。

在四大漏洞平台收录的工业系统漏洞中，高危漏洞占比 56.6%，中危漏洞占比为 35.8%，中高危漏洞占比高达 92.4%，具体分布如（右图）：

在威胁侧而言，勒索病毒仍然是 2020 年全球工业企业面临的重大挑战，这些安全事件均不同程度地造成了工业企业的生产异常，甚至停工停产。

面对严峻的安全形势，国内工业企业在工业互联网

安全方面的投入总体规模仍然较小，年投入超过 100 万元的企业不足三成。超过三成的企业认为，本单位的工业互联网安全建设水平仅为初级甚至裸奔。

仅有 40.9% 的受调研企业表示，未来两年在工业互联网安全方面的投入会有明显增加；另有 40.3% 的企业表示可能稍有增加；15.5% 的企业表示，没有明显变化。

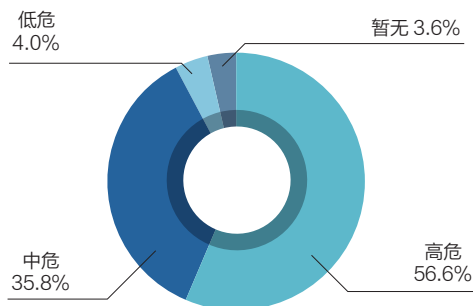
调研显示，阻碍当前国内工业互联网安全投资建设的三大因素分别是：看不到收效、缺少预算和担心影响正常生产。同时，安全人才匮乏是近半数工业企业安全建设过程中的最大痛点。

在选择供应商方面，综合能力强的安全大厂商在工业互联网安全市场竞争中优势明显。半数以上的工业企业倾向于通过与安全厂商深度合作加强自身安全能力。

在服务方面，“工业互联网安全托管”服务或将成为主流。其中，最受欢迎的是远程安全运维服务，其次是定期上门服务，再次是驻厂服务。

报告建议，工业企业应从以下几个方面进一步做好工业互联网安全工作：设置网络分段，做好安全隔离；缩小网络攻击面，最大限度减少网络攻击风险；采用身份认证、安全加密的方式进行远程访问；加强行业合作，选择具有内生安全框架的工业互联网安全特色产品等。[安](#)

2020 年工控系统新增漏洞危险等级分布



白帽人才： 首份实战化能力图谱发布，高阶能力尚十分欠缺

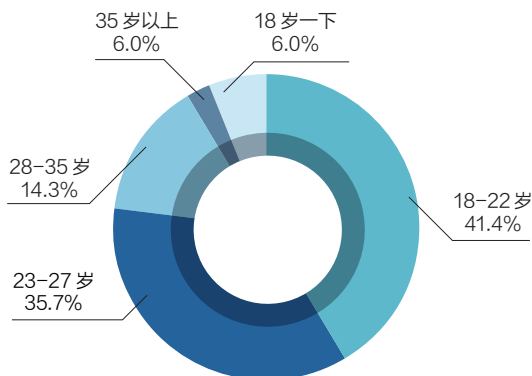


由补天漏洞响应平台联合奇安信安服团队、奇安信行业安全研究中心，发布了业内首份《2020 中国实战化白帽人才能力白皮书》，首次提出了实战化白帽人才能力的概念，绘制了首份实战化白帽人才能力图谱，为实战化白帽人才的系统性培养提供重要的科学参考依据。

白帽人才年轻化

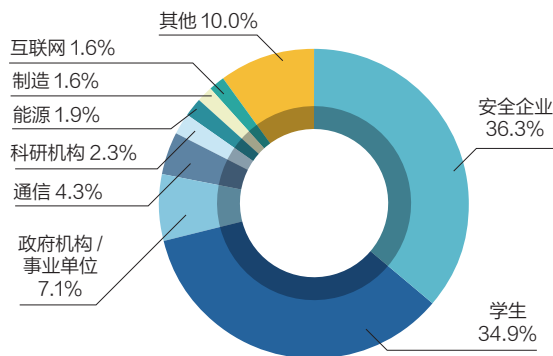
数据显示，在接受调查的具备实战攻防经验的 645 名白帽中，近 8 成年纪在 27 岁及以下，其中 23-27 岁的白帽占 35.7%，18-22 岁及约占四成（41.4%），甚至还有 6% 尚未成年；学历方面，本科及以下学历超过 9 成。其中甚至不乏中学在读的白帽人才。由此可见，年轻是白帽人才的主要关键词，在年龄上符合人们对于“现男友”的预期。

实战白化白帽人才年龄分布



在接受调研的白帽子中，36.3% 的白帽子来自于安全企业，34.9% 的白帽子为学生，7.1% 的白帽子来自政府机构事业单位。这主要由于白帽子所需技能及时间积累，人员更多集中在专业对口的安全企业从业者或精力充沛、时间充裕的学生党。

实战白化白帽人才行业分布



首份实战化白帽人才能力图谱发布 高阶能力尚十分欠缺

为提升国内白帽子群体的整体能力水平，适应日益重要的攻防演习实战需求，白皮书结合 1900 余个目标系

统的攻防实战经验，首次系统性地总结了“实战化白帽子能力需求图谱”。

实战化白帽子能力图谱



该能力图谱综合考虑了掌握技能的难易程度、市场人才的稀缺程度、以及实战化能力的有效性这三方面因素，将白帽子的实战化能力从低到高依次分为基础能力、进阶能力和高阶能力，并详细拆分为3个级别、14大类、85项具体技能。白皮书中对这14大类、85项基本技能均提供了详解说明。将对安全行业的实战化白帽子人才发展及能力培养，提供重要参考和依据。

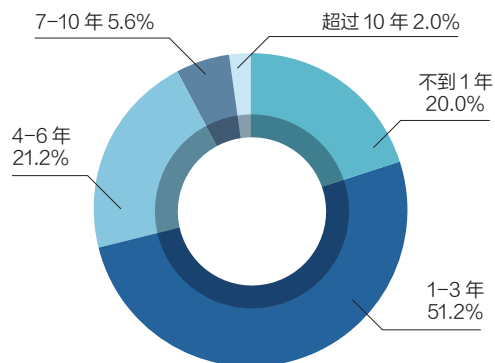
调研显示，目前国内白帽子人群所掌握的实战化攻防能力，仍主要集中在基础能力方面；而具备高阶能力的白帽人才十分稀缺，特别是不同平台程序的分析能力、在系统层漏洞的挖掘与利用，以及相应的PoC或EXP的编写等方面人才极为稀缺。

这或许与绝大多数白帽人才从业时间较短有关。数据显示，超七成受访人员从业时间不超过3年，其中入行时间不到一年的白帽子占比达到了20%。

全网实战攻防演练推广 实战化白帽考验全面能力

近年来，随着网络安全实战攻防演习工作的持续深

实战化白帽子人才从业时长



入开展，对于白帽子在实战对抗环境、实际业务环境中的能力提出了更高要求。

在这种背景下，白皮书对“实战化白帽子能力”的定义为：在政企机构实际运行的业务系统、生产系统上进行的实战攻防演习过程中，作为攻击方的白帽子所需要具备各种攻防能力的集合。

与传统的挖洞型白帽人才能力要求不同，在实战化攻击过程中，白帽人员不仅需要针对真实的业务系统或生产设备，发现高级安全漏洞，还要对机构内部的IT架构、运行管理机制进行有效分析，找到路径，实现有效攻击。期间允许使用社会工程学方法，以人为突破口进行攻击。与此同时，面对防守方的反制防守和攻击溯源，白帽人员还需要掌握一定的身份隐藏技能，通过多人协作，共同完成整套动态实战攻防。这就对白帽子能力提出了“可攻、可防、能潜、能藏”的综合能力要求，成为“一专多强”的T字形人才。

不过，在接受本次调研的645名白帽子中，尽管有约74.0%的白帽子具有组队参加有关部门组织的实战攻防演习活动的经验，但仅有19.4%的白帽子表示自己能够胜任团队协作中的任意角色。因此，这还要全社会共同努力，加大对白帽人才的挖掘和培养力度。来自腾讯、字节跳动、京东等厂商安全团队负责，以及安全团队创始人，对白皮书对于实战化白帽子人才培养的指导意义表示肯定。安

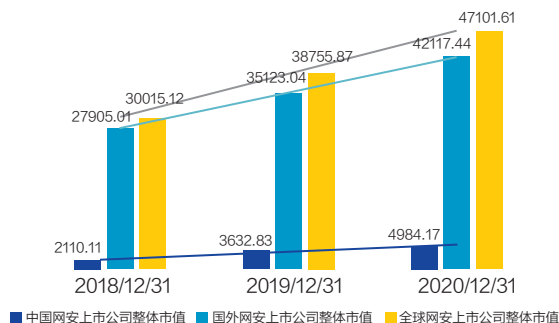
投融资： 云安全、应用安全、身份安全、数据安全成热门领域

受疫情影响，全球经济形势不容乐观，网络安全产业也受到了一定的波及，增速放缓。在这样的背景之下，网络安全产业的资本运作活动却没有受到过多影响，远程办公、数据合规、隐私保护、万物互联等新场景的涌现，为网络安全创业和资本市场带来了新鲜活力。

从投融资市场的表现来看，包括 Insight Partners、红杉资本、Accel、Bessemer Venture Partners、Sequoia、Bain Capital 以及国内的奇安创投等多家投资机构，都有大手笔的资本运作。

在二级市场，根据公开数据统计，截至 2019 年 12 月 31 日，106 家上市公司的市值总和（下述简称为“整体市值”）达 38755.87 亿元人民币，同比增长 29.12%。截至 2020 年 12 月 31 日，整体市值达 47101.61 亿元人民币，同比增长 21.53%。

过去三年全球主要网安上市公司整体市值（亿元人民币）



图：网络安全上市公司市值变化情况

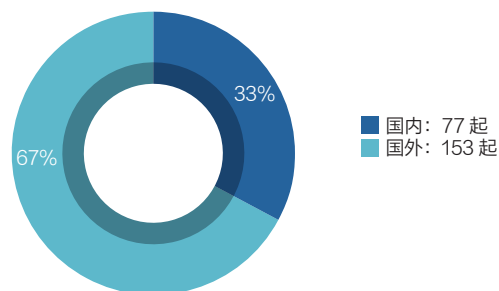
2020 年全球投融资整体情况

实际上自 2016 年以来，全球累计投资网络安全公司

标的数量在 10 家以上的投资机构就超过 15 家。仅 2020 年，网络安全投融资市场至少发生了 232 起融资并购额度相对较大的事件，其中国内 77 起，国外 153 起。

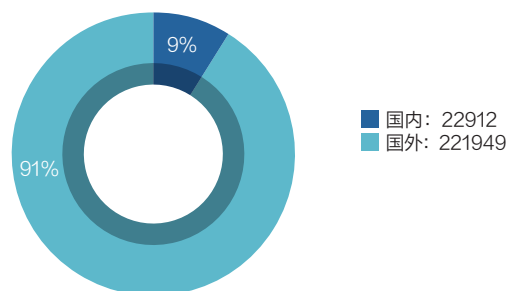
在资金规模方面，全球网络安全产业投融资及并购总金额约为 244.861 亿美元（根据已公开的财务信息统计，下同），其中国内的金额约为 22.912 亿美元，国外约为 221.949 亿美元（美元人民币汇率取 1 美元 ≈ 6.5 元人民币），占比分别为 9% 和 91%。

投融资事件数量



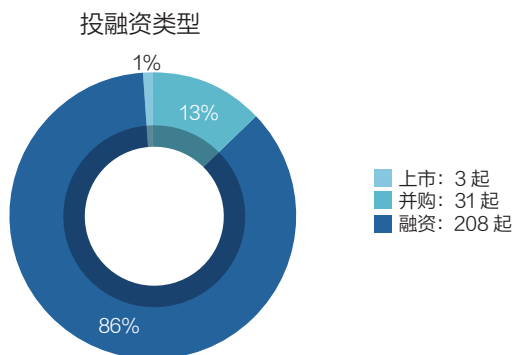
图：国内外投融资事件数量分布情况，公开资料整理

投融资额度 (单位：亿美元)



图：国内外投融资额度分布情况，公开资料整理

与此同时，根据投融资类型对本文收录的事件进行划分，上市事件有 3 起，并购事件 31 起，融资事件 208 起。进一步从细分领域来看，较为热门的主要包括云安全、应用安全、身份安全、检测与响应、数据安全、安全服务、工业安全和业务安全等。



图：投融资类型分布情况，公开资料整理

2020 年投融资整体特点

第一，疫情催生的新场景带动了新一轮网络安全风投热潮。远程办公需求的激增，是疫情给企业机构带来的最大变化之一，因此针对常态化远程办公或者远程访问场景的安全防护企业受到了资本圈的重点关注。2020 年获得融资的企业当中，做身份认证及管理的企业占据了绝大多数，其中多因子认证、基于用户实体行为分析的身份认证已经成为主流。

值得关注的是，“零信任”的架构体系已经深入网络安全管理的各个环节，开始进入规范化、落地化发展阶段。继 NIST 推出《零信任架构》标准之后，

由奇安信牵头的零信任国家标准也正式启动，并在 2020 年已经出现了相对较为细分的、可落地的解决方案。

第二，头部 IT 巨头的并购脚步逐步放缓。回顾过去两年，IT 巨头们的资本动作都十分活跃，然而 2020 年行业巨头们似乎“安静”不少。2020 年国际上出现高达数十亿美金的并购事件，基本都出自股权私募公司的手笔，并不涉及过多的产品或者业务整合。

第三，安全合规使得数据安全和个人隐私保护成为香饽饽。这源于疫情引发了公众对于个人隐私保护方面的担忧。与此同时，伴随着 CCPA 的正式实施以及国内的《数据安全法》、《个人信息保护法》等法规草案的亮相，安全合规将大幅提升政企机构对于数据安全和个人隐私保护领域需求。

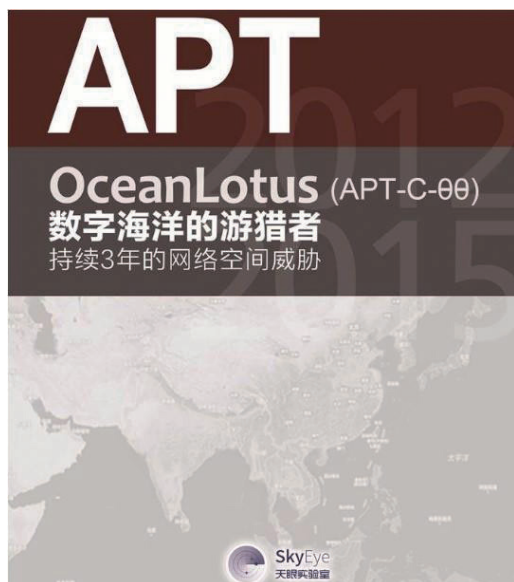
第四，检测与响应领域热潮不退。不论是 2019 年还是 2020 年，从资本交易事件数量可以看到，检测和响应都被当做企业的重点战略，这主要是因为过去几年安全事件频发，行业希望寻找某些基于端点、基于网络或者基于用户的方法，去获得持续的高级威胁检测、调查和快速响应的能力。未来的一段时间内，检测和响应依旧是投资机构追捧的热点。

第五，中国网络安全企业或步入千亿市值时代。2020 年，奇安信正式登陆科创板。过去，网络安全头部公司的市值均在二三百亿上下，尽管一些“安全”公司的市值突破千亿元大关，但其网络安全收入在总收入的占比不高（最高的在 60% 左右）。奇安信登陆科创板后的第二个交易日，市值便一度超过 900 亿元，随着网络安全市场规模的快速提升，以及资本市场对于行业形势的看好，奇安信市值突破千亿元是大概率事件。安

不咬钩也被钓鱼？ 当黑客团伙盯上了供应链， 千里之堤竟毁于一旦

● 公关部 魏开元
根据奇安信威胁情报中心真实 APT 处置事件改编

2015 年，天眼实验室（奇安信威胁情报中心前身）首次披露了一起针对中国的国家级黑客攻击细节，这也是我国披露的第一起 APT 团伙攻击事件。因为其攻击目标多为我国海事机构、海域建设、航运企业等与“海”相关的重要领域，安全分析师为这个组织取了一个相当好听的名字——海莲花。



数年来，安全工程师们和海莲花进行了无数轮的较量，并成功挫败了多次攻击。然而，在 2020 年，海莲花依然猖獗并屡次得手，其变幻莫测的攻击手法，让政企机构防不胜防。

复工复产，一个新的阴谋正在酝酿

2020 年 2 月 9 日元宵节刚过，复工复产的大幕已经悄然拉开。

出于疫情防控需要，软件外包公司员工上门服务基本上是不被允许的。为了保证项目开发的进度，一些机构特地为他们的开放了 VPN 服务，允许外包公司员工远程访问内网代码服务器。

达七正是众多外包公司员工中的普通一位，他所在的公司正在为部委甲的 OA（协同办公软件）进行定制化开发。

到公司后，达七从双肩包里掏出了自己的电脑，熟练地登上了 VPN，准备开始新一天的工作。不过在每天开始工作之前，达七会检查一篇自己的收件箱，看看是否有漏掉的重要邮件。

果然，“一封来自客户的邮件”吸引了达七的注意。正文部分空白，只有一个 word 附件，标题为《关于推进有序复工复产的通知》。

出于好奇，达七打开了附件。粗略一览，文档内容大多跟自己没有关系。达七呵呵一笑，“谁这么无聊把内部邮件转给我了？”

随手关掉邮箱，达七一天的工作开始了，口中还默念着一个流传已久的梗：PHP 是世界上最好的语言。可他怎么也没想到，一次针对部委甲的网络渗透，就从这封邮件这儿开始了。

恰在此时，位于东南亚的的一台服务器上，收到了海莲花组织特种木马传回来的信息。一场精心策划的

APT 攻击已经成功了第一步。

线索扑朔迷离，竟然难住了安全老鸟？

若干天后，转眼又入冬。刚吃过午饭的 DP 半躺在办公椅上打着盹，他是奇安信威胁情报中心的主力分析师，和海莲花组织已经交手过太多次。

突然，负责人 Star 的一通电话让 DP 睡意全无。客户侧部署的奇安信天眼高级威胁检测系统产生告警，疑似发现 APT 攻击，需要 DP 到客户现场配合安全服务团队进行排查。

这是个苦差事。

由于部委甲的特殊性，因此对来访人员管制措施较为严格。DP 紧了紧外套的领口，时不时还跺着脚，排队等待进入客户现场。

天气似乎显得格外寒冷。

来到办公区后，DP 根据告警日志第一时间找到了中招的电脑终端（失陷终端）。在将该终端的 DNS 解析记录、域名访问信息与奇安信威胁情报比对后，DP 心里已有了谱：“呵，又是海莲花，你就不能换个服务器地址么？”

经验告诉他，钓鱼邮件是海莲花等 APT 组织最常用

的攻击手法之一，简单直接。如果黑客是通过钓鱼邮件渗透进来的，那么一定会在邮件服务器里，发现一些蛛丝马迹，从而找出所有失陷终端，并还原整个攻击轨迹。

一下午的时间很快就过去了，DP 双眉紧锁。邮件拦截记录显示，带毒邮件或者其他垃圾邮件都被拦截了，黑客很难用这种方式攻进来。

“不是通过钓鱼邮件？”DP 揉了揉有些发酸的眼睛，转过头问客户到，“咱们这儿应该不让用自己的电脑吧。”

“嗯，不让。我们也装了终端安全管理的软件，对接入内网的电脑、手机，都有非常严格的管控。”该部委的安全负责人说到，“今天先到这儿吧，快下班了，按规定我得把你们送出去。”

“行，那我先回去，中毒的那台电脑别用了。”

蹲点摸排，终于锁定 23 台失陷主机

离开客户现场之后，DP 并没有立即回家，而是就近订了一家快捷酒店住下，想着明天早点过去。他知道，接下来几天就要交代在这里了，自己住得太远不太方便。

房间里，DP 简单向 Star 汇报了一下今天下午排查的基本情况。Star 倒是没有觉得奇怪：“嗯，没关系。



这些域名均为海莲花所使用的 C2 服务器域名和 IP 地址。

像他们这种安全防护做的比较完善的单位，钓鱼邮件已经很难了，你注意排查一下网络边界设备，比如防火墙、VPN 这些，我估计海莲花这次是通过边界渗透进来的。这几天你就在那盯着，有困难后方随时支援。”

第二天一大早，DP 就出门了。“今天这么早啊。”客户寒暄了一句。

“嗯，这不想早点搞定问题么。”DP 说，“对了，你们最近远程办公么？”

“最近应该没有，你也知道我们单位比较特殊，都是要求在办公区的。不过早些时候我们给一家外包公司开放过 VPN 端口开发 OA，那时候不是不让上门么，我们又要赶项目进度。你怀疑？”

“嗯，昨天晚上我们仔细复盘了一下，有这个可能。前段时间 VPN 曝出很多漏洞，也出现了一些漏洞利用的事件。”

正说着话，DP 似乎发现了一丝端倪。漏洞扫描工具显示，VPN 存在一个远程绕过漏洞，允许攻击者在未经授权的情况下访问内网。顺着这条线，DP 果然找到了来自外包公司的异常访问，木马应该是从外包公司带进来的。

DP 随即通过流量分析工具和恶意文件分析工具，分别针对异常流量和可疑文件进行了特征提取，得到了非常完整的失陷威胁情报（IOC）信息，包括文件 MD5 和与木马通信的 C2（命令与控制）服务器域名、IP 地址等。

“接下来应该就容易了，只需要排查哪些终端与这些地址发生了连接就行。”完成了最关键的一步，DP 终于松了一口气。经过两天的蹲点排查，日志分析结果显示，与这些域名发生通信的共有 23 台终端。

还原攻击过程：国内首次基于 VPN 漏洞的供应链攻击

从客户那里回来后，DP 向威胁情报团队复盘了整个攻击事件。

事实上，海莲花组织并非一开始就尝试这种渗透方法，而是走他们的老路子，钓鱼邮件攻击。只不过后来

他们发现，发出去的钓鱼邮件如同泥牛入海，没什么太大效果，因此黑客绕了个弯，把目标放在了部委甲的上游供应商上。

外包公司的安全防护水平参差不齐，黑客也知道老太太捏柿子——挑软的欺负的道理。一封略加伪装的钓鱼邮件，便攻破了达七的电脑。

恰逢疫情爆发，远程办公需求猛增，很多机构不得不开放 VPN 端口，这就给了攻击者可乘之机，等于多了一个入口。有调查数据显示，疫情期间，VPN 使用率较平时提升了 30% 左右。

“可能平时的漏洞管理工作不够细致，这次海莲花利用远程绕过漏洞并不是 0day，而是一个 Nday。意思就是 VPN 厂商很早就公开披露过漏洞详情，并提供了补丁，但该部委并没有及时更新。”

正是这个不起眼的漏洞，让海莲花组织原本在达七电脑上植入的木马，放到了部委甲存储代码的服务器上，并以此获取了服务器的控制权。DP 说，这是奇安信威胁情报中心发现的国内首次基于 VPN 漏洞的供应链攻击。

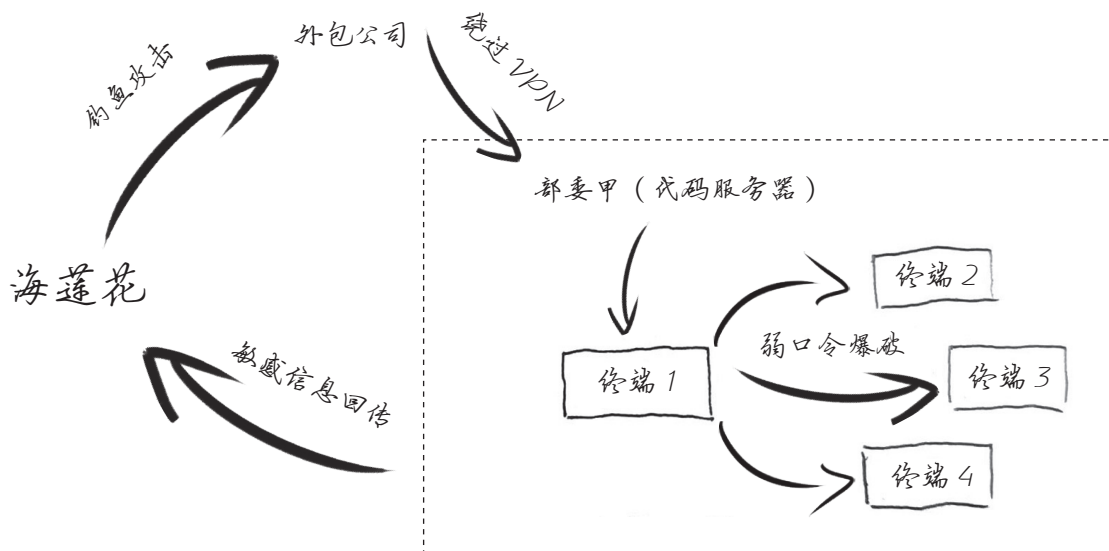
拿下服务器后，为了获取更多敏感信息，海莲花针对员工办公终端开始了渗透。

理论上，内部任意一台电脑都可能与服务器发生互联，所以海莲花可以向任意一台电脑下发他们的远程控制木马。但这一次，他们只选择了一台登录口令强度不高并且连接互联网的电脑作为目标。

为了对抗检测手段，海莲花组织做了很多工作。

第一项是免杀，通俗理解就是躲过杀毒软件的检测。海莲花组织一旦发现其下发的木马被杀毒软件干掉了，就会远程修改木马配置，直到杀毒软件检测不出来为止。DP 说，最多的时候海莲花组织曾做过 5 次修改。

第二项是与电脑的物理地址（MAC 地址）绑定。由于物理地址具有唯一性，因此在木马与其绑定后，便不能在其他电脑上运行。它有一个很重要的作用就是逃避沙箱（沙盒）检测。沙箱可以理解成一个虚拟电脑，把可以文件放在沙箱里运行，观察其行为、特征，从而判断文件到底是不是病毒。



由于海莲花植入的木马只能在绑定的电脑上运行，在沙箱里便不能运行了，因此普通的沙箱并不能得到检测结果。但经验丰富的DP耍了一个“小聪明”，把沙箱的MAC地址调整为和宿主电脑一样，对木马来了个“将计就计”。

第三项是持久化。为了防止木马文件意外丢失，海莲花组织将其木马模块与输入法进行绑定，从而保证开机自动运行，实现长久潜伏。

“海莲花这次内部横移是怎么做的？”有同事提问。

“还是老套路，基本上都是通过局域网里面的445、80这些没有关闭的高危端口，进行横向弱口令暴力破解。破解成功后，再次重复上面的三个动作。”DP回答。

当年，大名鼎鼎的永恒之蓝勒索病毒也是通过445端口在内网传播的。

后来，DP跟笔者聊起了这次攻击事件，他拿起了一张事先准备好的草图。拿起来一看，此次攻击的轨迹一目了然。这种利用上游供应链完成攻击渗透的方式，业界喜欢它们叫做供应链攻击。

举例来说，不久前，奇安信披露的2020年度最严重APT攻击事件，即导致200多家全球重要机构受害的SolarWinds（太阳风）事件，就是典型的供应链攻击，

其幕后组织“金链熊”更是多达数百人。

海莲花的牌还没出完 猎人狐狸的游戏还在继续

“海莲花远不止采用这一种攻击方式。”DP说，“后来排查的时候，还发现了他们获取了杀毒软件后台的控制权。”说起来也巧了，海莲花组织在对部委甲进行端口扫描时，恰好发现了处在同一网段的杀毒软件，进而挖出两个0day漏洞，完成攻击。

当然，在安全厂商的围追堵截之下，海莲花的日子也不好过。单说奇安信威胁情报中心，每年都能抓住他们很多次。每抓住一次，就把他们使用的C2服务器域名、IP地址、木马文件配置等信息提取下来并生成威胁情报，下次他们如果再使用相同的IP地址发动网络攻击，就会直接被拦截了。再加上奇安信和友商之间的威胁情报共享机制，时间一长，他们手上的服务器被查的七七八八，不得不换新的服务器。

那么问题来了，下一次如果海莲花用全新的服务器，还能查出来么？

“你说第一次披露海莲花组织攻击的时候，是怎么发现的呢？”DP反问了一句。安

为区域基层医疗机构 构筑“积极防御”体系

——探秘网络安全运营的“江干模式”

走路十几分钟，头疼脑热就能治好；小病不用去大医院排队挂号，免去舟车劳顿之苦。近年来，基层医疗卫生改革深入开展，数字化水平大幅提升，给患者和医生都带来了极大便利。但随着医疗数据的开放共享，信息安全也面临新的挑战。

基层医疗机构数量众多，规模较小，地理位置分散，导致信息化和网络安全建设层次不齐，总体水平相对落后。不仅自身广泛存在着后门程序、僵尸网络、木马蠕虫、勒索病毒等安全问题，同时由于需要接入卫生专网，更给卫生专网和数据中心带来巨大安全隐患。

如何保障医疗数据信息安全，保护患者隐私，满足信息安全等级保护要求，确保医疗服务稳定开展？如何将网络安全防御框架“下沉”到医疗卫生体系末端，让基层医疗机构也具备事前防控的“积极防御”体系？如何保障医疗数据信息安全，保护患者隐私，满足信息安全等级保护要求，确保医疗服务稳定开展？面对这些问题，2020年1月开始，浙江省杭州市江干区卫生健康局携手国内领先的网络安全公司奇安信，以奇安信态势感知与安全运营平台（简称：NGSOC）为核心，建成全国首个覆盖社区卫生服务中心的网络安全运营样板，打造了让各地医疗卫生机构广泛借鉴的“江干模式”。

杀毒、重装、格式化 基层网络安全“三板斧”

“没有部署网络安全系统之前，社区卫生服务中心的电脑一遇到蓝屏死机、中毒卡慢，通常招数就是先杀毒，不行就重装系统，甚至格式化硬盘，然后数据恢复。”江干区卫生健康局信息中心负责人谈起几年前的基层信息化现状，依然是感慨万千。



江干区，隶属于浙江省杭州市，是杭州城市发展战略的轴心所在，也是杭州的交通枢纽中心，曾先后获评全国科技工作先进区、全国卫生先进城区、全国社区建设示范区、浙江省科技进步先进区等荣誉。江干区卫生健康局作为区医疗卫生健康管理职能部门，打造出了3个全国百强社区卫生服务中心，曾先后接待国务院医改办、国家卫健委基层卫生司、体改司、中国社区卫生协会、WHO 扩大免疫规划组、国家卫健委免疫规划督查组等行业专家的多次考察与调研。

习近平总书记曾多次强调，“没有网络安全就没有国家安全，没有信息化就没有现代化。”在与民生紧密相关的卫生系统中，随着信息化建设的普及，医共体建设的有序开展，卫生系统常遭遇的各类勒索病毒、木马等高级攻击手段也蔓延到了卫生体系的末端，直接威胁基层医疗机构业务平稳运行和卫生专网的安全。

江干区卫生健康局信息中心的负责人对此深有体会。

他总结了五个方面：

首先是各社区机构信息建设普遍规模小，网络安全关注度低，对卫生专网构成不可忽视的威胁。

其次是资源相对紧张，信息化先天建设方面存在缺陷，自身不具备建设网络安全监测的能力。

第三是一线医护人员比重高，网络安全意识薄弱，更易感染木马病毒。社区卫生服务中心的IT人员基本上只有一名，日常工作繁杂，身兼多职，无暇处理各种安全问题。

第四是地理位置较为分散，难以进行统一监管、安全赋能。江干区卫生健康局辖区内有8个街道社区卫生服务中心，以及卫生健康局机房数据中心、青山湖IDC机房数据中心，地理位置很远，安全管理难度很大。

最后是基层区域卫生专网数据中心亦需要相关专业的安全能力保障。由于数据中心承载了重要业务和敏感数据，一旦被攻击，导致业务停顿、数据泄密等，其损失不可估量。

“在部署NGSOC之前，街道社区卫生服务中心的网络安全停留在安装杀毒软件这样的被动防御层面。基本是各自为战、事后补救，非常被动。”江干区卫生健康局信息安全负责人鲁主任表示，“对于卫生系统专网的监管者和运营者来说，由于缺少指导和开展相关网络安全工作的工具和数据，无法对网络安全做到高效运营和深度管控，很容易让专网的重要业务和敏感数据，暴露于攻击者面前。”

安全分析、服务等优势明显 奇安信NGSOC脱颖而出

江干区卫生健康局始终对网络安全高度重视，2018年，当基层区域卫生信息化建设完成之后，几乎同期，整个系统就全线部署了奇安信天擎等安全产品。2019年开始，为了强化安全分析、威胁发现和管理能力，构建积极防御体系，态势感知和安全运营的建设部署被列上日程。

“几家厂商竞争非常激烈，经过几轮筛选，奇安信

走到了最后。”提起选择过程，鲁主任谈到，参与的几家厂商各有千秋，都有很强的实力。考虑到卫生健康局现状，主要考量参与厂商的两方面能力：首先是安全分析能力，其次是安全服务能力。

高性能无疑是安全分析能力的基础保障。当时，2家竞标厂商提供的是一体机的方案，1家提供了2台服务器的方案，而奇安信是唯一一家提供基于三台服务器高性能并发方案的厂商。

谈到这次项目实施，鲁主任回忆了当时的一个小插曲。

从2019年底招标确定下奇安信作为合作伙伴，到2020年初NGSOC等主要设备基本到位，和奇安信的合作非常顺利。即便中间受到春节和疫情因素影响，奇安信仍然在复工复产之后，第一时间进行上门部署。不过，当时却遇到过一次意外。

“三台服务器几次调试，同步总是不成功，延迟比较厉害。”奇安信项目工程师向卫生健康局信息中心反馈了部署中遇到的问题。

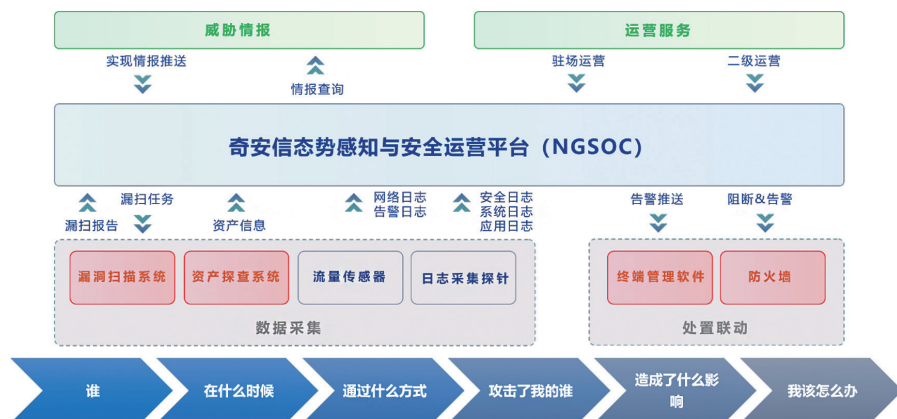
“所有业务都是正常的，应该不是网络的问题。”卫生健康局信息中心当时也感到很困惑，但第一反应并没有想到网络设备的因素。

三月初的杭州乍暖还寒，那几个晚上，奇安信工作人员经常干到深夜，一次次的调试，排查故障，寻找原因，甚至凌晨一两点才离开机房。

到3月10日，鲁主任感觉有些奇怪，于是带上网络技术人员，去现场反复排查网络设备，终于有了重大发现，找出了故障原因。

“原来，当时我们用的是某网络设备厂家型号较老的交换机，为了2台做堆叠，后来增加了两块万兆光板卡和两块电口板卡进行数据交换，当时从业务正常运行的层面，没发现异常。但在测试中发现，2块新的板卡，在数据同步的时候，未能达到千兆。所以当流量很大的时候就会出现延迟。”鲁主任表示。

当晚，信息中心就对网络设备进行了系统升级，之前数据同步延迟的问题彻底得到了解决。“之前我们都以为是NGSOC安装调试的问题，没往网络设备上想。现在想起来，奇安信人的敬业态度和认真负责，着实让



人钦佩。”

不仅如此，奇安信的专业服务和快速响应能力也让鲁主任记忆深刻。“网络安全的核心是人，再强大的产品，再聪明的机器，都需要人来运营，人来使用。奇安信提供了日常巡检服务、应急响应服务、重要时期安全保障服务，尤其是每月都有专业的NGSOC分析报告，对月度告警情况、僵尸蠕毒活动事件、安全处置建议等详尽分析。”

提前洞悉威胁 将安全风险化于无形

“我们为客户提供的不是单一产品，而是一套在防御、检测、响应、预测、持续监控分析周期内提供威胁发现和响应综合性一体化平台。”负责江干项目的奇安信浙江分区医疗销售总监蒋宝尧表示。

在威胁发现和感知方面，通过部署NGSOC，可提

前洞悉各种安全威胁，同时联动本地防火墙、终端安全管控系统以及云端的威胁情报数据，能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源，并为后期安全加固提供有效依据。

对于客户最关心的性能和

安全分析能力，一方面，奇安信信NGSOC具备千亿级数据

处理能力，可以大大提升安全分析和响应的速度和效率；另一方面，NGSOC基于国内首款分布式关联分析引擎Sabre，通过场景化检测规则、机器学习和关联分析进行多维度威胁研判，大幅降低了威胁检测的误报率和漏报率，其DGA域名检测准确率高达99.94%。

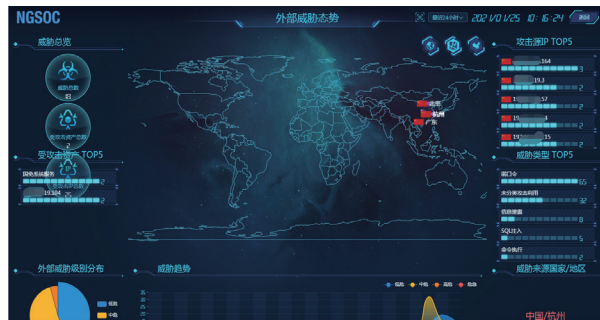
在边界防护方面，通过部署防火墙对整个网络形成分区分域，一方面对内外网出口及重要边界进行安全防护，另一方面可以更好的进行访问控制。

在联动方面，该项目形成“云管端”联合解决方案，将终端安全管控、控制中心、新一代防火墙“病毒云查杀”、云端反馈和NGSOC等实现无缝联动，提升告警和阻断效率。

而在服务方面，奇安信推出了专业运营服务，将人、数据、工具和流程，四个维度进行了有机的结合，彻底帮助卫健委下属部分机构客户解决产品不能用、不会用



业务资产外连态势



外部威胁态势



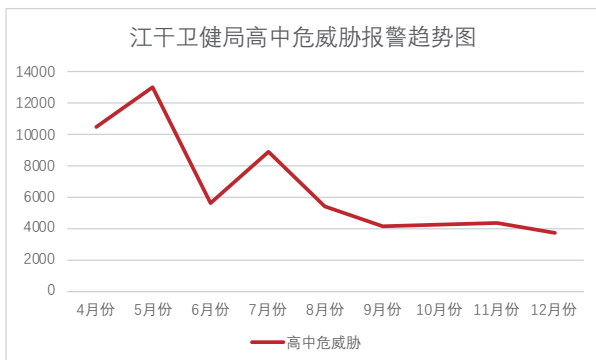
内网威胁态势

的问题，让态势感知实现了真正落地。

网络威胁持续降低 解决缺钱缺人两大矛盾

对于该项目，奇安信负责人归纳了四方面的效果。

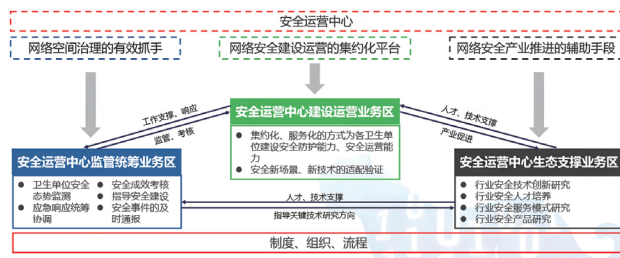
首先是威胁告警事件数量明显降低。结合 NGSOC 提供的持续监测威胁告警信息，安服人员协助客户进行了积极处置，经过半年多的持续安全运营，目前已完成相关后门、病毒的排查和处置工作，江干区卫生专网威胁告警事件总体已呈现明显下降趋势。



其次是发现反复感染风险并及时处理。通过 NGSOC 发现了部分卫生服务中心存在反复感染迹象，由安服人员进行了协助排查并及时处理，提高了区卫生健康局的网络安全监管处置能力。客户通过监测中心定

期下发病毒、漏洞扫描任务，针对安全风险进行有效的事前排查，并与终端控制系统联动进行实时防护。

第三是解决了社区卫生网络安全的人财问题。通过区卫生健康局统一规划、统一建设、统一运营，有效解决了社区卫生服务中心无资金投入、缺网络安全人员运营的问题，这种集约化的投入和管控方式，不仅极大节省了人力和财力，也有效减少了社区卫生终端对卫生专网造成的安全威胁。



最后是形成安全能力下沉的典型经验。该项目针对医疗卫生体系大数据时代的安全需求，基于大数据思维下沉安全业务流程和企业体系架构，以数据为核心，形成医疗卫生体系末端安全能力下沉典型经验，打造出体系化、合规化、可视化、持续化、可复制的江干模式，现已吸引了省内多个市区县卫生健康局前来考察调研和学习。

结束语

杭州江干区卫生健康局的“江干模式”运行成功之后，在全国医疗卫生行业迅速获得广泛借鉴。仅仅一年的时间，就有广西医疗保障局、内蒙古医疗保障局、河南省卫健委、吉林省卫生健康中心、天津市河西区卫健委、武汉市卫健委等数十家单位，纷纷借鉴江干模式，将安全管理前移到规划建设早期阶段，并将态势感知融入系统运行维护过程之中，实现常态化的威胁发现与响应处置工作，变被动防御为主动防御，构建起“关口前移，防患于未然”的网络安全管理体系，进而显著提升医疗卫生行业的信息安全保护和智慧治理水平。安

齐向东：五五制 打造高效有战斗力的组织

2020 年公司进入新的发展阶段，公司提出系列管理举措以不断提高组织能力，自 2020 年四季度起，齐总通过与一线干部的对话活动，澄清公司管理举措逻辑，传授管理经验，针对五五制进行深入讲解。

一、为什么要推行五五制？

五五制是结合公司发展实际，推出的一套系统性管理人、培养人、促人成长的机制。

集团上一阶段取得高速发展，很短时间成了网安一哥，说明事情管的没问题，但是我们要实现第二阶段高质量发展，还要进一步提高效率，尤其是我们对人的管理不成体系，缺方法，要求也不统一。

现在，公司已经是近一万人规模，必须建立严密的组织，没有五五制，组织混乱，导致行动和要求不统一。更严重的是，导致每一个战斗员不能够主动规划自己的路线。俗话说，不想当元帅的士兵不是好士兵，所以部队里每个基层都在抢最难攻的山头，打最艰苦危险的战役。企业也是如此，只有严密公平的组织，才能激发员

工的积极性。员工高绩效产出，拼搏奋斗，公司才有希望，所以我们必须要改革！

五五制机制，通过打造严密公正的组织，能让干部真正负起责任来，从而激发员工的积极性，增强团队战斗力，有效提升工作质量和服务质量，给客户创造更大的价值，提升奇安信的 brand，永葆第一的地位，引领行业前进。

二、什么是五五制？

五五制是我们通过管人推动管事的一套体系。五五制作为一个组织设置的规则，日常工作重点在管人，通过管人推动管事，通过做事成就人，核心要加强对人的管理。

五五制把组织分成一线二线三线：一线干部管行为，保证执行到位；二线干部管目标，保证组织目标达成；三线干部管方向，保证业务方向正确。

五五制把组织标准化了。原来公司组织有五六层，效率低，决策慢。现在把组织变成了一二三线，压成三层，二三线干部减少了近一半，效率提升了，员工上升通道也清晰了。

这就是五五制，确保人，目标，方向都有人负责管起来，这样一来，我们就能成为高效有战斗力的组织。

三、什么是五五制的一线干部？

一线干部是不脱产的劳动者 + 管理者，每个团队不能少于 5 个人，不能超过 10 个人。

试想 9000 人有 1000 个精英骨干，如果都不干活脱产搞管理，那么提拔一个一线干部，公司生产力就下





降一截。一线干部既要管人，又要干活，那么管理幅度就不能大，我们把底线设为5个人，上线不能超过10个人，这是五五制组织设置的规则。

五五制下，干部岗位设置和要求清晰明了，员工只要工作努力，有卓越贡献，心态积极正能量，就有被提拔的机会。

四、五五制的一线干部管什么？

一线干部的核心是管人，人管好了事自然就管好了。总结一下，一线干部要做到“七管”：

第一，管人心。俗话说，“人心齐泰山移”。拔河比赛是人心齐的胜利。人心齐有三个标志，其一，有成为共识的奋斗目标；其二，充满乐观、向上、友爱、互助，无怨气；其三，遵守纪律步调一致。一个团队劲都往一

处使，都认同一个方向，这就达到了管人心的目的。

第二，管当责。俗话说，“两军相遇勇者胜”。团队作战讲究“守土有责”。当责有两个标志：其一是说到做到，日清日结；其二是遇到难事、急事能替身而出，不推托、不畏难。在工作中总会有难事、急事，遇到这些难事急事时，团队中有没有人，能主动牺牲自我，克服自己的困难，成就团队的目标；有没有人，能主动跳出来当董存瑞，用自己的牺牲来减少团队的伤亡；有没有人，能像黄继光用自己的胸膛堵枪眼，为队友向前冲赢得时间。只有答案是肯定的，才能说明你管好了当责。

第三，管奋斗。管奋斗让组织目标按时实现，为什么强调按时？因为目标拖期后果很严重，会导致协同部门白白浪费精力，造成大量内耗。完成目标的过程中会有很多困难，不能因为有困难就擅自修改目标。定目标的时候会对困难估计不足，对技术预见不足，对突发性

问题估计不足……出现困难的时候，是通过拼搏完成，还是任由拖期？在这种情况下，一线干部必须带头奋斗，按时完成目标。华为“以奋斗者为本”有三条，其一加班，其二精益求精，其三提升、成长。记者采访孟晚舟，华为是不是强迫员工加班？孟晚舟回答，华为从来没有强迫员工加班，但是在华为有成就的人，都是加班加点有奋斗精神的人。

第四，管正直。敢说，敢清理。首先，要培养团队简单、明了、直接的文化，不要拐弯抹角。每个人都有自己管人的风格，比如脾气火爆的人说话难听，但并不一定对员工不好。怕就怕，平时软绵绵，突然强硬，组员就很难接受，所以要形成自己的管理风格。其次，发现不合格的人敢于撤掉，明明发现不合格了，就不清理，过度容忍，反而让全组感觉不公平。一个人干80%的工作不表扬，剩下的人干20%不感到可耻，那团队无法留住人，完全丧失战斗力。

第五，管诚信。不说谎，重承诺，一诺千金。哪怕有错，咬牙也要承认，诚信为本，不能什么事只想着自己，这是人心齐的基础。

第六，管分配。分配任务、分配利益要落在线。如果你分配搞大锅饭平均主义，肯定不行，得拉开档次。手指长的多给点，短的少给点。五个人，如果没做到有区分，就会让先进的变落后，出现劣币驱逐良币，本来一个能战斗的组织，慢慢变得失去战斗力。

第七，管成长。一线干部要关心团队每一个人的职业成长。俗话说，长江后浪推前浪，一代更比一代强。一个一线干部，每年都能为公司培养一个干部，这就是一个好干部。

所以，只要管人，你每天就得面对这些问题。把这几个问题解决好了，就是把人管好了，通过管人达到了管事的目的。如果不愿意处理这些问题，你就不是一个合格的一线干部。

五、把晨会用好打造团队奋斗正气

1、晨会不是工作分配会，不是“难题”讨论会，也

不是经验分享会。

很多一线干部利用晨会检查进度，检查进度有两种方法：一种是发现进度不齐，有快有慢，让快的帮慢的，时间久了，鞭打快牛，产生不公平；另外一种发现进度不齐，对进度慢的提出批评，责令他追赶，当他尽了力也赶不上，才让快的帮慢的，如果多次帮助反复发生，就要考虑优化掉。

前一种检查进度的方法不可取，时间久了，它会让“进度慢”的人有借口，让“进度快”的人有抱怨。后一种检查进度的方法是我们鼓励的，它能让“进度慢”的人有压力，让“进度快”的人有团队荣誉感。所以，晨会的核心任务还是管人。

2、晨会是管人的会，是日清日结，是表扬与批评会。

一线干部管人，责任重大。公司对员工有纪律要求，部门对员工有目标要求，组里对员工有任务要求，如果有人总是违反纪律：总是丢失目标、总是不完成任务，就会拖团队的后腿，就会影响团队的氛围、就会使团队因不公平而不团结。

晨会是日清日结。“日清日结”要求分任务时要清楚、可度量，否则无法做到。如果能把中长期任务，量化到天，每天或每三天都有锚点，就可以及时检查，实时对齐目标。

晨会要针对日常行为，提出表扬和批评。晨会要营造一个场域，要让奋斗的人、优秀的人得到激励，让不合格的、落后的行为得到制止。表扬和批评是最好的管理，敢于批评人的干部，是对自己要求高，对荣誉和目标有追求的人。如果员工对自己人生也有追求，其实他喜欢这样的头儿。比如李云龙很严厉，又打又骂，但是士兵喜欢跟着他，因为能打胜仗，能成长。团队内有坏人坏事，你不批评不制止，导致氛围不好，有追求有奋斗的人在你团队里憋屈，觉得不公平。

当然，管理有各种风格，批评为主还是表扬为主，都可以，只要对团队里的干好干坏的人差异化管理，有奋斗精神积极努力的人得到了激励，不努力不奋进的人没得到好处，就能有好氛围。我们鼓励一线干部，八仙过海各显其能，打造一套自己的晨会方法。[安](#)

云安全管理平台

云安全的智慧大脑



运用软件定义安全的设计思路，将云的属性赋能给安全体系

在公共服务云安全建设中，协助云服务商搭建可按需交付、分权管理和业务增值的云安全资源池。在行业私有云安全建设中，使安全具备敏捷上线、集约化部署和易于统一监管的能力。云安全管理平台为各行业客户提供安全产品服务化、安全能力一体化、安全运营自动化三大核心价值，为云保驾护航。

我在奇安信 一层一层叠出世界

作者 公关部 孙丽芳



2021年是黄鑫在奇安信工作的第八年。

八年来，一个行业、一家公司、一件事。90后黄鑫的“一成不变”，最初有点出人意料。“他们觉得我干两年肯定就换了，刚毕业换几个行业、几家公司很正常。但其实，我理解找到自己真正喜欢的事，在坚持中适应变化，在变化中成长，那才是有意义的”。

这件让黄鑫真正喜欢的事是数据可视化与可视化分析。

数据可视化与可视化分析是将数据呈现给用户以易于感知的图形符号，让用户交互式地探索和理解数据。在互联网时代，可视化通过借助计算机图形、图像的制作手段，从数据中挖掘出的有价值信息，让用户知道数

据背后的故事，帮助用户判断与决策。

在变化中成长起来的黄鑫，目前任职奇安信雷尔可视化平台研发部负责人。

离很酷的人近了一步

“雷尔”这个名字是在团队头脑风暴中，由黄鑫一锤定音。“雷尔”是英文 layer 的音译，而 layer 是可视化最基础也最核心的元素——图层。

“一生二、二生三、三生万物，可视化的世界就是由一层层的图层叠加而成”。黄鑫觉得“雷尔”既具象又抽象地表达出可视化的含义。除了取名，黄鑫参与了雷尔

可视化平台研发部建设的全过程。

外型上这是一个标准的 90 后 IT 男，思维和语速都很快，帽衫仔裤，黑框眼镜。但镜片之后的眼神，透露着和 29 岁的年龄不相称的成熟。

这种成熟不是与生俱来，就像可视化也不是黄鑫本来的专业。转折来自于 2013 年。这天，原本在一家电话会议公司实习但觉得意思不大的黄鑫，提前结束实习，如愿被推荐进入奇安信实习。“当时我暑假刚参加了公司举办的第一届全国信息安全技术大赛获得了三等奖，又觉得公司的一些技术大牛很酷，所以对这里非常向往。”

能和很酷的人一起工作，这几乎是黄鑫当时全部的想法。而事实上，后来短短几年时间，黄鑫自己就成长为了很酷的人。

历来如此不是不可改变

黄鑫实习的部门是信息安全部，部门的一项主要工作是管理公司内部员工的网络访问。当时这项工作有个痛点，公司所有机房交换机的 ACL 条数无法及时有效的监控，需要逐条敲命令行，既繁复又易疏漏，一旦溢出会对网络安全带来严重影响。

虽然痛点明显，但这项工作历来如此。能打破历来，做出改变，让监控更简便，结果更直观吗？

计算机专业的黄鑫回答：能！他萌生了制作一套网络设备 ACL 监控可视化系统的想法。

没有经验、没有参考，但黄鑫得到了领导的大力支持和同事们的热情帮助。“我自己感受的奇安信的第一点好，就是它有拥抱变化的文化。这个变化可能是外界带来的，也可能是你自己驱动的。所以，哪怕你是实习生，它也会充分信任你，允许你尝试和创新。”

在公司积极融洽的环境中，黄鑫边摸索边求助，终于把当时公司办公网络的核心交换机的使用情况全部做了可视化。之后，他每天早上发出一个统计邮件，展示所有设备的 ACL 使用情况、风险等级等信息。

这套可视化系统让黄鑫获得了当年的全校优秀毕业

设计，也顺利留在了奇安信，更重要的是，让这个刚毕业的大学生找到了自己未来的方向。

业务驱动变化，变化带来成长

找到了方向的黄鑫学习劲头十足，入职后的第一年，大部分时间都用于了可视化技术的学习。

“奇安信的另一个好处就是允许你有学习的空间，这里有一点校园的感觉，学习的氛围很浓。除了允许我在工作时间学习，公司还给了我展示成果的机会。我做可视化研究期间，领导经常会带人来看，能产品化的就产品化，能推广的就推广。”

可视化在企业级安全领域帮助发现和解决问题的优势非常明显，不论是安全运营，威胁情报，态势感知都必须具备“看得见”的基础能力，从而进行更有效更智能的分析。公司对可视化研究非常重视。2014 年，奇安信和北京大学联合组建了可视化实验室，黄鑫也得以跟随业界顶尖的专家团队直接学习。

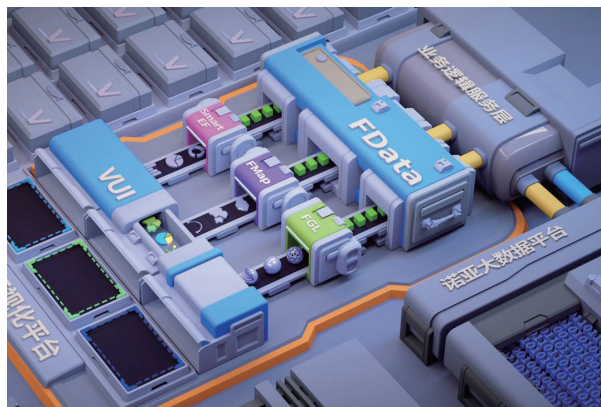
短短几年时间，黄鑫快速成长，在他的身边也聚集起一群小伙伴。

“这一时期可以说是小而美阶段，我们一边做学科研究，一边在实践中基于学科技术解决客户的实际问题。”

小而美的阶段很快迎来了挑战，原因在于随着安全场景越来越复杂，网络安全行业的品类趋于分散、功能



趋于细分，客户需要高度定制化的开发，而且新型攻击形式层出不穷，新产品研发需要更短周期。针对这种情况，奇安信很早就布局四大研发平台，以通过“乐高化”的方式，大幅度缩短新产品研发周期。这其中就包括可视化研发平台。“以前可视化可能只是辅助，但后来已经成了网络安全产品的标配。”



黄鑫就此承担起更重要的任务。2018年，奇安信雷尔可视化平台研发部正式成立，黄鑫任负责人，也是公司当时最年轻的直属部门负责人。

“业务驱动变化，我们积极拥抱这种变化。我以前主要注重个人技术能力的提升，现在要把重心转到带领团队规模化成长。公司大部分的产品团队都有一些可视化的开发人员，但水平参差不齐。雷尔的组建不是把这些人集中起来做开发，而是输出强有力的引擎、组件、平台产品，实现技术的复用，为公司所有团队提效降本。”

形成多赢的局面

时光未曾有许诺，但绝不辜负努力的人。年轻的雷



尔一步一个脚印，对公司各产线的支撑作用越发显现，稳扎稳打来到2020年。

12月18日，黄鑫正在组织本年度最后一个大活动——CSIG图像图形中国行——走进奇安信。多位中国可视化分析圈的大牛到场。黄鑫是现场主持人，不主持的时候，他就站在台下，时不时拿起手机拍照记录现场。这很像黄鑫这一年的角色，既在台前，也忙幕后，能冲到业务一线，也把更多精力投入到管理、投入到雷尔整体效率的提升与产品规划及落地之上。

“2020年最大的收获是雷尔开始做产品，这是我们主动的一个变化。雷尔以前做的是能力平台，也就是代码库，没有产品，所以要提供很多的人力服务支持。但这样一个个项目做，很多时候工作是重复的，工程师觉得自己没有进步，而且一旦扎进去某个项目，就无暇顾及及其他。今年雷尔做的是平台级产品，比如WIDE、胶囊、3D地图、哥伦布，把门槛降低。各部门的工程师进入产品的软件界面，参考用户手册就能用起来。我们更多地做产品迭代，更少去做人力服务支持。”



WIDE
轻松做大屏



Capsule
展厅黑科技



Map
酷炫地图可视化

这样做的效果非常明显。以 WIDE 为例，它是雷尔研发的交互式大屏编辑器。可视化大屏系统是公司各业务的刚需，需求源源不断。而可视化大屏系统的生产过程十分低效，它的问题与古时候的书籍生产如出一辙：难度高、耗时重、产量低。2019 年下半年，雷尔开始探索降低大屏生产难度和耗时的方法，于 2020 年推出了 WIDE，这被称为可视化大屏界的活字印刷术。WIDE 集成了雷尔自有的丰富组件，并且支持自定义组件。组件配置足够简单，几个动作就能配出想要的效果。还能一键导出源代码，省去繁琐的项目开发搭建流程。

在 WIDE 帮助下，设计师和开发工程师只需要少量工作就能完成一套可视化大屏系统的生产；胶囊 - 多端交互展厅演示平台，目前已成为展厅必备，在全国各地开花结果；哥伦布 - 时空可视化分析，用零代码完成数据的时空展现与交互式探索，奠定了进入可视化叙事赛道的重要基础；3D 地图编辑器，大批量快速的定制地图样式、建筑样式、环境样式等。这些都是雷尔‘乐高化’的产物，把产品和技术都做成乐高模块，用标准化生产实现个性化定制，避免重复劳动，提质增效。

在这一思路下，2020 年雷尔完成了以人力服务为主到以产品服务为主的升级，形成了多赢的局面，既提升了项目交付的质量和效率，又让平台人员有了长足进步的空间，还能让平台有更多为公司创造直接商业价值的可能。

让定制快一步

2020 已经画上句点，提到 2021 年的愿望，黄鑫说：“生活上是希望能多点时间陪女儿”。

相比较这种简单、朴素，黄鑫的工作愿望则宏大很多。

“雷尔 2021 年要做更高生产力的平台，由 Web 端一体化平台、客户端一体化平台两条核心生产线构成，让定制快一步，成为这个行业真正的头部玩家！同时在雷尔的强势成熟领域 - 地图可视化，我们也将主动挑战新赛道 - 成为国内最强时空可视化叙事平台，用故事打动人心，让炫酷再次升级。”

这其实是黄鑫一直以来的愿望，就像他在公司内部通讯系统蓝信的个人签名上所写“做好眼前事，看清远方路。让更多普通人在一起用简单普通的方式获得集体的成功。”

在黄鑫看来，这条远方的路，必将通往可视化更广阔的应用空间。这个“一层一层叠出的世界”犹如真实世界的倒影，而在大数据和人工智能时代，可视化技术连接了人、大数据与智能，给很多问题提供了直观且有效的回答，从而使“倒影”拥有比真实更加真实的力量。未来，雷尔将持续深耕可视化分析前沿技术，产出更有价值、更好用的可视化产品，继续让“数据驱动安全”看得见、用起来。安



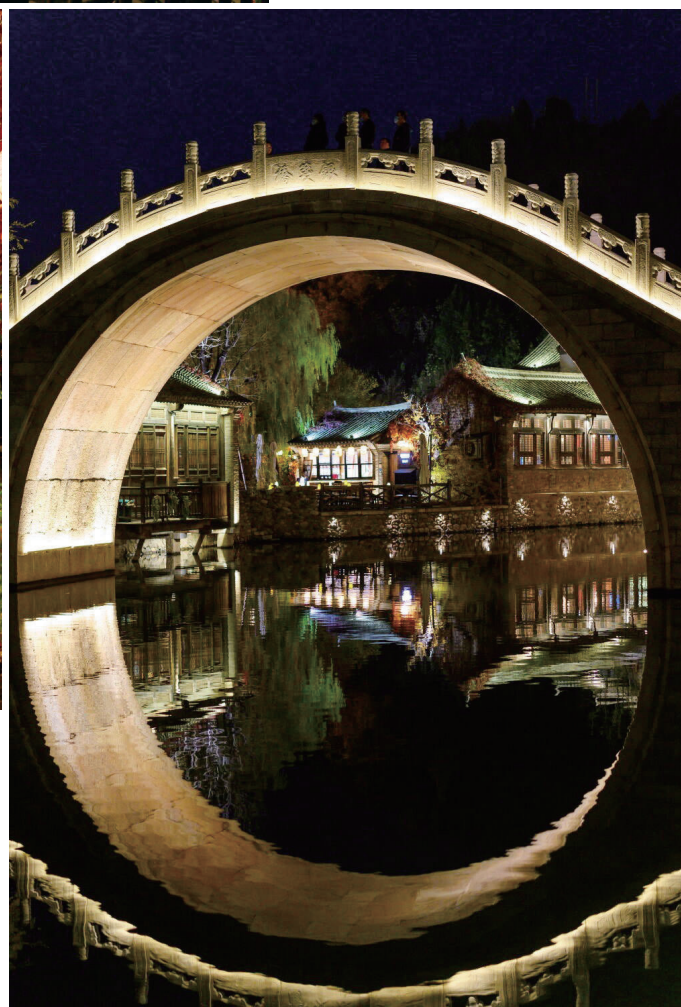
摄影 / 威胁情报中心 黄朝文



“不管你愿不愿意，5G、物联网、正在与传统景观与文化交融。图为北京大柵栏步行街，5G与千兆网络已经遍布每个角落，拍照分享、扫码付款、网络直播，通过手机就可以马上与这个智慧城市链接起来。”



图为奇安信威胁情报中心完成奇安信威胁情报检测引擎 QTDE 和红雨滴高级威胁检测引擎 RAS 发布，并将其与各产品线集成后，团队到古北水镇团建，黄朝文用相机记录了当时的景色。





奇安信荣获第三届进博会“网络安全突出贡献奖”

第三届中国国际进口博览会网络安全表彰授牌仪式上，奇安信凭借在网络安全任务中的突出表现，被授予“第三届中国国际进口博览会网络安全突出贡献奖”。

第三届进博会是在特殊背景下，我国举办的一场规模最大、参展国别最多、线上线下结合的国际经贸盛会，吸引了近40万名专业观众注册报名。奇安信作为第三届进博会网络安全的技术支撑单位，在网络安全值守期间为进博会核心区域提供了7*24小时的应急响应服务，并在必要时提供漏洞验证、漏洞检测、修复等方面的技术支持和工作支持，圆满完成了大会期间的网络安全任务。



奇安信双向网闸荣获中国信息安全测评中心最高级别认证



奇安信网神 SecSIS3600 安全隔离与信息交换系统（双向网闸）顺利通过中国信息安全测评中心分级评估测评，成为业内首家获得该类产品最高级别、即 EAL4+ 证书的厂商。

EAL4+ 级别是目前国家信息安全测评中心针对网络安全隔离类产品所颁发的最高级别认证。经过测试，奇安信网神 SecSIS 3600 安全隔离与信息交换系统在保密性、完整性和可用性等方面完全满足 EAL4+ 级的所有要求，成为业内首家获得该认证的厂家。这是继奇安信单向光闸获得 EAL4+ 资质后，安全隔离与信息交换类产品再次获得权威认可。

奇安信代码安全实验室获微软官方致谢

2020年1月，奇安信代码安全实验室研究员为微软发现两个“重要”级别的漏洞，于第一时间向微软报告并协助其修复漏洞。1月13日，微软发布了补丁更新公告以及致谢公告，公开致谢奇安信代码安全实验室研究人员。

两个漏洞分别为 CVE-2021-1709 - Windows Win32k 提权漏洞和 CVE-2021-1646 - Windows WLAN 服务提权漏洞。提权漏洞会在 Win32k 处理内存对象出错时触发，导致攻击者在内核模式下运行任意代码，之后安装程序，查看、更改或删除数据，或以完整的用户权限创建新账户；服务提权漏洞存在于 WLAN Service 中，可导致攻击者在易受攻击的系统上执行提权操作。目前微软已修复这两个漏洞。



奇安信威胁情报荣获“2020 年度‘新基建’优秀解决方案”奖

奇安信威胁情报中心推出的“基于本地数据的文件威胁鉴定与情报生产解决方案”，凭借多源化的威胁情报采集能力、精准检测和闭环运行能力，荣获《网络安全和信息化》杂志颁发的“2020 年度‘新基建’优秀解决方案”奖。

《网络安全和信息化》杂志认为，该方案具备多源化的威胁情报采集能力，针对采集情报可进行有效处理、生产、运营等全生命的周期管理。同时能基于内生情报多属性、多维度的关联分析与检索，根据情报消费方的需求开发相应的检测、展示、关联分析系统，满足各个业务部门基于内生的威胁情报数据实现深度监测与分析的需求。



“格格病毒”潜伏十余年发威 奇安信公布病毒发作日历

1月13日，奇安信 CERT 监测到一个潜伏十余年的病毒——“格格病毒 (incaseformat)”。根据样本分析发现，该病毒程序中存在 bug，导致获取的系统时间错误，到了定时日期存活病毒还会再次发作，后续还将在 2021 年上半年发作 19 次。中招电脑表现为：除系统 C 盘外其他文件全部被删除。奇安信 CERT 将该病毒风险评级为“高危”，风险等级定位“蓝色”（一般事件），已安装天擎用户不受任何影响。

由于该病毒隐蔽性强，难以根除，奇安信公布了 2021 年（上半年）格格病毒发作日历，同时强烈建议客户“应检尽检”，全面在终端上安装天擎等集中式安全管理软件，构筑无死角的防线。



奇安信董事长齐向东谈职场：干网络安全要甘于寂寞

“我们做技术，尤其是网络安全技术，往往需要能够甘于寂寞。”奇安信集团董事长齐向东在热门职场节目《职场是个技术活》上说，他最看重能够坚定干自己的事，“命长”的员工，走得更远。

在《职场是个技术活》节目中，奇安信实习生全方位深入了解奇安信的网络安全产品和创新的网络安全服务，也让大众对于网络安全有了更直观的感受。

奇安信从成立时起，就致力于“让网络更安全，让世界更美好”，齐向东也曾表示，“网络安全的本质是人与人之间的攻防对抗”。对优秀人才的激励和凝聚，激发员工的积极性和创造性，都将在未来转化为奇安信未来发展的竞争优势。

2021 数字中国创新大赛启动 第二届“虎符网络安全赛道” 升级助推数字中国建设

1月17日，“2021 数字中国创新大赛”启动仪式在福州举行，作为大赛的重要部分，第二届虎符网络安全赛道也同步开启了报名通道。

今年的“虎符网络安全赛道”将在去年首次把 PK 体系与传统 CTF 竞赛模式结合的优势基础上，继续保持 Wintel+PK 双体系并行模式进行比赛，以“PK 体系”

在传统 CTF 竞赛中的创新升级应用作为赛事的核心驱动，并在场景、阵容、选手权益三个方面进行升级。

比赛将分为线上初赛和线下决赛两个部分。线上初赛，将通过“夺旗赛”（CTF）模式最终选拔 35 支行业 / 高校战队，与 5 支特邀战队共同进入决赛；决赛现场将通过“攻防兼备”（AWD PLUS）的比赛模式进行角逐。同时，决赛现场 PK 体系题目占比将从去年的 35% 提升至 45%，以促使行业及高校提升对 PK 体系的重视程度。



奇安信浏览器关于 Adobe Flash 无法正常加载的客户建议

针对客户反馈“业务系统因未能正常加载 Flash，导致无法正常运行，甚至出现系统瘫痪”的情况，奇安信浏览器立即响应，继续延长针对 Flash 的支持，以确保客户业务平稳和安全运行，免受影响。

奇安信浏览器事业部也特此建议，客户应尽快通过长期解决方案解决 Flash 加载问题，或采用替代方案对业务系统实施改造。奇安信可提供 Flash 技术迁移的顾问服务，及技术迁移完成前的应急方案，客户可联系奇安信市场人员获取。

目前，奇安信可信浏览器支持 Windows、信创、Linux、Mac 等操作系统平台。以“多方兼容、统一管理、内生安全”为设计理念，具备广泛的业务系统兼容、访问行为防护及客户端统一管控能力，已为近千家政企客户提供专业的统一业务承载平台解决方案。

奇安信携手交通银行开展金融行业网络安全攻防研讨会



由奇安信与交通银行网络联合实验室共同举办的首场金融网络安全攻防演练研讨会在云南昆明举行，旨在整体提升金融行业信息安全水平和网络攻防能力。

在研讨会上，奇安信安全服务团队资深讲师分享了网络安全攻防实操经验和技巧，主要涵盖了金融网络安全攻防基础、全流量威胁分析、攻击技术解析、场景化防御技术等内容。

除了攻防经验分享外，作为活动主办方的交通银行—奇安信网络安全联合实验室，与参会人员、交通银行信息技术人员等展开联合研究，通过复盘以往金融行业网络安全攻防案例，梳理网络安全攻防各种技术手段，此前遇到的问题，寻找最佳解决方法。

奇安信相关负责人表示，将通过交流和培训的方式将攻防经验分享给更多的金融机构从业者，整体提升金融行业的网络安全水平和能力。

齐向东委员畅谈“三好”委员读书群

作为网络安全读书群群主，奇安信集团董事长齐向东在政协北京市第十三届委员会第四次会议“我是委员”采访活动回答媒体提问时表示，“委员读书群有‘三好’。”

第一“好”：线上线下相结合的场景化读书。《漏洞》

一书是齐向东根据十几年的从业经历对网络安全产业的总结和思考。但网络安全技术性强、行业门槛高。因此，他组织委员读书群的群友，参观奇安信应急响应中心和网络安全实验室，通过现场场景读书，把复杂的技术问题直观化来方便理解。

第二“好”：解决了碎片化阅读和系统性思考之间的矛盾。有人形容数字化时代的学习虽能随时随地快速获取信息，但也缺乏思考的过程，所以系统化读书很重要。而委员读书群中，有专家带读、解读，能够用比较短的时间，让成员进行系统完整的学习，不仅向书本学，也向群主学、向群友学、向实践学，切实提升履职尽责的水平。

第三“好”：群主是专家，提纲挈领让读书变得更容易。委员读书群的群主都是各自领域的专家，能深入浅出划重点，提纲挈领抽逻辑，高瞻远瞩见未来。例如习近平谈治国理政读书群，群主就是吉林主席。此前，吉林主席带领科技委委员，在奇安信进行了一次读书座谈会，要求大家读书“常学常新”，并谈了四点体会：一是坚定信心；二是温故知新；三是做到与时俱进；四是及时跟进学习。

最后，齐向东表示，希望委员读书群能一直办下去，也希望更多人养成爱读书、读好书的习惯，和委员们一起掀起全民阅读风潮，加快推进我国社会主义精神文明建设建设。安



《安全运营中心调研分析报告》

随着《网络安全法》、《网络安全审查办法》、“等保 2.0”等政策法规的逐渐落地，网络安全运营中心的建设及运营成为企业网络安全保障的常态化工作，迎来良好的发展机遇。

赛迪顾问针对国内安全运营中心的现状和问题进行了深入调研。调研对象为 27 个省市自治区 300 家机构的网络安全负责人，涉及金融、互联网、软件与信息服务、政府、运营商、交通物流、能源、制造、烟草、广播传媒、商务服务等行业。

调研结果显示：

1、国内安全运营中心仍处于起步阶段，主要以满足合规性为主。运营时间较短，团队人数和投入金额尚没有形成较大规模。

2、专业人才的缺乏是制约安全运营中心发展的重要因素。安全团队编制不足正在严重阻碍威胁监测与响应等运营工作正常开展。

3、安全运营中心是未来企业安全建设重点之一。大部分企业将进一步提升自身安全运营中心的成熟度，安全运营平台和终端安全是未来建设重点。

1. 安全运营中心的定义

1.1 概念界定

安全运营中心由一个全天候轮班执行运营工作的团队以及一套专注于帮助运营团队执行预测、防御、检测、评估并对威胁或事件进行响应的工具和运营管理流程组成。

同时，安全运营中心应该包含但不仅限于以下能力：



图 1-1 安全运营中心能力图谱

数据来源：赛迪顾问，2020.08

1.2 安全运营中心成熟度模型

为应对日益严峻的网络安全威胁，网络安全运营中心的成熟度模型被设计用来帮助企业评估自己目前的安全运营中心的能力水平。网络安全运营中心的成熟度模型能够帮助企业快速找到安全运营中的短板并制定有针对性的策略，提升企业“安全竞争力”。



图 1-2 安全运营中心能力图谱

数据来源：赛迪顾问，2020.08

从安全运营中心的成熟度来说，安全运营体系的建设也是循序渐进、按需建设的，即由安全技术体系、安全管理体系、安全运营体系组成成熟度模型。不同的级别对应不同的安全度目标。

级别	状态	运营成熟度目标
预备级		处在基础设施建设阶段，安全建设以合规为主，尚不具备安全运营工作的开展条件。
一级	初始状态	预防为主，具有防火墙、防病毒系统运维能力，资产不清晰，缺少漏洞管理机制，对整体安全威胁不可见，没有事件响应处置流程。
二级	基础运行	以合规为主，安全基础设施处于一定阶段，具有安全监控人员，有资产管理动作，有漏洞管理认知，对安全威胁有一定的可见性，但不具备对威胁事件深入分析的能力，没有建立成熟的事件响应流程。
三级	运行可控	有成熟的事件响应流程，资产管理及漏洞管理具备常态化流程与机制，具备威胁监测、分析、事件处置能力，各岗位职责明确，对整体安全威胁态势可见，初步的量化管理。
四级	体系运营	具有安全事件响应中心或安全运营中心等安全运营常态组织，各岗位之间紧密配合，资产、漏洞等基础工作扎实有效，能够高效地开展监测、响应、处置、调查取证分析工作，成熟的量化管理。能够积极主动挖掘威胁情报，能够应对高级别的安全攻击（APT）。
五级	深度运营	除可自主成熟开展各项安全运营工作外，具备网络取证分析和威胁情报收集能力，能够使用各项技术与措施发现未知威胁（0day），能够通过自动化手段开展安全监测、事件响应处置工作，能够7x24小时应对高级安全威胁（APT）。

数据来源：赛迪顾问，2020.08

2. 国内安全运营中心建设现状

表 2-1 安全运营中心目前面对的主要困难与挑战

TOP1	安全团队编制不足
TOP2	运营经费不足
TOP3	缺乏明确而可落地的目标和考核指标
TOP4	缺乏跨部门的网络威胁事件响应处置流程和机制
TOP5	缺乏高层领导的支持
TOP6	缺乏跨部门的协同机制获取必要数据

数据来源：企业调研，赛迪顾问整理，2020.07

（1）中国安全运营中心建设处于起步阶段

调研结果显示，中国安全运营中心还处于起步阶段。本次调研中有 68.2% 的企业已经建立了专门的安全运营中心，但有 1/3 的企业安全运营中心才建立了一年时间。运营时间较短，团队人数和投入金额没有形成较大规模。

（2）核心驱动力依然以满足合规性要求为主

中国安全运营中心主要以满足合规性为主。如何将现有的安全系统纳入统一的管理平台，实现安全形势全局分析和动态监控已成为各企事业单位面临的主要问题。

（3）人是制约安全运营中心发展的重要因素

调研结果显示，专业人才的缺乏是影响发展的重要因素，安全团队编制不足正在严重阻碍威胁监测与响应等运营工作正常开展。绝大多数企业安全运营团队由自有团队或自有团队 + 外包团队的形式构成，而安全团队中没有设置 SOC 运营专岗的企业占绝大多数。

（4）安全运营中心缺乏明确目标及评价标准

无法衡量安全运营工作的成果和进展，缺乏评价结果来促进安全运营工作的持续提升，影响高层领导对安全运营中心价值认可和持续投入。

多数企业（69.2%）没有设定衡量 SOC 运营有效性的指标评价体系，少数设立指标的以安全事件处理数量、安全事件处理平均时间、消除特定攻击行为的进展三种指标最为常见。

（5）缺乏跨部门的响应处置流程

明确各部门的安全职责，通过建立跨部门的协同响应流程和机制是安全运营工作成败的关键要素。

企业安全运营平台普遍拥有的能力有：流量审计与检测、日志采集与管理与资产管理三种。只有极少部分的企业的安全运营中心拥有安全编排与自动化响应等能力。

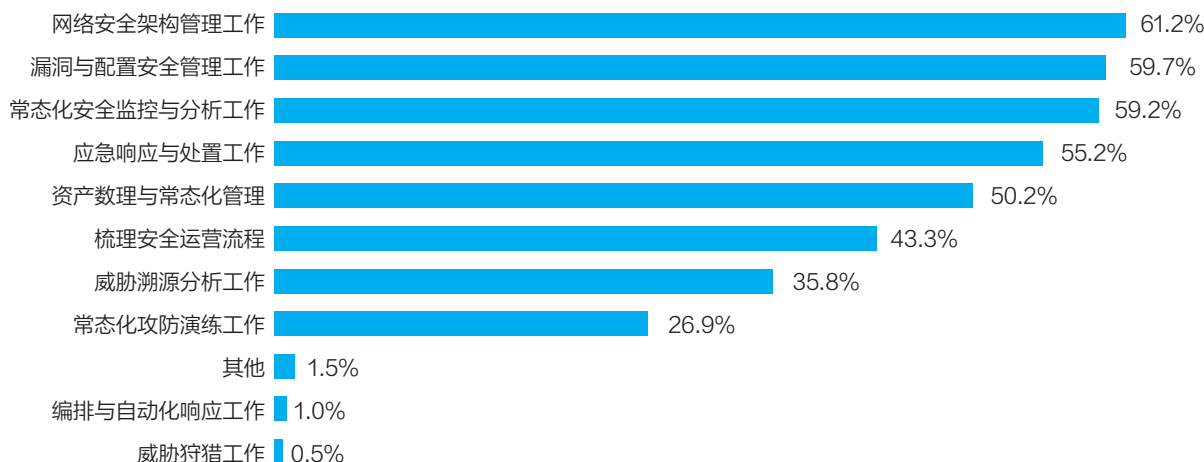


图 2-1 已开展哪些维度的运营工作

数据来源：企业调研，赛迪顾问整理，2020.07

3. 安全运营中心建设的未来预测

表 3-1 安全运营中心未来所需的支持和帮助

TOP1	设定明确而可落地的安全运营中心建设目标和绩效指标
TOP2	增加安全运营团队的编制
TOP3	增加安全运营的预算
TOP4	设立独立的网络安全部门
TOP5	建立跨部门的网络威胁事件响应处置流程和机制
TOP6	促进跨部门的协同获取必要数据

(1) 安全运营中心是未来企业安全建设重点之一

大部分企业将进一步提升自身安全运营中心的成熟度，大部分企业将进一步提升自身安全运营中心的成熟度，安全运营平台和终端安全依然是未来建设重点。

(2) 对安全运营人员的要求进一步提升

对运营人员的分工具有一定要求，责任更清晰，分工更明确。

(3) 安全运营中心外采服务的需求将进一步体现

未来国内安全运营服务市场将会在整体安全市场投入中占有较高比例。自有团队 + 外包团队将是未来企业持续选择的建设方式，外采安全服务的需求量较大。

(4) 安全运营中心是体系化的建设过程

随着大数据、云计算、人工智能等领域的出现，安全运营从被动转变为主动，建立从防御、检测、响应到预测的闭环运营理念，使安全运营体系化。建立标准化的数据及业务流程体系、组织的安全运营管理体系是未来安全运营中心建设的必然选择。

4. 建议

从建设方角度来看，

(1) 安全运营中心是一个长期投入的过程；
(2) 设定准确明晰的目标与机制是安全运营的必要条件；

(3) 安全运营中心应当与业务场景相契合；

(4) 安全运营团队的建设非常重要。

从提供商的角度来看，

(1) 要与业务价值紧密相连。安全提供商在安全运营中心建设过程中，要时刻保持与业务价值的密切关系，从而帮助客户在市场上创造某种形式的竞争优势；

(2) 重视先进的网络安全架构研发与落地；

(3) 推进智能驱动的安全运营。重视人工智能技术在安全运营中心中的实践，以人工智能技术推进安全运营流程和过程向着更加标准化、规范化和自动化的方向发展；

(4) 构建安全产品的技术标准。安

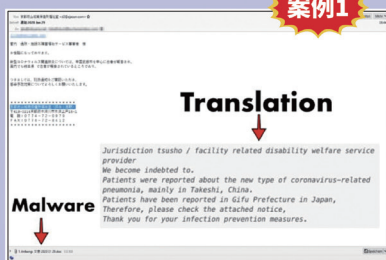


“在重大公众事件中,趁火打劫是网络犯罪分子的一贯伎俩。例如世界杯、马航事件、日本福岛核泄漏等事件中,都伴随着大量恶意软件传播和网络欺诈行为,随着新冠肺炎疫情引发全球关注,一系列新的恶意软件和攻击手段也蜂拥而来。”

“近日,网络安全公司Mimecast、KnowBe4、IBM X-Force和卡巴斯基先后发现了一系列针对“新冠病毒恐慌”恶意软件传播的活动,攻击者利用公众对新冠病毒的恐慌,发送含有恶意链接或恶意文件的邮件给用户,并以冠状病毒关键词为主题诱骗收者打开恶意文件或链接。”

公司也发现部分同事收到类似钓鱼邮件,邮件内的链接为钓鱼链接或恶意域名,请不要点击链接并联系公司网络安全部。”

假冒健康机构针对日本用户的钓鱼邮件样本,下面是IBM X-Force发现的使用日语编写的钓鱼邮件,含有一个Word宏攻击文件,诱骗用户启用宏以后,可通过PowerShell将Emotet安装在用户设备中。



案例1



案例2

以下是伪造高管邮箱发送邮件,这类邮件通常会带有附件,要求大家回复公司敏感信息(如人事信息,财务信息,商机信息等等)。请大家仔细查看发件人邮箱,不要打开陌生发件人邮箱发来的附件,也不要回复该类邮件。钓鱼邮件附件样例



案例3

这些恶意软件电子邮件的特征

身份冒充

假冒疾控中心或相关疫情防控机构、公司老板、人力资源部、IT部门或安全部门等。

邮件主题

大多与冠状病毒相关、人事通知、考勤异常、域名变更或安全通告等。

邮件内容

这些钓鱼电子邮件包含恶意附件或恶意链接,伪装成与病毒、公司相关的通知和文件。部分钓鱼邮件会直接要求回复账号信息。

钓鱼风暴才刚刚开始

对于身处冠状病毒重灾区的中国用户,虽然目前尚未有利用新冠病毒发送钓鱼邮件的正式报道,但是我们仍需时刻保持警惕。共同做好抗“疫”工作!目前,美国、日本等国家都发现此类冠状病毒主题的钓鱼邮件攻击。

八点安全建议

★ 特殊时期,请大家增强安全意识,谨慎甄别邮件,警惕攻击者或不法分子以当前时事进行钓鱼攻击。

请您在收到邮件后:

1. 确认收件人名称与收件人邮箱地址一致;
2. 若邮件内含有链接,请谨慎点击,若链接要求输入您的用户名和密码,或要求下载文件,请先通过微信或电话与发件人联系确认,不要直接输入或下载;
3. 若邮件内有无加载的图片,或打开后产生弹窗,请提高警惕;
4. 请安装天擎,对下载的邮件附件进行查杀;
5. 若您收到任何可疑邮件,可联系公司网络安全部。

请保管好自己的账号密码,不要将账号密码共享给其他人使用
安全事件、钓鱼邮件反馈等问题请发邮件至

g-sec@qianxin.com

—END—



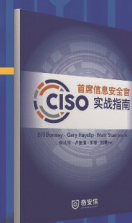
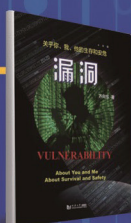
奇安信



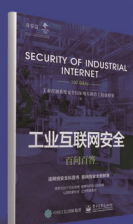
BEIJING 2022

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

奇安信图书馆



国际经验分享系列



网络安全科普系列

网络安全认证系列



网络安全实战系列



网络安全教育系列

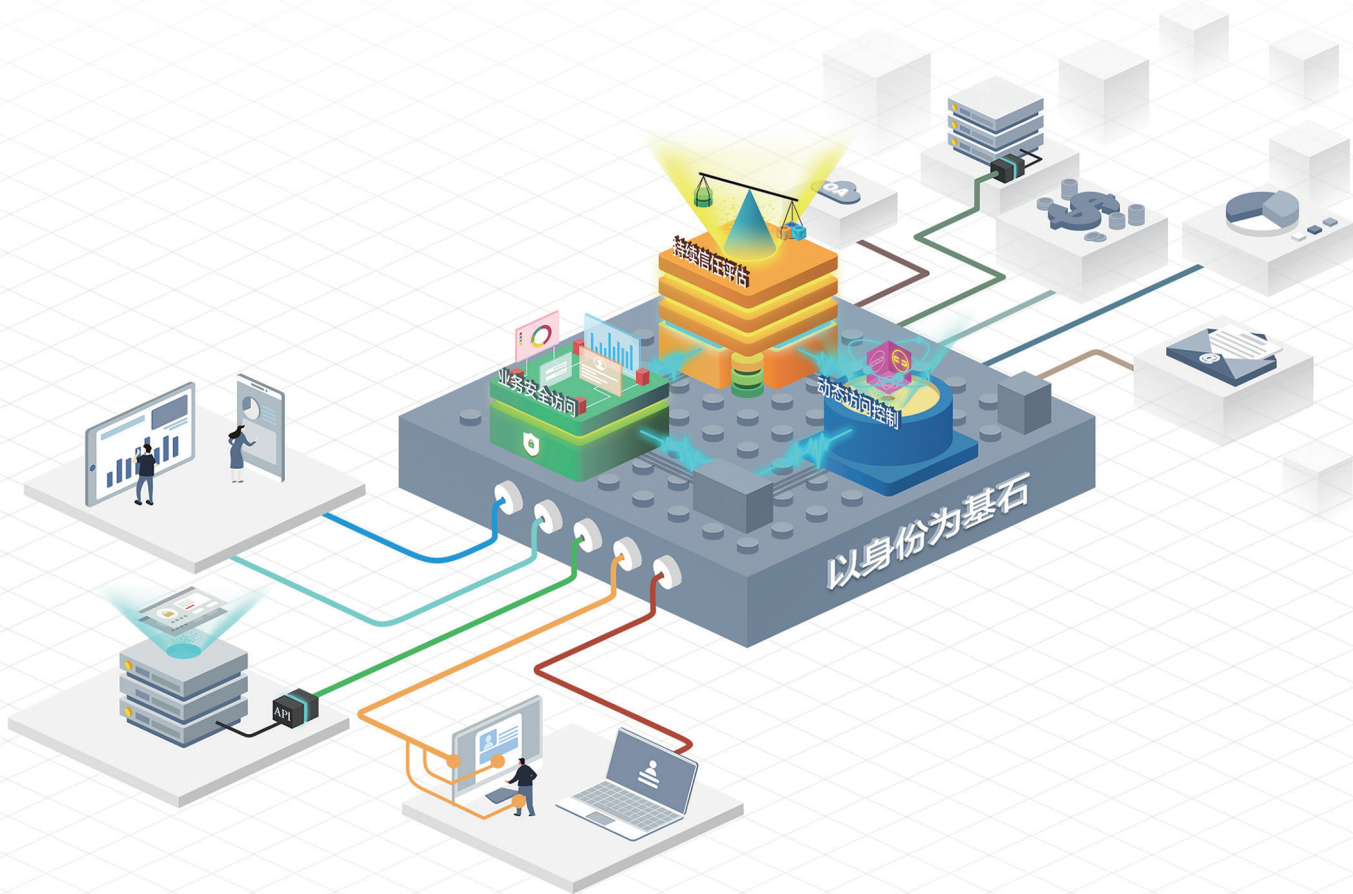


扫码购书

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

云计算和大数据时代
网络安全边界逐渐瓦解，内外部威胁愈演愈烈
传统安全架构正在失效

零信任安全 新身份边界



以身份为基石

- ◆ 为人和设备赋予数字身份
- ◆ 为数字身份构建访问主体
- ◆ 为访问主体设定最小权限

业务安全访问

- ◆ 全场景业务隐藏
- ◆ 全流量加密代理
- ◆ 全业务强制授权

持续信任评估

- ◆ 基于身份的信任评估
- ◆ 基于环境的风险判定
- ◆ 基于行为的异常发现

动态访问控制

- ◆ 基于属性的访问控制基线
- ◆ 基于信任等级的分级访问
- ◆ 基于风险感知的动态权限

构筑基于身份的动态虚拟边界

全面身份化 | 授权动态化 | 风险度量化 | 管理自动化



🌐 www.qianxin.com

✉ kefu@qianxin.com

☎ 400-930-3120

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