SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

美政府网安投资揭秘

P16

P26
3.8 亿次网络攻击与
冬奥“零事故”承诺背后的攻防博弈

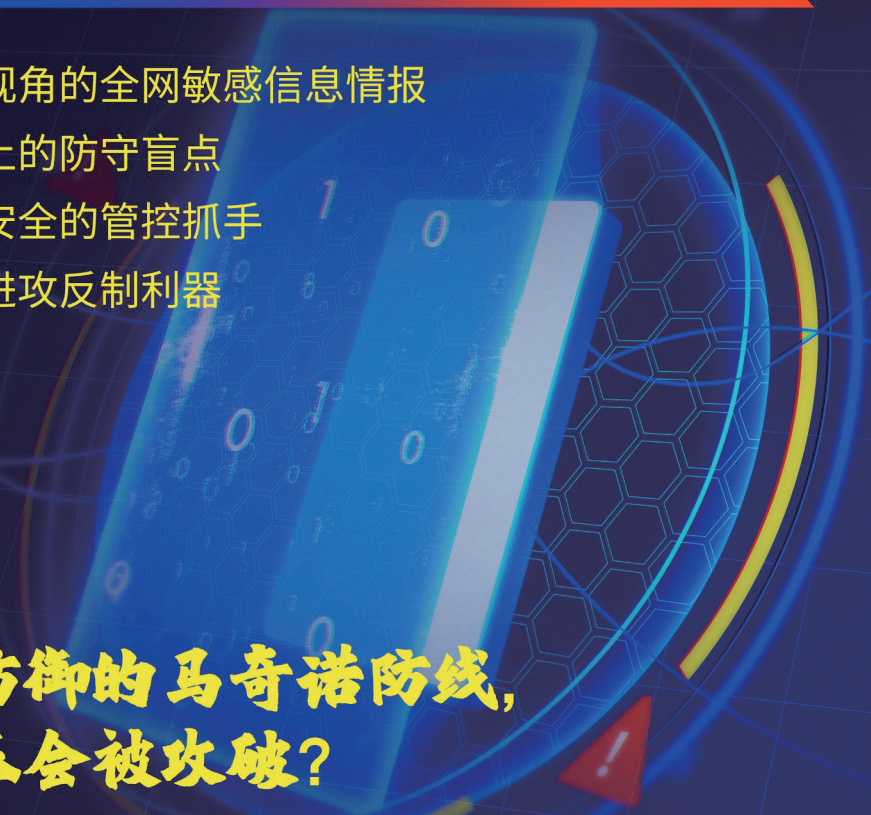
P34
以创业者心态
投身工作

第16期
2022 年 4 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

零信任、克虏伯野战炮及武器代差

美联邦政府 2023 财年网络安全支出中，对零信任及其配套技术的投入与重视，不禁让人想到正在进行的俄乌冲突，以及战争中的武器代差。

我们经常说，人是战争胜利的决定因素，但在人类战争史上，借助创新性武器赢得战争的事例比比皆是。1870–1871 年的普法战争就是这样的例子。

普鲁士军队正是凭借领先的克虏伯野战炮击败了数量众多的强大法国军队。克虏伯野战炮采用钢制线膛炮管，通过后膛装填，标准射速是 6 发 / 分钟，经验丰富、训练有素的炮兵手可以做到 10 发 / 分钟。与之形成鲜明对比的是，法国火炮的最大射速不超过 2 发 / 分钟。在射程方面，克虏伯野战炮同样具有优势，最远射程达到了 3500 米，而法国火炮最大射程不超过 2500 米。性能优异的克虏伯野战炮确保普鲁士军队赢得了多数重要战役，并获得普法战争的最终胜利。

同样是在 19 世纪，中日之间的甲午海战中，中国海军与日军除了军舰吨位和火炮数量的不足，在武器的性能上也存在代差：中国舰队在舰龄、机动性、火炮射速和炮弹威力等方面处于明显的劣势，很难同日本匹敌。这些不利条件导致北洋舰队在战术发挥上受到了严重限制，在作战中被对手火力压制，以至最终海战失败。

战争的胜利是众多因素综合作用的结果，各国军队纷纷在战争中试验各种新式武器，以期借助这种差异，改变战争的走向与最终结果。保守僵化、不及时采用新武器，往往会成为战争失败的一方。这一规律同样适用于与战争类似的网络攻防战：攻击者使用各种新式攻击方式，防护者则部署各种新式的防护措施，以求在网络攻防战中赢得先机。因此，不同于追求可靠稳定的 IT 系统，网络安全建设需要大胆采用各种新技术，否则就无法获得网络攻防中的主动。

美国政府 2023 年财务预算给我们做出了很好的示范：大笔的资金被用于支持相关联邦机构的零信任转型及相关新技术部署。事实上，美国联邦政府一直试图通过部署零信任架构，推进联邦政府网络安全防御的现代化，鼓励对相关新技术的采用。2022 年 1 月，拜登政府再次向行政部门发布备忘录，要求在 2024 财年 (FY) 结束前实施特定的网络安全标准。具体而言，要求美国所有政府机构向零信任网络安全原则迈进，安全自动化、编排和响应 (SOAR) 则是必需的技术之一。

对于网络安全负责人来说，要在攻防战中不成为被动挨打的靶子，时刻要思考的是，网络安全的克虏伯火炮，自己是否已经及时部署。

总编辑

李建平

2022 年 4 月 1 日

CONTEN

目录

安全态势

P4 | 美国中情局主战网络攻击武器曝光，世界各地重要信息基础设施已成美国“情报站”

P4 | 我国电信设施曾遭网络窃密，部分数据传至境外

P4 | 境外公司谎称调研窃取我国高铁数据：月采集信号数据达 500 个 G

P5 | Fodcha 僵尸网络在国内大规模传播，日活跃感染终端超万台

P5 | 多名欧盟高官遭以色列间谍软件监控，国际政要安全风险凸显

P6 | Apache Struts2 安全漏洞（CVE-2021-31805）通报

P6 | Spring Cloud Function 安全漏洞（CVE-2022-22963）通报

P7 | 国内攻防演习 3 月态势：哪些薄弱点最易被利用?

P10 | 中央深改委审议通过《关于加强数字政府建设的指导意见》

P10 | 中办国办印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》

P11 | 证监会就修订《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》公开征求意见

P11 | 美国食品和药物管理局发布医疗器械网络安全指南草案

P12 | 美国《2022 年关键基础设施网络事件报告法案》要点概述

月度专题

美政府网安投资揭秘

美国政府 2023 财年网安预算重点关注关基保护、零信任转型及网军能力建设。

TS

攻防一线

P26

3.8 亿次网络攻击与冬奥“零事故”承诺背后的攻防博弈

安全之道

P30

零事故背后：揭秘 NGSOC 如何助力冬奥安全运营中心

奇安信人

P34

以创业者心态投身工作

安全叨客

P40

比十三香！这份 IT 人“无忧长假指南”有点东西

奇安资讯

P42 | 北京市政协主席魏小东一行莅临奇安信调研

P42 | 北京数十家国资与高新企业齐聚奇安信 交流冬奥网安“零事故” 经验

P43 | 中海油走进奇安信 交流冬奥网络安全“零事故”经验

P43 | 奇安信举办研发平台战略发布会

P44 | 奇安信中标中国广电 5G 安全大单

P44 | 齐向东：“零事故”应成为网络安全防护新目标推动行业高质量发展

P45 | 齐向东出席统战部服务北京冬奥会、冬残奥会工作总结会暨主题教育活动启动会

P45 | 十八国驻华国防武官参访 奇安信全面开启国际市场

P46 | IDC 报告：奇安信终端安全多赛道领先 连续四年市场份额第一

P46 | 奇安信入选信安标委 “网络安全国家标准 20 周年优秀实践案例”

P47 | 奇安信代表顾鑫荣获冬奥会、冬残奥会北京市先进个人

P47 | 奇安信通过全球软件工程领域最高级别 CMMI 5 级评估认证

P48 | 奇安信 SOAR 入选国际权威机构 Forrester 报告

P48 | 《中国网络安全行业全景图》第九版发布 奇安信蝉联“入选最多企业”

第 16 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

安全叨客主编：王梦琪

奇安资讯主编：陈　冲

奇安信集团　虎符智库　安全内参

电子版请访问 www.qianxin.com 阅读或下载

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com

地　　址：北京市西城区西直门外南路 26 院 1 号

邮　　编：100044

联系电话：（010）13701388557

出版物准印证号：京内资准字 2021-L0058 号

印刷数量：4500 本

印刷单位：北京七彩虹印刷有限公司

下载地址：www.qianxin.com

版权所有 ©2022 奇安信集团，保留一切权利。

非经奇安信集团书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

无担保声明

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

事件篇

4 · 15 全民国家安全教育日，国家安全机关公布多起典型案例，包括关键信息基础设施领域遭网络攻击窃密、境外公司谎称调研窃取我国高铁数据等；乌克兰声称成功挫败“断电行动”，为迄今俄乌冲突中最严重的已知网络攻击。

美国中情局主战网络攻击武器曝光，世界各地重要信息基础设施已成美国“情报站”

据环球网 4 月 19 日消息，国家计算机病毒应急处理中心发布报告，披露了美国中央情报局专用的“蜂巢”恶意代码攻击控制武器平台。据介绍，“蜂巢”平台具备智能化程度高、隐蔽性强、攻击涉及面广、设定有重点攻击对象、突防能力强等五大特点。中情局对全球范围的高价值目标实施无差别的攻击控制和间谍窃密，世界各地的重要信息基础设施已经成为美国情治部门的“情报站”。近期，我国网络安全机构连续揭开了美国国家安全局“电幕行动”“APT-C-40”“NOPEN”“量子”等多款网络攻击武器的真面目。

我国电信设施曾遭网络窃密，部分数据传至境外

据新华社 4 月 16 日消息，国家安全机关公布多起典型案件，包括一起关键信息基础设施领域遭网络攻击窃密案。2020 年以来，国家安全机关工作发现，我国有关电信运营商、航空公司等单位内网和信息系统先后多次出现越权登录、数据外传等异常网络行为，疑似遭受网络攻击。国家安全机关依法开展技术检查，确认部分骨干网络节点设备、核心业务系统服务器等被植入特种木马程序，已有部分数据被发送至境外。通过进一步深入调查证实，相关攻击活动是由某境外间谍情报机关精心策划、秘密实施的。该机构调集强力网络攻击力量，使用全球多地网络资源和先进网络武器，妄图实现对我国关键信息基础设施战略控制的目的。最终，国家安全机关成功粉碎其对我国“停服断网”的图谋。

境外公司谎称调研窃取我国高铁数据：月采集信号数据达 500 个 G

据央视新闻 4 月 13 日消息，国家安全机关破获了一起为境外刺探、非法提供高铁数据的重要案件。这起案件是《数据安全法》实施以来，首例涉案数据被鉴定为情报的案件。一境外公司借口调研，委托国内某公司采集中国铁路信号数据。公司法务曾提示项目可能危害国家安全。而面对高额利润，这家公司仍按要求采集数据，还为对方开通登录端口，甚至介绍其他公司赚分成。此项目一个月就采集 500G 数据，若不法分子利用数据进行干扰，可威胁铁路运营。目前，相关嫌疑人已被逮捕。

俄乌冲突：乌克兰成功挫败对其电网的破坏性网络攻击

据 ZDNet 4 月 12 日消息，乌克兰 CERT 和

ESET 披露，归因于俄罗斯的沙虫黑客组织针对乌能源工控设施发起破坏性网络攻击，希望切断区域电力供应，但被成功阻止。此次攻击是迄今为止俄乌冲突中最严重的已知网络攻击。攻击者使用了曾导致乌克兰大停电的 Industroyer 更新版、CaddyWiper 数据擦除软件。据分析，此次攻击发生在 4 月 8 日晚间，Industroyer 更新版在两周前已经准备好，被攻击网络至少在 2 月已经被渗透。

Fodcha 僵尸网络在国内大规模传播，日活跃感染终端超万台

据 CNCERT 4 月 12 日消息，国家互联网应急中心（CNCERT）监测发现一个新的且在互联网上快速传播的 DDoS 僵尸网络 Fodcha，通过跟踪监测发现其每日上线境内肉鸡数（以 IP 数计算）已超过 1 万，且每日会针对超过 100 个攻击目标发起攻击，给网络空间带来较大威胁。Fodcha 僵尸网络位于境内肉鸡按省份统计，排名前三位的分别为山东省（12.9%）、辽宁省（11.8%）和浙江省（9.9%）；按运营商统计，联通占 59.9%，电信占 39.4%，移动占 0.5%。

多名欧盟高官遭以色列间谍软件监控，国际政要安全风险凸显

据路透社 4 月 11 日消息，据欧盟官员透露，欧洲司法专员 Didier Reynders 等多位欧委会官员遭到以色列 NSO 集团间谍软件监控。欧盟官员称，在去年底苹果公司发布警告后，欧委会才发现相关官员已经被间谍软件监控的情况。此前，美国、中国、印度等多国官员都曾爆出遭 NSO 间谍软件监控的消息，国际政要是间谍软件的主要监控目标，如何保护政府官员的数据安全成为当前一大难题。

为应对网络攻击，德国风电设备巨头 Nordex 关闭 IT 网络

据 The Record 4 月 4 日消息，德国风电设备巨头 Nordex 在 3 月 31 日遭遇网络攻击，导致多地业务部门的 IT 系统被迫关停。据报道，Nordex 官网曾在事件早期显示“由于维护工作，本网站暂时无法访问，请稍后再试”，不过现在网站已经恢复正常运行。近半年来，全球多家风电上下游厂商因网络攻击导致业务受影响，网络安全已成为风电行业重大风险。

黑客伪造“政府传票”窃取科技巨头敏感数据，苹果、脸书等均受影响

据 KrebsOnSecurity 博客 3 月 29 日消息，安全博主 Brian Krebs 披露了一种伪装为政府执法部门向互联网公司套取用户数据的攻击手法，攻击者窃取执法部门邮箱等官方账号，向互联网平台发送“紧急数据申请”，从而套取用户敏感数据。最近兴起的 LAPSUS$ 数据勒索团伙正是利用这一手法，成功入侵了微软、Okta、英伟达等知名企业内网窃取数据，苹果、Meta 等巨头曾应黑客要求提供过用户数据。

南非几乎所有公民征信数据泄露：弱密码惹祸 预计损失超百亿元

据 Daily Maverick 3 月 19 日消息，美国征信巨头 TransUnion 的南非公司遭巴西黑客团伙 N4aughtysecTU 袭击，5400 万消费者征信数据泄露，绝大多数为南非公民，南非总人口约有 6060 万人。黑客团伙透露，通过暴力破解入侵了一台存有大量消费者数据的 SFTP 服务器，该服务器的密码为“Password”。TransUnion 公司称，将为受影响的消费者免费提供身份保护年度订阅服务，预计成本将超过 114 亿元。

漏洞篇

4月，多款基础应用开发框架/软件被爆高危漏洞，涉及Struts2、Spring、Spark等，部分漏洞细节已公开，建议用户尽快自查并更新修复。

Apache Struts2 安全漏洞（CVE-2021-31805）通报

4月18日，国家信息安全漏洞库（CNNVD）收到关于Apache Struts2 安全漏洞（CVE-2021-31805）情况的报送。成功利用此漏洞的攻击者，可在目标服务器远程执行恶意代码，进而控制目标服务器。Apache Struts2 2.0.0版本至2.5.29版本均受漏洞影响。目前，Apache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。该漏洞是由于Apache对Apache Struts2代码注入漏洞(CVE-2020-17530)修复不完整导致，攻击者可绕过漏洞补丁，通过构造恶意数据对目标服务器执行命令。

Spring Cloud Function 安全漏洞（CVE-2022-22963）通报

4月2日，国家信息安全漏洞库（CNNVD）收到关于Spring Cloud Function安全漏洞（CVE-2022-22963）情况的报送。成功利用此漏洞的攻击者，可在目标服务器远程执行恶意代码，进而控制目标服务器。Spring Cloud Function 3.0.0.M3-3.2.2版本均受漏洞影响。目前，Spring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。

Spring 框架远程命令执行漏洞安全公告

3月30日，国家信息安全漏洞共享平台（CNVD）收录了Spring框架远程命令执行漏洞（CNVD-2022-23942）。攻击者利用该漏洞，可在未授权的情况下远程执行命令。使用Spring框架或衍生框架构建网站等应用，且同时使用JDK版本在9及以上版本的，易受此漏洞攻击影响。目前，漏洞利用细节已大范围公开，Spring官方已发布补丁修复该漏洞。CNVD建议受影响的单位和用户立即更新至最新版本。

Apache Spark 命令注入漏洞安全风险通告

3月29日，奇安信CERT监测到Apache Spark命令注入漏洞细节在互联网上流传。Apache Spark是一种用于大数据工作负载的分布式开源处理系统。当Spark任务的文件名被攻击者控制时，‘Utils.unpack’采用命令拼接的形式对tar文件进行解压，存在任意命令注入的风险。成功利用此漏洞可实现任意命令执行。目前，此漏洞细节已在互联网上流传。鉴于此漏洞细节已公开，建议客户尽快做好自查及防护。

对抗篇

国内攻防演习 3 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 3 月，奇安信 Z-TEAM 团队共承接攻防演习服务 15 场，其中省级攻防演习 3 场，省级行业攻防演习 1 场，地市级攻防演习 2 场，客户自主攻防演习 9 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	58	62	82	33	79	173	1032

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分散，涉及的目标业务比较广泛，涵盖了专项任务、政务、金融和互联网企业等目标，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不足、内网弱口令及口令复用普遍等。具体情况如下：

1、外部应用漏洞仍是主要突破口

本月任务中针对不同行业的目标网络，外网应用漏洞利用仍是主要突破口。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 Spring 组件漏洞、Java 反序列化漏洞、Shiro 反序列化漏洞、未授权访问、log4j2 远程代码执行漏洞等，多因外部应用及系统组件更新不及时造成。这类问题给目标网络带来了严重的安全隐患。

2、弱口令仍是内网严重安全隐患

本月任务中目标内网弱口令和口令复用问题依旧比较突出，其依旧是实现内网横向拓展的主要手段，通过弱口令或口令复用可轻易实现对内网数据库服务器、安全设备、网管系统和域控等核心网络节点的拓展控制，为内网渗透拓展带来极大便利。

3、访问策略缺陷是严重的安全威胁

本月多个目标网络的业务系统存在未授权访问问题，未授权访问多因对外部接入的安全配置或权限认证相关策略设置存在缺陷。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，造成数据库或网站目录等敏感信息泄露，未授权访问漏洞利用已成为外部突破的重要途径之一。

4、 敏感信息泄露是严重的安全风险

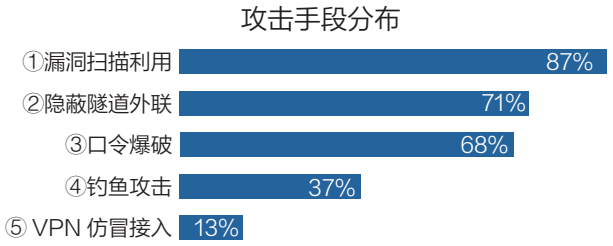
本月任务中目标网络敏感信息泄露较为严重，如内网 IP、内部文件、网站目录结构、应用源码、安全认证信息在内的敏感源码等泄露，这些敏感信息泄露原因多为安全配置疏漏、平台审核不严。此类敏感信息常常被用来实现针对性的快速突破及渗透。

5、内部业务网络缺乏纵深防御机制

本月任务中发现目标网络缺乏纵深防护机制。主要表现为从外部突破进入目标内网后，内网安全部署缺乏功能域划分、Vlan 隔离等措施，尤其是核心业务系统强防护或隔离措施极少。纵深防护机制的缺乏会导致目标核心业务安全防护非常脆弱。

三、主要攻击手段分析

基于本月奇安信 Z-Team 团队实战成果分析，对目标网络的外网突破，多采用互联网侧系统漏洞利用和钓鱼攻击实现，内网横向拓展则以隐蔽隧道外连、内网漏洞利用、水坑攻击、弱口令和口令复用等手段为主。使用的主要技术手段分布如下：



1、漏洞扫描利用

本月任务中漏洞利用主要集中在互联网侧应用或网络平台组件，被利用漏洞以网络组件反序列化漏洞、未授权访问、任意文件上传和 SQL 注入为主。这些漏洞主要是由于系统组件更新不及时、安全策略设置缺陷引起的，直接反映出客户网络运维人员安全意识不足、网络运维缺乏常态巡检机制、对存在的漏洞及安全威胁应对不够实时高效等问题。

2、隐蔽隧道外联

本月任务中因专项任务、金融对内网业务防守较为

严密，大部分客户目标系统网络无法通过外网直接访问，需要借助端口转发、隐蔽隧道技术等手段实现转发通信，对于网络功能区划分严格、核心业务隔离措施完善的内部网络，往往需要借助多层隧道转发才能实现对目标核心业务内网的渗透拓展。

3、口令爆破

本月任务中互联网侧系统应用弱口令情况比较少，但内网弱口令、口令复用情况依然严重。常见问题为未修改安全应用默认口令、多台设备管理员账户口令相同等。直接反映出目标网络对弱口令和通用口令缺乏统一监管，尤其是对账号口令复杂度设置和安全使用缺乏严格要求，口令爆破成为内网横向拓展的主要手段。

4、钓鱼攻击

本月任务中针对关键目标网络整体安全防护相对严密，外部系统难以直接突破的情况，钓鱼攻击成为另一种实现突破的主要手段，并且具有较高的成功率。外部主要从客户中安全意识相对薄弱的客服、人事等内部目标人员实现钓鱼突破，内网则通过水坑攻击对网络运维、平台研发及核心业务人员等目标钓鱼实现重点突破。

5、VPN 仿冒接入

本月任务中行业目标网络核心业务相对集中，对 VPN 入网范围限制较严，只有少量目标业务网络通过 VPN 仿冒接入实现渗透，利用手段包括外网通过 VPN 网关漏洞利用、内网通过口令复用获取VPN认证信息等。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某金融目标业务系统存在远程代码执行漏洞，通过漏洞利用获取数据库管理权限 3 个、ThinkCMF 服务器权限 3 台、敏感数据 2 万余条。

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

（3）某金融目标 OA 系统存在任意代码执行漏洞，通过该漏洞利用解密 OA 系统的数据库连接信息，获取数据库 1435 条可登录用户数据，并横向移动到 12 台 kubelet API 控制的容器，均可以 root 执行任意命令。

（4）某目标外部物质信息采集系统存在 CVE-2021-42278、CVE-2021-42287 漏洞，通过漏洞利用获取到大量服务器控制权限。

（5）某目标视频网大数据平台存在未授权访问漏洞，通过该漏洞可直接控制多台大数据平台终端和数据节点。

2、钓鱼攻击

（1）通过某目标监管平台找到客服 QQ 号，并添加该 QQ 号，发送钓鱼文件，成功上线 3 台机器。

（2）某目标针对客服钓鱼，获取客服业务服务器控制权限，成功进入目标内网。

（3）通过某目标官网招聘栏上找到的 HR 联系方式，添加微信向其投递木马文件，获取网站后台权限。

3、口令爆破

（1）某目标内网域控存在弱口令，通过弱口令控制域控后，同时可控制内网 8 个域控、13 台 Linux 服务器和 10 台 Windows 服务器。

（2）某目标统一权限管理系统存在弱口令，可直接登录该系统，查看用户名、电话、住址、角色等敏感信息。

（3）某目标外网业务工作培训平台存在弱口令，可登录业务后台并进一步拓展控制平台服务器。

（4）某目标业务人事系统存在弱口令，可直接访问并登录该系统，对内部人员档案信息进行查询操作。

4、VPN 仿冒接入

（1）通过对某学校进行水坑钓鱼，在成功上线的主机上 dump 出 VPN 账号、密码，并成功进入目标内网。

（2）某目标外网 VPN 网关存在 0day 漏洞，利用漏洞获取 VPN 网关控制权限，进一步通过 VPN 仿冒接入目标内网。

政策篇

国内，中央深改委审议通过《关于加强数字政府建设的指导意见》，要求强化数字政府安全管理。

国际上，俄罗斯总统普京签署总统令，禁止国家重要基础设施部门采购外国软件，以应对西方国家断供等安全威胁。

国内

中央深改委审议通过《关于加强数字政府建设的指导意见》

据新华社 4 月 19 日消息，中央深改委审议第二十五次会议召开，审议通过了《关于加强数字政府建设的指导意见》。会议指出，加强数字政府建设是创新政府治理理念和方式的重要举措，要始终绷紧数据安全这根弦，加快构建数字政府全方位安全保障体系，全面强化数字政府安全管理责任。

中办国办印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》

据新华社 4 月 18 日消息，近日，中共中央办公厅、国务院办公厅印发了《关于加强打击治理电信网络诈骗违法犯罪工作的意见》，对加强打击治理电信网络诈骗违法犯罪工作作出安排部署。《意见》要求，强化技术反制，建立对涉诈网站、APP 及诈骗电话、诈骗短消息处置机制；强化预警劝阻，不断提升预警信息监测发现能力；建立健全行业安全评估和准入制度；金融、电信、互联网等行业主管部门要全面落实行业监管主体责任，各地要强化落实属地责任，全面提升打击治理电信网络诈骗违法犯罪的能力水平。

《工业互联网专项工作组 2022 年工作计划》印发

4 月 13 日，工业互联网专项工作组办公室印发《工业互联网专项工作组 2022 年工作计划》，从夯实基础设施、深化融合应用、提升安全保障等方面，提出了 15 大类任务 83 项具体举措。安全保障强化行动方面，要求落实企业网络安全主体责任，加强网络安全供给创新突破，促进网络安全产业发展壮大，强化网络安全技术保障能力，开展企业网络安全能力贯标。

五部门印发《关于进一步加强新能源汽车企业安全体系建设的指导意见》

4 月 8 日，工信部、公安部、交通运输部、应急管理部与国家市场监督管理总局联合发布《关于进一步加强新能源汽车企业安全体系建设的指导意见》。《意见》提出，要健全网络安全保障体系，包括加强网络安全防护，强化数据安全保护，落实个人信息安全防护。企业要依法落实关键信息基础设施安全保护、网络安全等级保护、车联网卡实名登记、汽车产品安全漏洞管理等要求，履

行数据安全保护、个人信息保护义务。

证监会就修订《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》公开征求意见

4 月 2 日，证监会发布《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》修订版公开征求意见。修订版明确了企业信息安全责任，要求建立健全保密和档案工作制度，采取必要措施落实保密和档案管理责任，为境内企业境外发行证券和上市活动中境内企业、有关证券公司、证券服务机构在保密和档案管理方面提供更清晰明确的指引。

美国食品和药物管理局发布医疗器械网络安全指南草案

4 月 8 日，美国食品和药物管理局（FDA）发布《医疗器械网络安全：质量体系考虑和上市前提交内容》指南草案并公开征求意见。本指南草案旨在进一步强调确保设备设计安全的重要性，在整个产品生命周期中减轻新出现的网络安全风险，概述了 FDA 对上市前提交内容的建议，以解决网络安全问题。本指南草案将取代 2018 年发布的老版指南草案。

美国国会通过《国家网络安全防范联盟法案》

4 月 7 日，美国《国家网络安全防范联盟法案》先后获得参议院、众议院的一致通过，后续将提交总统签署生效。该法案为国土安全部授权，与美国全国大学培训项目联盟等国家网络安全防范联盟团体合作，共同推动网络安全事件响应与预防，为各州及地方政府、应急人员、行业利益相关方及关键基础设施所有者提供跨领域的网络安全培训。

日本《个人信息保护法（2020 年修订版）》正式施行

4 月 1 日，日本《个人信息保护法》最新修订版（2020 年 6 月）正式施行。2020 年修订版明确了国家和地方公关团体的责任、义务和保护措施，规定了信息处理者的义务、行政机关和个人信息保护委员会的职责等，旨在实现日本国家层面法律的统一化和形成地方公共团体的共同规则，通过个人信息保护委员会进行统一监管。

普京签署总统令，禁止国家重要基础设施部门采购外国软件

3 月 30 日，俄罗斯总统普京签署保障技术独立性的第 166 号总统令《关于确保俄罗斯联邦关键信息基础设施技术独立和安全的措施》，要求从 3 月 31 日起，禁止在国家采购中未经相关部门许可，为重要国家基础设施部门购买外国软件。从 2025 年开始，国家重要基础设施部门将完全禁止使用外国软件。

欧盟发布《网络安全条例》和《信息安全条例》提案

3 月 22 日，欧盟委员会发布《信息安全条例》提案和《网络安全条例》提案，旨在加强其面对网络威胁事件的反应能力，确保欧洲公共行政部门安全。《网络安全条例》旨在建立一个网络安全领域的治理、风险管理和控制框架，并加强 CERT-EU 职能。《信息安全条例》旨在为所有欧盟各机构、机关、办事处制定一套最低限度的信息安全规则和标准，以在信息威胁不断演变的情况下为它们提供有力与一致的保护。

政策解读

美国《2022年关键基础设施网络事件报告法案》要点概述

作者 史蒂文·斯特兰斯基，资深律师、曾任美国总统国家安全委员会副法律顾问

编者按

我国《网络安全法》《关键信息基础设施安全保护条例》都规定了运营者报告网络安全事件的义务，但目前还没有具体的落实文件。网络安全事件报告制度该如何设计？美国近期颁布的《2022年关键基础设施网络事件报告法案》可作为参考。《网安26号院》编译了资深网络安全律师史蒂文·斯特兰斯基的解读文章，以飨读者。

美国政府官员在俄乌战争的背景下发出警告，称莫斯科或其他黑客激进主义团体有可能加剧其恶意网络活动，对美国及本地市场造成直接或间接影响。为回应此种焦虑，以及近年来显著增多的网络攻击事件，美国国会已通过一项法律，即《2022年关键基础设施网络事件报告法案》（以下简称《法案》），要求私营部门遭遇网络安全事件或勒索软件支付时向网络安全和基础设施安全局（CISA）提交报告。该《法案》已被纳入《2022年综合拨款法案》，并在3月15日由拜登总统签字生效。

国会授权CISA起草并实施相关规章，以确定《法案》适用性和应用范围。根据《法案》要求，CISA应该在24个月内就规章制定一事发布初步通知，并在初步通知发布后的18个月内出台正式规章。需要注意的是，CISA在规章制定过程中不得对《法案》中提及的重要报告门槛、责任保护、合法特权保障及审管限值等要素进行替换。这些要素的设计初衷，是鼓励对法律的遵从度，提高网络事件报告的数量及质量。

对网络安全事件及勒索软件攻击的相关定义

根据《法案》的规定，遭受“网络事件”或实施“赎金支付”行为的实体，负有提交正式报告的义务。网络事件的定义，是指危及信息系统、数据储存或数据传输的完整性、机密性或可用性的重大安全事件。其应用范围仅限于非法行为，应信息系统所有者或运营者要求进行的渗透检测或漏洞扫描等（善意）网络活动，无需报告。CISA制定的规章应该描述出哪些网络事件会触发上报机制，并应要求对该规章实施执行。理论上，触发上报机制的**网络事件**至少包括以下网络攻击活动：

1 对某信息系统的机密性、完整性或可用性造成巨大损失的（网络攻击活动）；

2 对操作系统的安全性或弹性构成严重影响的（网络攻击活动）；

3 对市场或工业活动形成干扰的（网络攻击活动），如拒绝服务型攻击或0day漏洞攻击；

4 造成对信息系统的非法入侵或给市场或工业活动

带来负面影响的供应链攻击，如对云服务提供商或管理服务提供商的攻击。

“赎金支付”行为，是指“作为与某次勒索软件攻击相关联的赎金，对任何类型的货币、财物或有价财产（包括虚拟货币）在任何时候进行的转交活动”。“勒索软件攻击”是指实际使用或威胁使用恶意软件或类似网络攻击工具冲击信息系统、损害数据储存或传输以获取赎金的行为。与隐秘网络事件相同，“勒索软件攻击”也不包括根据信息系统所有者或运营者要求进行的善意网络活动。

适用范围

只有被 CISA 指定为“**涵盖实体**”的团体，才适用于《法案》规定的网络事件及勒索软件报告条款。涵盖实体可以是 16 个关键基础设施行业（如化学、制造、医疗、防务承包、能源、金融、核能、运输等）中的任何企业，且被 CISA 认定为符合法律规定的“其他标准”，包括：

- 该实体遭受网络攻击破坏后是否会影响国家安全、经济安全或公共医疗体系；
- 该实体被恶意网络攻击者锁定为目标的可能性有多高；
- 该实体及其攻击性网络安全工具遭受破坏后是否会扰乱其他关键基础设施的运营。

CISA 可能将在规章制定的早期阶段对涵盖实体进行指定，以便排除来自候选团体的意见干扰。

报告义务与时间要求

根据《法案》的授权，在有合理理由确认网络事件发生后，涵盖实体应该在 72 小时内向 CISA 提交报告。上述实体还被要求在发现与网络事件有关的最新或不同信息后，立即提交补充报告。另外，《法案》还要求涵盖实体遭遇赎金支付要求时，在 24 小时内向 CISA 提交

相关报告。

涵盖实体**提交报告的格式**由 CISA 负责制定，可能会与该机构正在使用的网络威胁信息共享平台格式相仿。《法案》已规定了涵盖实体在所提交的报告中应该关注的内容、类别，如关于网络攻击的描述及任何与恶意攻击者有关的已确认信息；网络事件对市场活动的影响；被突破的网络安全措施及被利用的网络漏洞；网络攻击运用的战术、技术和程序；被破坏数据的类型；赎金要求及用于支付的虚拟货币或有价物品的类别；赎金支付指示；赎金金额。CISA 应该在此基础上确定报告包含的内容。

《法案》明确允许法律公司、保险公司和数据泄露响应顾问等**第三方代表涵盖实体提交上述报告**。任何第三方在代表涵盖实体交付勒索赎金时都必须提醒该实体负有依法报告的义务。需要指出的是，此类第三方顾问的服务合同通常会包括根据《法案》编定的标准声明，以使服务提供者能够达到此领域的合规要求。

根据《法案》的授权，无论谁向 CISA 提交网络事件或勒索赎金支付报告，涵盖实体都应该**保留与其报告义务相关联的证据**。CISA 将在以后的规章中对证据保留的范围和程度做出规定。鉴于证据保留是任何网络事件响应项目的关键环节，所以涵盖实体不必为此承担新义务。

责任保护与强制性执行

政府之所以寻求实施与网络安全和勒索软件有关的强制性要求，原因之一就是涉事团体一直以来都没有根据政府提出的自由裁量信息共享计划公开此类信息。

通常，涉事团体不愿意公开此类信息，是担心公开后反而被政府抓住本团体的违法证据（如支付勒索赎金的行为就是对制裁法案的违反）。鉴于此，《法案》引入了与其他信息共享方案类似的**责任保护条款**。《法案》的主要支持者、参议员马克·沃尔纳表示，涵盖团体可根据《法案》享有“豁免权”，“我们不想让公司负责，”“我们想的是可以追踪恶意软件的来源。”沃尔纳说出了部分真话，因为《法案》中确实有依法针对涵盖团体的责任保护条款。但涵盖团体需要了解的是，这些责任保护条款是有很多限制的。

《法案》规定，因提交网络事件或勒索赎金支付报告而产生的案由，“不应该被任何人或团体保存在任何法庭”。不过该责任保护条款只适用于“基于提交上述报告产生的单一性诉讼”。《法案》还禁止（某些有限例外情况除外）联邦、州、地方或部落政府及机构利用从提交给 CISA 的网络事件或勒索赎金支付报告中获得的信息，实施针对涵盖团体的强制或其他执法行为。另外，《法案》规定了联邦机构出于其他非网络目的使用和公开 CISA 报告的场合，如反恐怖主义威胁、防止大规模杀伤性武器扩散等。

尽管有通用型责任保护条款的存在，《法案》仍允许 CISA 向司法部或其他合适的监管机构透露包含在网络事件或勒索赎金支付报告中的信息。随后，接收者会利用这些信息对不顺从的实体实施强制执行或犯罪起诉。不过，CISA 只有在（与司法部一起）向未遵守法案规定的强制报告要求的涵盖实体发出传票时，才能获得共享这些数据的授权。如果有实体胆敢视传票如无物，就会被扣上蔑视法庭的罪名。这样的规定可以让涵盖实体在违反法律时有激活责任保护条款的选择，进而鼓励他们遵守新的报告制度。

法律和证据特权

在针对网络攻击做出应急响应时，实体往往会依赖律师的指导和引领。这种方式可以更好地保证响应期间发现的信息和数据受到**律师 – 当事人特权**和**工作成果原则**的保护，从而避免遭到公开。

美国律师协会曾反复强调，“联邦机构迫使当事方公开受特权或工作成果原则保护的信息违反了存在已久的普通法原则，危及能够委以机密的律师与当事人之间的关系，以及律师享有的基本权利。”律师协会的观点非常适用于网络安全事件报告法案。《法案》非常重视法律特权问题。该法案认为，对网络安全事件报告的公开，

不应该构成对任何“法律规定的适用特权或保护特权”（包括律师－当事人特权和工作成果原则）的放弃。

在法案的实施规章中，CISA 应该考虑采纳信息共享环境下的指导原则，明确特权保护原则适用于所有联邦或州法律和证据特权可能遭受侵犯的环境，明确被普通法承认的特权（如律师－当事人特权和工作成果原则）都应该受到保护。

重复报告和其他

CISA 指定的“涵盖团体”可能还同时受到其他联邦数据泄漏通知制度的约束（如监管防务承包商和医疗机构的制度），这可能导致网络事件报告重复现象的出现。

《法案》认识到这一点并试图通过建立“**网络事件报告委员会**”来避免。该委员会由多个联邦机构组成，有权力对要求各异的网络事件报告制度进行“协调、消弭冲突和促进一致”。另外，网络事件报告委员会还负有对现行网络报告法规（如 DFARS 252.204-7012、《健康保险便携性和现任法案漏洞通知制度》）进行分析，确保此类制度出现“相互冲突、重复或加重负担的要求”。

在《法案》的规划中，CISA 与其他有网络事件报告要求的联邦机构之间应该存在一种机构间协议，并有明确条款保证 CISA 能够及时获取其他机构的网络事件报告。这一点意义重大，因为《法案》规定，按照法律要求或合同约定向联邦机构（非 CISA）提交网络事件报告和勒索赎金支付报告的涵盖实体可不再向 CISA 提交有关此类事件的重复性报告。

这一规定旨在避免重复性工作，但其实现是有前提的。首先是 CISA 必须与其他联邦机构建立起信息共享机制，其次是向其他联邦机构提交的报告在时间要求和内容要求两方面与《法案》的要求相同。鉴于目前网络事件报告制度的多样性，联邦政府机构有必要对本机构的制度进行修订，使其与《法案》保持一致。这样才能最大限度地减轻私营部门的报告负担。 安

栏目主编　李建平

美政府网安
投资揭秘

美国政府 2023 财年网安预算重点关注关基保护、零信任转型及网军能力建设。

增长 11%！美政府 2023 网安预算解析

作者 虎符智库专家 叶蓬

美国时间 3 月 28 日，白宫公布 2023 财年美国联邦政府预算提案，在总共 5.8 万亿美元的预算中，民事机构 IT 建设预算 650 亿美元。其中，包括约 109 亿美元的民事机构网络安全资金，用于包括联邦 IT 和国家最有价值的信息（包括美国公众个人信息），比 2022 财年支出增长 11%。2022 财年这一数字为 98 亿美元（比上年增长 14%）。

此外，美国国防部申请了 112 亿美元的军事网络空间行动预算，以对抗恶意的网空行为体和网空行动。比 2022 财年的 104 亿美元有所增加。

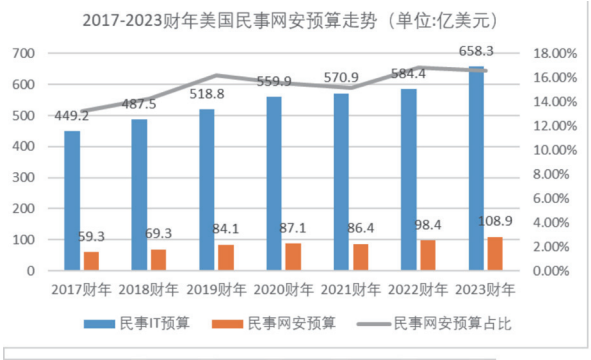
2023 财年，民事与军事两项网络安全支出合计 221 亿美元。2020 财年是 174 亿美元，2021 财年是 188 亿美元，2022 财年是 201 亿美元。

一、政府民事机构网安预算创新高

2023 财年，美国政府民事机构网络安全的预算比上一年增长了 11%，创下近几年之最。

同时，民事网安预算占整个民事 IT 预算的比重达到了 16.5%，总体呈上升趋势，并创历年新高。

下图展示了根据笔者自己收集的数据所作的统计。



二、政府行政令推动预算大幅增长

在其发布的网络安全预算专项分析报告中，白宫列举了近几年来颁布的重要法律法规，以支持该项预算大幅增长的原因。

这些法律法规包括：

1.2021 年 5 月的 14028 号总统行政令《改善国家网络安全》。该行政令要求重视和改善政府和私营部门间的信息共享，以增强政府和私营部门的网络安全。同时要求采购相关软件，改进对联邦系统的网络威胁和漏洞的检测，并增强美国在针对网络安全事件的响应能力。该行政命令还提出了采用零信任原则作为实现联邦政府对系统和数据保护现代化的关键举措。

2.2022 年 1 月，美国行政和预算管理局（OMB）通过了 OMB 备忘录 M-22-09《推动美国政府实现零信任战略和行动计划》。该备忘录制定了一项多年度计划，要求在 2024 财年末达到特定的网络安全标准和目标。

3.OMB 备忘录 M-21-30 为机构发布《通过加强安全措施保护关键软件的指南》。该指南要求机构清点关键软件，以确保软件供应链安全，并保护软件在机构运行环境中的使用。

4.OMB 备忘录 M-21-31《提升联邦政府应对网络安全事件时的调查和补救能力》。要求机构实施安全日志记录措施，以更好地了解潜在威胁，加快事件响应工作，以便更有效地对联邦机构进行防护。

5.OMB 备忘录 M-22-01《通过 EDR 提升对联邦政府系统的网络安全漏洞与事件的检测》。要求机构对所有端点设备（如电话、桌面 PC、打印机、笔记本 PC 等）实现实时的持续监测与响应。

此外，预算还体现了供应链风险管理、加大网络安

全劳动力建设等方面的努力。

三、民事网安预算组成分析

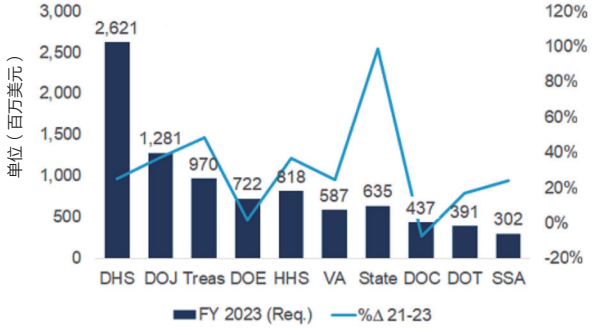
进一步分析民事网安预算的构成，如下表所示：

美国联邦民事机构网络安全支出（单位 百万美元）

机构	FY2021	FY2022	FY2023
民事 CFO 法案机构	$8,173	$9,387	$9,387
农业部	$223	$239	$239
商务部	$472	$422	$422
教育部	$165	$225	$225
能源部	$711	$793	$793
卫生与人口服务部	$598	$715	$715
国土安全部	$2,097	$2,409	$2,409
住房与城市发展部	$81	$76	$76
司法部	$934	$1,241	$1,241
劳工部	$109	$105	$105
国务院	$320	$447	$447
内务部	$124	$144	$144
财政部	$653	$829	$829
交通部	$334	$345	$345
退伍军人事务部	$472	$450	$450
环保署	$28	$29	$29
联邦总务署	$80	$78	$78
航空航天局	$155	$$187	$$187
国家科学基金会	$244	$256	$256
美国核管理委员会	$27	$25	$25
联邦人事管理局	$44	$44	$44
联邦中小企业局	$17	$17	$17
社会保障总署	$243	$266	$266
国际开发署	$44	$43	$43
非 CFO 法案机构	$468.5	$454.7	$454.7

可以发现，2023 财年，美国国土安全部（DHS）的网安预算高达 26.2 亿美元，位居所有民事政府机构之首（除了 DOD），占比为 24%；其次是司法部（DOJ），网安预算为 12.8 亿美元。这两个部门网安预算高的关键原因是，这笔预算不仅用于自身的网安建设，更主要的是服务于整个国家，承担美国民事网络安全防护的主要职责。

2023 财年网络安全预算 Top10 民事部门



来源：美国管理和预算办公室 (OMB)

下属的 CISA（网络安全与基础设施安全局）作为联邦政府掌握、管理和降低国家网络和物理基础设施风险的主责部门，提出了 25.1 亿美元的预算申请，其中，纯网络安全预算申请为 15 亿美元，占整个 DHS 的 26 亿美元网安预算的 58%。

这 15 亿美元中的主要项目包括：

- **4.07 亿美元用于 NCPS**（也叫爱因斯坦计划，相当于外网态势感知），与去年预算基本持平，累计已经投入了 32 亿美元，其中运营与建设的比例升到了 3.5:1，基本以运营为主了。值得一提的是，借助《美国救援法案》，CISA 计划投入 2100 万美元对爱因斯坦计划进行扩展，让 NCPS 采集和分析新的数据集（如 EDR、保护性 DNS），并将其命名为 MSEE（使命系统工程环境）。目前，NCPS 的主要供应商是雷神和 BAE。
- **4.25 亿美元用于 CDM 计划**（相当于内网态势感知），比去年增加了近 1 亿美元，包括了今年新增的针对联邦民事机构的高优先级主机和终端实施 EDR 项目的 7300 万美元。CDM 累计已经投入了 15 亿美元，2023 财年的预算运营与建设比例在 1:3.6，也就是说 CDM 主要处于建设阶段。此外，2023 财年的 CDM 预算中，网络安全管理的预算（包括边界保护、安全运营等）达到了 1.2 亿美元，比去年增加了 8000 万美元。目前，CDM 的主要供应商是 BOOZ ALLEN HAMILTON，CGI 和 CACI。
- **1.47 亿美元用于 2021 年 8 月新成立的 JCDC（联合网络防卫协作组织）**，支持其制定面向公私实体的网络防卫计划。
- **威胁狩猎的运营与支撑预算达到 2.22 亿美元**，相较于去年增加了 6300 万美元。
- **新的 SCuBA 项目，预算 2700 万美元**，包括开发 eVRF（可扩展可见性参考框架）（如日志记录、SOC 监测、审计优先级排序）；设计安全云业务应用（Secure Cloud Business Applications）的政府运营技术参考架构与指南，以识别支撑安全运营（如威胁猎捕、事件响应、安全监测）的云监测能力。

另一方面，根据司法部的预算，将有 12.8 亿美元用于网络安全，再创新高；美国联邦调查局（FBI）和美国

检察署都申请了专门的网络安全预算，以打击网络犯罪。其中，包括近 1.5 亿美元的网络计划用于加强对联邦机构的保护以免受网络威胁，识别网络攻击者并最终将其绳之以法。

如果将 2023 财年的民事网安预算映射到联邦政府采用的 NIST 的 CSF（网络安全框架）的 IPDRR 五个部分，则分布如下：

NIST 框架功能资金合计（百万美元）

（NIST FRAMEWORk FUNCTION CIVILIAN CFO AGENCY FUNDDING TOTALS）

NIST 框架功能	2022 财年	2023 财年
发现	$2,891	$3,469
保护	$3,617	$4,741.3
检测	$1,106	$1,483.8
响应	$1,485	$1,208
恢复	$289	$410.6
合计	$9,387	$10,890

分析不包括国防部支出

四、军事网安预算 IT 占比超 20%

根据美国国防部（DOD）的预算概览，2023 财年的网空战略目标是：提升联合部队的网络弹性，能够在争议环境（contested environment）下达成使命；通过实现零信任架构增强 DoD 自身的网络安全；保卫美国的关键基础设施，确保国防信息系统免受恶意网络攻击。

在 2023 财年，DOD 申请的网空安全预算达到 112 亿美元，高于去年的 103 亿美元，增长了 8.7%。同时，结合近 7 年的美国网安预算，可以发现，每年的美国整体网安预算中，军事网安预算始终高于民事网安预算。

这 112 亿美元的预算内容主要包括：实现跨军事部门和国防机构的零信任架构实战化（Operationalize），增强网络司令部（CYBERCOM）对网空计划与能力的采办角色，通过试点项目和服务增加对国防工业基础（DIB）的网络安全支持，将网络使命部队（CMF）从 137 支增加到 142 支（增加 5 支），为网络司令部从 2024 财年开始具有网络使命部队（CMF）的预算资源做好准备。

对此，国防部长评论道：“我们正在开发新的作战概念，将美国战争方式带入 21 世纪”。

目前，美国国防部尚未公布 2023 财年的 IT 预算，因此尚不能得知 2023 财年美国政府总的 IT 预算。

但根据 2021 财年的预算，2021 财年总网安预算占总 IT 预算比重为 20.4%，军事网安预算占军事 IT 预算比重为 25.6%。根据 2022 财年的预算，总网安预算的 IT 预算占比约为 20.8%。

鉴于这几年来民事网安预算总量和占比持续增长，笔者估计，2023 财年军事网安预算的占比一定也是增长的，而总的网安预算占总 IT 预算的比重应该超过 20%。

美政府网安预算三大投资重点

作者 虎符智库 李建平

美国政府 2023 财年预算表明，网络安全仍是联邦政府的首要任务。预算还继续强调 2021 年 5 月开始推进的零信任安全战略。

在联邦民事机构网络安全支出中，负责关键设施网络安全的国土安全部的网络安全和基础设施局 (CISA) 获得的资金最多，这表明对关键设施网络安全防护将持续加强。

网安仍是美政府工作的重中之重

美国政府 2023 财年预算文件称，网络安全仍是当务之急，因为对手持续寻求新的创造性手段来破坏联邦系统。

美国政府已经聘请了来自全国的顶级网络安全专家为其制定新的安全路线，探寻彻底革新保护联邦信息系统安全的方法。

预算文件指出，“网络威胁已对政府的关键服务构成最大风险，政府致力于解决根本问题，并采取转型措施推动联邦网络安全的现代化。”

文件补充说，拟议的投资“将根据政府的优先事项，专注于解决根本的结构性问题，促进联邦机构之间加强合作和协调，并解决阻碍政府技术愿景的能力挑战。”

美国众议院国土安全委员会资深共和党议员约翰 · 卡特科认为，预算对网络安全的关注自然不足。“这一预算要求在一年前是值得称赞的，但当前的网络威胁形势已经发生了巨大变化，显然需要更多资金。”

关基保护是网安投资重点

在俄乌冲突的背景下，美国总统拜登近期要求关键基础设施所有者和运营者，提高网络安全能力并增强网络弹性。事实上，拜登一直要求将联邦政府的网络安全提高到创纪录的水平，以兑现其政府关于美国网络防御现代化的承诺。

2023 财年预算计划向联邦民事机构拨款的 109 亿美元网络安全资金，比 2022 财年的 98 亿美元增加了 11%。国土安全部的网络安全和基础设施局 (CISA) 从这一支出增长中受益，将获得高达 25 亿美元的预算元，比当前预算增加近 5 亿美元。

这笔资金应有助于改善对联邦基础设施和服务交付的保护，以抵御复杂的网络威胁，包括维持《2021 年美国救援计划》实施的关键网络安全能力，扩大网络保护能力，覆盖所有联邦行政部门，并增强云业务应用、增强分析和利益相关者参与等支持能力。

这笔预算将（为 CISA) 提供 10 亿美元用于增强网络风险分析能力，加强联邦政府网络的安全态势，并提供保护 IT 基础设施的集成系统。

2023 财年预算还将帮助美国国家网络总监办公室，“应对政府和关键基础设施不断升级的网络攻击”，改善“国家协调能力”。除了《2021 年基础设施法案》获得 2100 万美元的启动资金，预算还将为其提供 2190 万美元。

目前，网络攻击威胁到政府向公民提供服务的能力，并可能影响经济、医疗保健提供者和系统、国防系统、电网、公用事业和其他关键基础设施、道路和高速公路系统、食品检验系统及介于两者之间的一切。这是美国积极为国防、基础设施和 IT 保护，加强立法和提供资金支持的重要原因。

此外，预算中还有 3 亿美元专门用于技术现代化，

旨在使联邦机构的 IT 系统现代化。联邦机构存在各种历史遗留系统：过时版本的 Windows 和其他不再接收安全补丁的软件系统，都无法得到充分保护，免受网络攻击。这些资金将尽可能实现系统的现代化。

美国网络联邦紧急事务管理局（FEMA）也将从联邦预算中获得相关资金，用于资助各州和地方政府及寻求改善网络安全的关键基础设施机构。

持续推动零信任架构

在美国联邦政府为民事机构申请的 2023 财年 109 亿美元网络安全资金中，一大部分将用于支持联邦机构转向零信任架构，以帮助联邦机构更快速检测、隔离和响应网络威胁。

零信任代表网络防御理念的转变，意味着转向更全面的 IT 安全模型，在不牺牲性能和影响用户体验的同时，使机构对网络、应用和环境的访问进行控制，从而可以提高安全性。

白宫要求所有联邦机构制定具体计划，在 2024 财年年底前部署零信任架构。美国管理和预算办公室（OMB）在 2022 年 1 月发布的零信任战略备忘录，为各联邦机构设立了最后期限，要求在 2024 财年年底之前，明确建立零信任架构的具体实施目标。

美国管理和预算办公室（OMB）发布零信任战略时，各机构已基本敲定了所需的预算，但 OMB 表示，将与各机构合作，以确保预算包括零信任能力所需的资金。

作为实施零信任计划的一部分，各联邦机构将在计划中明确实施零信任计划的里程碑。例如，根据备忘录，实施计划应明确 “计划隔离其应用和网络环境”的方式和时间。

除了 2024 财年目标，OMB 备忘录还设定了一些具体截止日期。例如，在一年内，各联邦机构的所有面向公众的服务，必须支持防网络钓鱼的多因素身份验证。

在 2023 财年预算中，一些美国联邦机构包含了更详细的零信任计划。

例如，商务部在 2023 财年预算中，申请 5000 万美元专门用于零信任计划。根据预算文件，这笔资金用于提升终端检测和响应能力、统一的日志管理和端点加密。

财政部要求在 2023 财年获得 2.1 亿美元用于网络安全，其中约 8600 万美元，专门用于零信任架构的实施。根据预算文件，财政部的近期建设规划包括“更改密码政策、建立新的数据分类模型，以及使‘内部’系统可以通过互联网访问”。

此外，2023 财年预算计划向国防部拨款 112 亿美元用于网络空间建设，其中同样包括在所有军事和国防机构实施零信任架构，以保护网络和数据。

国防：对抗中国的网络能力

在国防部副部长办公室发布的《国防预算概要》强调，2023 财年预算支持和实施新的国防战略，其中将中国列为其主要战略竞争对手。2023 财年的资金将优先支持应对中国与俄罗斯在太空、核与网络方面的能力。

美军 2023 财年网络空间方面的主要战略目标包括提高联合部队的网络弹性，保护美国关键基础设施并保护国防部信息系统免受网络攻击，实施零信任架构提升国防部网络安全等。

如前所述，2023 财年预算计划向国防部拨款 112 亿美元用于网络空间建设，超过民事机构的网络安全支出，这一数字比 2022 财年的网络支出增加了 8 亿美元，即近 8%；比 2021 财年增加了 14 亿美元。其中包括用于海军网络安全的 10 亿多美元，与 2022 财年相比增加了 2 亿多美元。

为了推进其在网络空间的目标，美国国防部计划增加对国防承包商的网络安全支持、强化自身网络安全能力、实施零信任架构、投资网络靶场，并增加五个网络司令部网络任务部队，使总数达到 142 个。网络任务部队成立于 2009 年，是网络司令部的“行动部门”，承担进攻和网络空间的防御任务。

分析人士认为，最终预算在获得批准前会经历许多变化，但对网络安全的投资增加将是确定的大概率事件。

头部网安企业财报分析：市值增长， 投资回报丰厚

作者 虎符智库 李通

通过对全球最大10家国际网络安全上市企业2021年资本市场和经营情况分析，可以看出，在新技术新场景推动下，上市公司市值持续增长，投资回报丰厚。

1、头部网安企业市值持续增长，长期投资者获得丰厚回报

截至2022年3月31日，美股企业网络安全2021最新财年营收前二十大的公司排名如下：

序号	公司简称	营收（亿美元）2021最新财年	总市值(亿美元）2022-03-31
1	PALO ALTO NETWOR	42.56	613.08
2	阿克迈技术	34.61	192.10
3	飞塔信息	33.42	549.57
4	F5网络	26.03	126.91
5	CheckPoint	21.67	183.61
6	CROWDSTRIKE	14.52	477.00
7	OKTA	13.00	226.02
8	ZSCALER	6.73	340.41
9	CLOUDFLARE	6.56	333.34
10	TENABLE	5.41	63.44

注：相关数据主要来自各企业最新财年信息，由于美股财年起止日期不统一，部分企业最新财年横跨2021—2022年度，本文统称为2021最新财年数据。

2022年3月31日，10家企业的市值达到3105.48亿美元，较上年同期增长45.1%，大幅跑赢纳斯达克指数的13.34%涨幅。拉长来看，10家网络安全企业的股价表现也同样强劲，过去三年增长134.06%，对长期持有者回报颇丰。

资本市场的靓丽表现是对网络安全行业快速发展的积极肯定。根据各企业2021最新财年数据，前10大企业的收入合计达到204.52亿美元，同比增长22.99%，对应3月31日收盘价，估值指标PS（静态）达到15.18倍。不过，与收入持续高速增长相背离的是行业净利润率由5%进一步下滑至-1%，行业内部不同企业之间差异很大。但总体来看，行业净利润的短期下滑并未导致投资者大面积丧失信心。这可能是由于美股投资者更关注企业长期的市场空间潜力和竞争力提升而非当期净利润。

2、新技术新场景和国际化收入持续提升

新技术新场景带动网安需求升级。财报中并没有详细披露细分领域收入情况，但从高速增长企业的业务布局和优势产品来看，云安全、零信任、SASE、SOAR和身份管理等技术方向的厂商仍是网络安全领域高增长的领头羊，相关企业持续高速增长，如云安全龙头Crowdstrike、零信任龙头Zscaler、SASE和SOAR等综合性龙头厂商Palo Alto、身份管理龙头Okta等。

国际化持续推进，全球市场收入已成为重要组成部分。在披露收入地区分布的9家公司中（除Check

序号	公司简称	营收	营收增速	销售费率	管理费率（注）	研发费率	净利润率
1	PALO ALTO	42.56	17.55%	41.21%	9.19%	26.79%	-11.72%
2	阿克迈技术	34.61	10.52%	13.35%	15.98%	9.69%	18.83%
3	飞塔信息	33.42	19.94%	40.27%	4.31%	12.69%	18.16%
4	F5 网络	26.03	4.83%	35.72%	19.70%	19.19%	12.72%
5	CheckPoint	21.67	3.51%	27.60%	5.12%	13.25%	37.6 d4%
6	CROWDSTRIKE	14.52	81.64%	42.50%	21.84%	25.58%	-16.18%
7	OKTA	13	42.55%	59.22%	33.15%	36.09%	-65.25%
8	ZSCALER	6.73	42.41%	68.19%	14.41%	25.95%	-38.93%
9	CLOUDFLARE	6.56	50.18%	49.97%	18.28%	28.85%	-39.66%
10	TENABLE	5.41	24.15%	49.90%	16.63%	21.52%	-8.63%

注：本文管理费用是指美国会计准则中的一般和行政支出

Point 外），2021 最新财年国际收入合计达 82.25 亿美元，相比两年前的 51.47 亿美元增长 59.8%，收入占比由 43.29% 提升至 44.98%。

3、头部企业大部分实现盈利，成长企业高研发高增长

从 10 家企业的财务表现来看，可以根据收入排名将其分成两类。第一类是头部企业（前 5 名），收入大于 20 亿美元，呈现稳步增长态势，且大部分已经实现稳定盈利。第二类是高成长企业（后 5 名），表现为收入高速增长，但由于扩张期间投入大量资源加强研发和销售，积极抢占市场，企业普遍还处于亏损阶段。

头部 5 家企业中已有 4 家实现稳定盈利，分别为阿克迈、飞塔信息、F5 网络和 Check Point，其 2021 最新财年平均净利润率高达 22%。Palo Alto 仍处于亏损阶段，2021 最新财年净亏损由去年的 -2.67 亿美元扩大至 -4.99 亿美元，比例由 -2.82% 扩大至 -7.83%。这主要是 Palo Alto 持续积极扩张，包括大幅提升研发费率 4.25 个百分点至 26.79% 等，但公司也更多采用股份支付方式，股权相关薪酬由 6.65 亿美元增长 39.4%，达到 9.27 亿美元。因而扣除其影响的现金流表现更加强劲，其非公认会计准则下的自

指标	平均毛利率		平均销售费率		平均管理费率		平均研发费率		平均净利润率	
年度	2019	2021	2019	2021	2019	2021	2019	2021	2019	2021
头部企业	77.58%	75.87%	33.69%	31.63%	11.02%	10.86%	14.06%	16.32%	17.90%	15.12%
成长企业	76.89%	75.74%	57.86%	53.96%	21.97%	20.86%	26.14%	27.60%	-27.87%	-33.73%

由现金流由去年的 8.21 亿美元，大幅增长 68.94% 至 2021 最新财年的 13.87 亿美元。因此，净利润亏损扩大，但从自由现金流来看公司发展向好趋势非常明显。

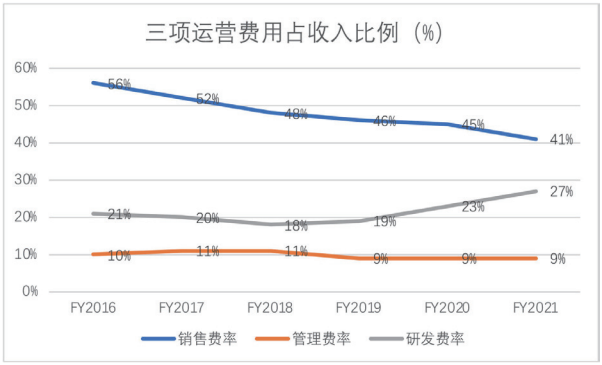
纵向比较高成长企业的各期盈利能力来看，各项费用比例已出现明显改善趋势。过去两年，平均销售费率下降 3.9 个百分点，管理费率下降 1.11 个百分点。平均研发费率和净利润率出现恶化，主要是 Okta 2021 年积极扩张，将员工由 2806 人大幅扩增至 5030 人，导致运营开支大涨，净利润率由 −32% 暴降至 −65%，扣除其影响后，平均净利润率为 −25.85%，相比两年前和三年前分别收窄 0.08、10.78 个百分点，改善明显。但横向与头部企业相比，高成长企业的销售费率、管理费率，研发费率仍然明显高出很多，分别高出个 22.33、10 和 11.28 个百分点，以此来看未来下降空间还非常大。

收入高增的同时研发和销售费用高企，这是成长期公司典型的财务特征。预计未来随着收入的持续高速增长，企业扩张将进入平稳增长期，规模效应也会开始凸显，财务表现会逐步向头部企业靠拢，即各项费率明显下降，盈利能力大幅提升。另外，值得一提的是，从美国资本市场经验来看，这类企业对投资者回报也是最为丰厚，5 家企业复权后的股价自 IPO 以来涨幅分别高达 5.68、7.88、14.08、6.98、1.51 倍，年化复合增长率对应为 97.44% 、54.77% 、95.69% 、126.41% 和 28.53%。

4、代表性企业分析

（1）Palo Alto

Palo Alto 是下一代防火墙的龙头，于 2005 年成立于美国，2007 年公司首先提出下一代防火墙概念，但公司 2017 年之后开始转型升级，持续加强在云安全、安全运营等方向的投入，目前，公司已经形成企业安全平台（Strata）、云安全平台（Prisma）和安全运营平台（Cortex）三大安全平台，能够为用户提供从端到云的整体解决方案。



得益于平台化战略顺利推进的规模效应，公司销售费率和管理费率逐渐下降。2021 财年，公司销售费率已经大幅下降至 41%，五年下降 15 个百分点，而管理费用则呈现小幅波动下降趋势。近三年来公司大幅提升研发费用比例，增强长期竞争力。研发费率由 2018 财年的 18% 提升至 27%。

公司基于对强劲的现金流和行业发展前景的信心，目前仍未选择在短期内实现盈利，2021 财年净亏损 4.99 亿美元，但非美国通用会计准则实现盈利 6 亿美元，主要是公司股权薪酬占比较高。此外，管理层预计公司未来三年收入复合增速可达 23%，将继续保持良好发展态势。

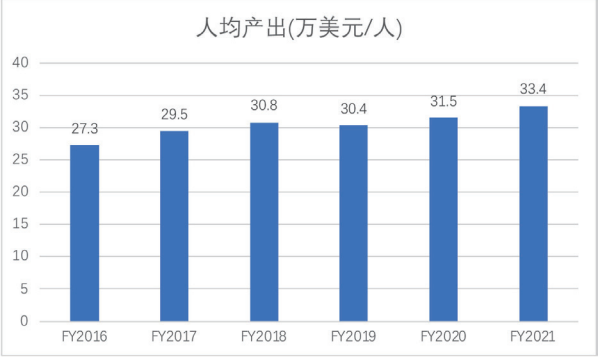
（2）Fortinet

飞塔是全球 UTM 技术的引领者。公司自 2000 年创立以来就致力于发展 UTM（统一威胁管理）技术，后续公司通过不断“自研 + 并购”，持续丰富公司产品线，加速扩大产品覆盖领域，打造出全覆盖的网安解决方案。公司 2021 财年实现营业收入 33.42 亿美元，同比增长 28.82%；净利润 6.52 亿美元，同比增长 24.22%。

与美股众多扎推云计算方向的公司不同，飞塔重点布局 SD-WAN 和基于 SDP 技术的零信任。美国云计算市场与中国完全不同，以公有云为主，孕育了大量云安全公司。但飞塔通过平台化产品战略也获得了成功。

积极推进产品体系平台化。平台对于拥有众多细分领域产品的网络安全行业非常重要，只有底层技术平台的统一才能够提供一揽子解决方案，但这需要将底层的产品研发打通。飞塔坚持创新，持续投入研发和销售，推出了兼具动保护、检测和响应功能的平台产品安立方（Fortinet Security Fabric），通过将公司专有的SPU 硬件架构、FortiOS 操作系统及相关的安全和络功能结合在起，形成了完整的服务平台。

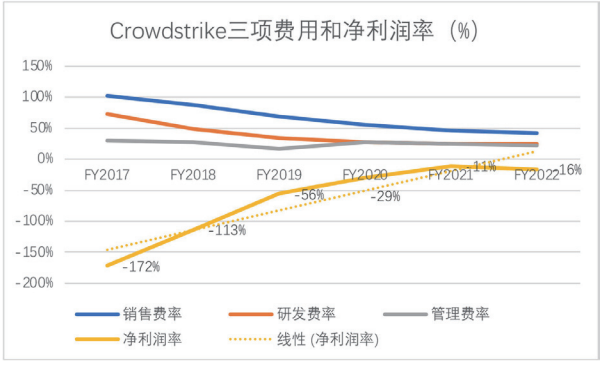
平台化的成功使得公司人均产出持续提升。公司在 2017 年发布安立方平台后，人均产出持续提升，由2016 财年的 27.3 万美元提升至 2021 年的 33.8 万美元。



（3）Crowdstrike

Crowdstrike 于 2011 年成立，它为下一代端点保护提供了云交付的解决方案，该解决方案通过基于SaaS 订阅的模型在其 Falcon 平台上提供了云模块。目前该公司提供四个类型的产品服务：终端安全、威胁情报、安全和 IT 运营及云安全。

单一产品向多模块发，提供了新一代网络安全平台。Crowdstrike 与传统的网络安全软件最大的不同，是它在单纯软件服务之外提供了新一代网络安全平台。2017 年之后，公司由单一产品向多模块发展，实现交叉销售和多模块集成订阅，覆盖端点安全、IT 运营、托管服务、威胁情报、云安全。Falcon 平台的功能模块灵活组合功能，让不同量级的公司可以选择最适用的



产品。CrowdStrike 同时覆盖大型企业和小型客户，美国的网络安全行业发展较为成熟，客户对产品的需求不限于自身的规模。CrowdStrike 基于自身的 SaaS 模式和多模块灵活组合的能力，使得公司客户覆盖面极广。平台的灵活性和可扩展性使公司能够无缝地向任何规模的客户提供解决方案——从拥有数十万个端点的客户到只有三个端点客户。

受益于模块化产品及开放平台，公司盈利能力持续改善。2017 财年以来，公司费用率持续下降，人均产出持续增长。2022 财年公司研发费用率下降为 43%；销售费用率下降为 26%；管理费用率为 22%，相比 2017 财年大幅下降。另一方面，公司员工数量和人均产出也保持较快增长，公司 2022 财年人员达到 4695 人，相比 2017 财年同比增长 7.53 倍，而收入同期增长 26.55 倍，人均产出提升 2.23 倍。公司 2022 财年亏损加大，净利率下滑 -5% 至 -16%，主要原因是公司当年积极扩张，人员大增 74%，而当期收入仅增长 66%，导致当期利润上表现较差，但从长期趋势线来看，扭亏为盈已经指日可待。 安

3.8 亿次网络攻击与冬奥“零事故”承诺背后的攻防博弈

作者 研究员 张少波

“这是一场不对称的战争。”

3.8 亿次网络攻击（含社会面）、上千个攻击者组织、数万起 APT 组织活动事件……

从攻击视角，和历届奥运一样，从冬奥会前准备，到冬残奥会闭幕式结束，为期 2 个月的时间内，针对北京冬奥的网络攻击从未间断。而在开幕式、闭幕式和重要赛事期间，攻击频次更密、强度更烈。

从防守视角，作为奥运史上首家网络安全赞助商，奇安信对冬奥做出了网络安全“零事故”的承诺，承担“完全、彻底、端到端”的责任，即“托底责任”。

一边是数以亿计的网络攻击，一边是“零事故”的保障承诺，这就如同足球场上的守门员，无论你有多少次精彩的扑救，只要有一次防守疏漏，就会导致丢球。这场冬奥网络安全保障任务的艰巨程度可想而知。

在这个看不见硝烟的网络空间战场上，一场场攻防博弈，一直在持续上演。

发现篇：“自动化”的天眼 让攻击发现更快一步

“聪者听于无声，明者见于未形”。提早发现、提早预警、以便提早处置，无疑是“零事故”的前提保障。这里，就不得不提在冬奥网络安全保障中无处不在的天眼。

“作为攻防态势感知，天眼更像是无数敏锐的‘眼睛’，它广泛部署在两个网络中心、两个数据中心、12

天眼网络安全态势大屏

个竞赛场馆、26 个非竞赛场馆，以及给冬奥提供网络及业务平台支持的多家运营商、合作伙伴、外部单位等，第一时间检测与发现任何的网络异常行为。” 奇安信冬奥保障总架构师尹智清表示。

可见，冬奥网络安全保障，首先离不开天眼的“广泛部署”，如同城市公共安全的摄像头一样，只有无死角、全范围的覆盖，才能避免有漏网之鱼。

仅有广度还不够，还要有发现和响应速度。凭借自动化流转的机制，冬奥中天眼大幅提高了威胁发现和处置效率。尹智清表示，“北京冬奥会共计使用 26 个竞赛场馆和非竞赛场馆，这些场馆分布在北京赛区、延庆赛区和张家口赛区。为了保障每个场馆内的网络安全，天眼部署在各个赛区，实时动态监测威胁，第一时间发现异常行为，形成告警，并自动同步上报到运营态势感知（NGSOC，即态势感知与安全运营平台）”。

整个冬奥会期间，天眼日均产生告警日志和流量日志逾 25 亿，其中告警日志传输给运营态势感知进行进一步的人工分析和研判。天眼检测威胁的整个过程大大降低对人的依赖度，实现完全自动化的流转。

得益于自动化处置威胁的模式，天眼对网络威胁发现的平均检测时间（MTTD）和平均响应时间（MTTR）得到了极大缩短。安全服务子公司白永帅分享了一个故事。“就在 2 月 5 日当晚，中国短道速滑队冲击混合接力冠军之时，各个直播转播系统流量激增。我们发现了一次对通信运营商系统的可疑攻击行为，凭借安服团队和天眼的珠联璧合，仅仅用时 8 分钟，就处理了这起安全事件。”

“冬奥‘零事故’背后不是没有安全风险，而是及时将风险扼杀在摇篮里。 天眼在日常运营中就像一只眼睛，可以从流量上帮助我们精准发现各种威胁，无论是针对 DGA 域名的 DNS 隧道攻击、还是 APT 攻击，天眼都能及时发现，自动同步上报，确保安全分析人员快速处理，才没有造成任何影响”，冬奥安全运营工程师初雪峰表示。

存储流量日志数 1074 亿条，发现真实网络攻击 5,008,746 次、安全漏洞数 9,135 个、恶意样本数 54 个……天眼作为奇安信冬奥指挥态势、运营态势、攻防态势“三合一”实战化态势感知中的重要组成部分——“攻防态势感知”，完美诠释了“天下武功、唯快不破”的攻防之道。

研判篇：看的清、看的透 白泽 + 天炬实现精确分类高效应对

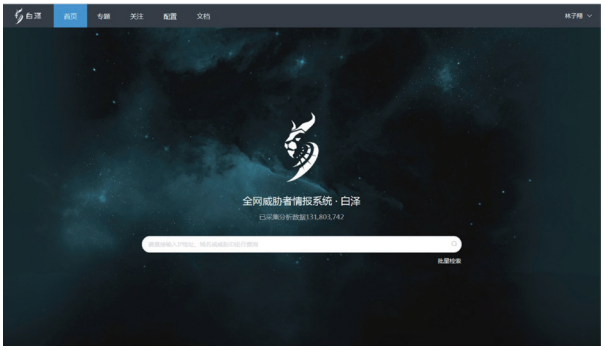
明枪易躲，暗箭难防。每一次攻击的背后，都有藏在暗处的“凶手”。然而 3.8 亿次网络攻击，平均每分钟 4400 次，如果没有强大的分析研判体系，应对这些海量攻击会让安全人员疲于奔命，将精力淹没在处理无效告警的海洋之中。冬奥期间，来自奇安信 A-TEAM 的白泽情报平台和天炬分析工具珠联璧合，为“零事故”立下了汗马功劳。

“面对海量的告警和攻击行为，我们不能仅仅满足于‘看见’，更需要对攻击者‘看清’‘看透’，这样才能正确掌握网络安全攻防态势，针对敌人开展工作才可以做到‘零事故，无担忧’。”在冬奥开幕式前期，作为奇安信冬奥网络安全保障的副总指挥，奇安信总裁吴云坤看到大屏上海量的告警信息，感受到了网络安全保障工作的艰巨。随即，他立即和 A-TEAM 团队召开电话会议，紧急部署工作，以解决数以百万记的告警难题。

“最难的是标记工作，并不是所有的攻击行为，都

是黑客的恶意入侵，所以不能‘一刀切’的简单粗暴式封禁处理。”A-TEAM 团队实战化态势总设计师林子翔表示，“我们要根据攻击行为数据，进行快速分析，区别出 APT 组织、黑帽子、白帽子，进而判断出威胁严重程度，制定相应的反制或预防措施。”

然而，要对所有（尝试）发起攻击的 IP 地址全部研判分级，从天量的告警事件找到真正需要关注的攻击者，并进行针对性预防和观测，并不是一件很容易的事情。奇安信的白泽云端攻击者情报平台，发挥了关键性作用。

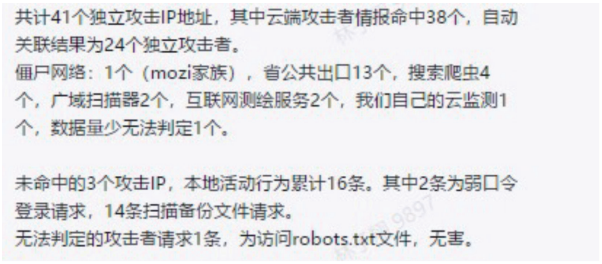


“在实际使用中，得益于白泽平台数年来积累的过亿量级的攻击者库，我们仅使用了 1 人 / 天，就把历史所有攻击来源 IP 完成了分级和分类。在开幕式前数以千万记的攻击中，快速筛查掉不需要关注的攻击主体，确定了 15 个高价值的攻击者。”

有了知识平台，还需要给分析员称手的工具。林子翔表示，“除了白泽平台，天炬是我们的本地流量告警分析工具。白泽和天炬两个结合可以达到 1+1>2 的效果，能够做到所有告警，无论是否成功 / 误报，都把最需要分析的事件和攻击者拎出来。从而把分析人员的精力放在最需要放的地方。”

据介绍，从正月初一到残奥会闭幕式，由于白泽多年的数据积累，每天研判增量攻击者仅需 1 个工时！这是对安全运营人员不可估量的精力解放。

研判分级之后，接下来需要针对不同类型的攻击主体，使用不同的弹性处理策略。“如果判断是僵尸网络等广域扫描器，我们就直接封禁来源 IP；对于一些友商的扫描测试行为直接下发通报；如果判断是境内的白帽子，会及时通告有关部门来跟进处理；而对于境外别有用心的 APT 组织，则协同相关部门采取反制措施。”



林子翔认为这些工作看似烦琐，但非常重要，“看清攻击者后，排除掉所有‘明面上’的攻击者，藏在黑暗处的‘未知攻击者’自己就会浮出水面。这时候安全工作就可以极具针对性，有的放矢。”

林子翔分享了一个故事：2 月 11 日，日常分析过程中，一组新出现的境外攻击 IP 引起了我们的注意。其攻击手段和历史攻击行为具有较强的针对性，有可能是境外高级黑客组织的前期侦查类活动。A-TEAM 团队立刻联系了冬奥现场安全运营组进行升级观测。2 月 12 日，在经过多方查证后，基本确认该组织为海莲花 APT 组织，其使用了多款自研的扫描工具和人工探测的方式尝试对冬奥相关设施进行渗透。由于奇安信在其前期阶段已经准确发现并识别，该组织的所有攻击尝试已经无法构成安全威胁，最终将该分析简报上报给国家有关部门。

整个冬奥期间，奇安信研判 IP 地址超过 5000 个，调查攻击者组织近千，100% 覆盖冬奥期间所有发起过攻击的攻击者。 经过对其过往的调查和总结，标记高价值攻击者和组织 50 余个，涉及 APT、黑帽子、白帽子等，同时预先发现了境外 APT 组织对我们的攻击试探，并成功实现反制和预防。

测试与情报篇：冬奥网络安全卫士与黑客赛跑、与漏洞赛跑

未知攻，焉知防？ 在冬奥网络安全保障的团队中，

除了奇安信3500位专业工程师，还有一支“神秘之旅”，行业内称他们为“白帽子”，他们就是冬奥网络安全卫士。

一辆汽车出厂之前，需要进行碰撞测试，同样，冬奥信息系统在正式运行之前，也需要经受各种苛刻的考验。而发动全民的力量，邀请民间白帽子进行攻防渗透测试，提前检查发现漏洞，无疑能为冬奥网络增强一道“保护锁”。招募冬奥网络安全卫士的重任，就放在了奇安信集团补天漏洞响应平台身上。

“刚一接触到冬奥系统，我就发现冬奥系统的测试难度非常大，这些系统经过前期科学的设计和严格的开发流程，以及各种黑白盒的测试，绝大多数漏洞都在上线前就被排查发现和修补了。不过越是如此，越是激起了我的好胜心与‘挑战欲’。功夫不负有心，通过不懈的努力，我终于还是发现了一些有效的安全隐患，并得到了组委会的认可。”

来自补天漏洞响应平台的白帽子 teachersday，目前在一家股份制银行做安全，擅长漏洞挖掘和攻防实战。他看到补天发起的招募活动，最终报名，并通过了层层筛选，成为冬奥网络安全卫士，在本次冬奥安全保障中，发挥了重要的作用。他的信条是：“作为中国的白帽子，我们绝不输给任何人。我们守护冬奥，绝不给破坏者留下可乘之机。”

奇安信集团董事长、奇安信冬奥保障团队总指挥齐向东这样评价，“网络空间是奥运会的另一个赛场，冬奥网络安全卫士是‘网络安全中国代表队’的奥运战士，通过和黑客赛跑、和漏洞赛跑，为北京冬奥会筑起坚固的网络安全防线，为守护冬奥荣耀贡献力量。”

3月16日，冬奥网络安全卫士总结表彰大会在奇安信冬奥网络安全保障指挥中心举行。来自国资委、国家卫健委、29家央企及鹏城实验室等单位的“冬奥网络安全卫士”获得表彰。中央网信办冬奥会网络安全专家研判组组长、中国工程院院士方滨兴表示，白帽子作为冬奥会网络安全的“测试员和情报员”，协助查找冬奥信息技术系统防护短板和漏洞，收集涉冬奥相关的威胁信息，发挥了重要作用。

此次冬奥网络安全卫士除了央企代表，还有一部分群体是在校大学生，鹏城实验室也组织16个校企单位、88名白帽子加入了冬奥网络安全卫士，表现优异。方滨兴院士表示，“这次白帽子大规模参加这么高级别的世界级赛事，足以说明白帽子群体是可信任、可管理的，同时更是有能力、有水平的。

据悉，经过层层选拔的冬奥网络安全卫士24小时在线，发起超过2000万次测试请求，测试总时长超过1万小时，成功发现了大量有效系统漏洞和冬奥相关威胁情报。

结束语：

“北京冬奥会做到网络安全‘零事故’，具有里程碑的意义。”方滨兴院士说道。北京冬奥组委专职副主席兼秘书长韩子荣也表示，“奇安信作为奥运会历史上第一家网络安全和杀毒软件的官方赞助商，筑起网络安全的铜墙铁壁，让北京冬奥会成为有史以来最安全的奥运会。”奇安信在冬奥“零事故”中积累的“中国方案”，更为国家关键信息基础设施保护和重大活动安保工作提供了实践经验。

3.8亿次攻击，研判IP地址超5000，调查攻击者组织近千，累计发现漏洞37908个，检测日志累积超1850亿……一组组数字的背后，是无数次的斗智斗勇、无数次的攻防博弈，更是3500位奇安信安全工程师，以及数百个冬奥网络安全卫士800多个日夜的坚守和配合。 安

零事故背后：揭秘 NGSOC 如何助力冬奥安全运营中心
——规划和建设篇

作者 安全运营 BG 张娜

2022 年 2 月 4 日至 3 月 13 日，北京顺利举办了第 24 届冬季奥林匹克运动会。时间拉回到 2019 年 12 月 26 日，北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商发布会在北京冬奥组委园区举行，奇安信正式成为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商。时至今日，已两年有余。从成为冬奥会赞助商，到以零事故的成绩圆满完成冬奥会安全保障，离不开从零开始搭建到流畅运转的冬奥安全运营中心。

提到冬奥安全运营中心，离不开一个贯穿全程的人，奇安信冬奥项目的总工程师尹智清，大家都叫他老尹。

“从 2019 年 12 月 26 日开始，奇安信正式成为北京 2022 年冬奥会和冬残奥会官方赞助商。” 回顾冬奥项目设计阶段，老尹提到，“早在 2019 年 3 月，冬奥项目的设计工作就已经开始。”由于 3 月份冬奥组委还没有正式发布应征文件，所以第一版设计方案并没有可参考的明确要求，其主要参考依据是奇安信多年的重保经验。

老尹说，当时参与做第一版方案的只有 3 个人，只能摸着石头过河。即便没有可参考的要求，这 3 个人的团队还是在 7 月份迭代了第二版方案。直到 2019 年 9 月份冬奥组委的应征文件正式发布，才有了明确的方案要求，也就是从那时候开始正式进入最终策划阶段。在数十人团队的共同努力下，直到最后中标，奇安信冬奥重保任务的第一阶段的正式完成。

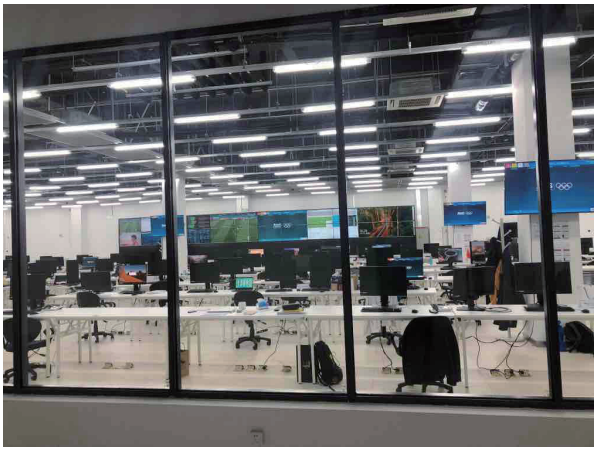
与以往重保不同的是，首先冬奥项目的网络安全建设耗时非常长，前后历时 2 年多。其次奇安信要全面承担冬奥会网络安全责任，从以往项目的甲乙方关系变成合作伙伴关系，这一点的转变非常关键，也给冬奥重保提出了更高的要求。

“冬奥组委对我们的最核心要求就是，要对冬奥会的网络安全承担完全的、彻底的、端到端的责任，最终目标就是零事故。”老尹说。

同步规划 同步建设 同步运营

在正式成为冬奥赞助商之后，项目也即将进入现场交付建设阶段。

“冬奥项目有数十家赞助商及第三方云上云下业务系统，涉及多个场馆，要保障冬奥项目全盘业务系统安全运行，就意味着，冬奥项目的网络安全建设要与多个业务系统保持同步规划、同步建设、同步运营，这也是项目初期最大的难点。”冬奥安全运营中心现场项目经理仝磊提到，几十个利益相关方要保持协同、进度计划适配、技术对接、系统联调，往往安全建设总是被安排在业务系统之后，还要面临着工期被压缩等诸多压力。不仅如此，在与有些业务相关方做技术对接的时候，还会遇到各种各样的“非技术性难题”。



入场后面临的第一个问题就是定位。冬奥安全运营中心在设计之初，包含三级指挥中心，即一个总指挥中心 + 三个赛区指挥中心 + 场馆指挥中心，但由于冬奥没有了赛区的概念，相应赛区指挥中心也随之取消，最终只有位于首钢园区的总指挥中心——即冬奥安全运营中心。

而作为冬奥安全运营中心的核心安全监测平台，需要汇集全量数据，因此该平台必须要拥有巨大的数据处理能力，以及相应的关联分析能力，对所有安全事件集中展示，且总指挥中心所有安全监测、分析人员都能够通过一个平台监控、分析、处置安全事件。于是在多次评估和讨论之后，奇安信态势感知与安全运营平台（NGSOC），顺理成章地成为了建设冬奥安全运营中心安全监测平台的核心。

与此同时，为了提升效率，冬奥安全运营中心采用全流程的标准化运营，制定了涉及安全运营、安全运维、应急响应的 SOP（标准作业程序），以上每个环节的决策和动作都对最终结果产生了重要影响。

“其实当时选择哪个产品作为核心安全监测平台，并没有那么顺利。”老尹回忆说，“作为总工程师，要对整体项目进行考虑和负责，总指挥中心人员有限，不可能让他们分散去监测多个设备，在事件处置上也无法做到及时和高效。” 作为冬奥安全运营中心核心安全监测平台，NGSOC 承载着从数据的接入、日常监控、应急管理、溯源分析、事件处置、态势呈现等全流程动作的对接和落地，因此需要最早一批进场交付部署。

熬夜、红牛，持续两周的交付部署

在 2020 年那个炎热的夏天，PNC 机房刚刚完成建筑施工，在网络条件还未完善的情况下，冬奥项目组几位工程师就奔赴现场，开始了第一次的平台迁移、部署工作。入场的时候着实被吓了一跳，交付团队的同学们

带着防毒面具在里面忙碌着。

机房建成初期，里面充斥着粉尘和不确定是否有害的怪味气体，冬奥安全运营中心项目的交付部署和建筑施工同步进行，当你认为耳边想起的轰隆声是服务器的声音时，却发现有可能是电钻和榔头，还有可能是空调调试的轰鸣声。大家在机柜之间，竖起服务器的纸箱子，作为电脑办公桌或半蹲半坐的椅子也或者走廊的“餐桌”。每隔一两个小时就要出去室外换个气、同时在夏日阳光下“取暖”。

据其中一位工程师回忆，持续高强度的工作，身体稍微有些吃不消，印象最深刻的一次是在机房升级到晚上近凌晨 1 点，按照升级流程一步步地进行着，不停地敲击着键盘，突然鼻血留在了键盘上。

“因为项目工期比较紧，所以大家住在了离冬奥安全运营中心最近的旅馆，早上 8 点进场、凌晨一两点离开，晚上大家为了提神，3 个人每 2 天就会喝掉一箱红牛，嗓子肿到 1 天只吃一顿饭，不敢喝太多、不敢吃太多，因为上厕所要去差不多 1 公里之外的地方，来回跑太耽误事儿。”另一位工程师补充到。

即便如此，时间也显得非常紧张

NGSOC 平台的部署工作持续了大概 2 周的时间，工程师们克服了恶劣条件带来的困难，解决了很多技术问题，在保障冬奥组委业务使用的前提下，平滑稳定地实现了平台集群拓荒部署、平台迁移、HA（Highly Available，是双机集群系统简称，提高可用性集群，是保证业务连续性的有效解决方案，一般有两个或两个以上的节点，且分为主活动节点及备用节点）上线、HA 初期技术验证等工作，为后续的安全建设工作提供了支撑。

高可靠、高安全，主备集群无缝切换

冬奥项目采用 HA（双机集群）的方式，这在 NGSOC 以前的项目中是没有遇到过的，也给研发人员带来了巨大的挑战。“主备集群的配合可

以有效保障业务系统稳定运行，通常我们完成主备切换需要 30 分钟。”NGSOC 事业部研发总监说，然而这个速度显然还达不到冬奥标准。而随着技术难关一个个被攻克，直到最后，主备切换不到 10 分钟即可完成。

为了达到冬奥会零事故的要求，NGSOC 研发团队从建设初期就开始研讨高可靠、稳定性和安全性要求，从架构设计出发，全面提升产品能力，目标是达到冬奥会的高质量标准，打造冬奥标准 NGSOC。

首先是高可靠。NGSOC 借鉴了传统安全产品的高可靠思路，通过主从的方式实现高可靠，但是很快就面临困难，海量的数据如何能够做到一致性关联、高并发的告警处置过程如何实现状态同步等。研发中心组建了攻坚团队，最终在架构层面成功解决。通过唯一性 ID 生成算法，在 HA 主从集群实现一致性关联。通过逻辑复制机制，实现告警处置过程的状态同步，并且顺利实现了可控的主从同步切换机制，在紧急故障情况下可实现业务不中断。NGSOC 平台最终在日均 35 亿日志高吞吐和 50+ 人并发运营的条件下，实现了数据的主从完全同步。

其次是稳定性。NGSOC 需要对自身的稳定性及输入异常做出反应，避免自身陷入异常。在研发过程中实现了对核心组件进行监控，包括服务监控、告警通知和自动恢复机制。一旦某个核心业务组件出现异常，NGSOC 可以自动感知，并通过冬奥会短信网关及时通知 7*24H 待命的安全运维人员及时介入并处置。同时，在 NGSOC 能够自动恢复的情况下，同时尝试自动恢复。其次是实现了对集群 EPS 负载进行监控，当集群负载超出集群告警阈值的时候，NGSOC 自动短信通知监控人员，通过冬奥应急响应 SOP，按要求进行降负载处置，避免数据积压等问题出现。还设计了限流保障机制，过载情况下也要确保 NGSOC 本身稳定运行。最终 NGSOC 在冬奥会和冬残奥会期间 7*24H 持续稳定运行，做到了运营平台零事故。

最后是安全性。NGSOC 作为冬奥安全运营中心核心安全监测平台，保障自身的安全至关重要。NGSOC 冬奥研发项目组联合奇安信集团多位架构师、攻防专家和研发人员，重点梳理了以下几项工作：

第一是进行源代码审计，从根源上找到所有可能被利用的攻击漏洞，进行彻底修复上线；

第二是参加冬奥会众测专项，将冬奥项目 1:1 环境搬到线上，接受渗透测试人员的攻击测试，对所有发现的攻击脆弱点进行修复和验证；

第三是冬奥现网暴露面梳理，对 NGSOC 的所有访问路径、账号和权限进行统一管理，权限做到最小化，将授权的访问路径梳理出清单并统一管理，其余非授权的访问路径全部设置封锁阻断策略。

第四是新增 NGSOC 自身安全性检测，安全从来不是绝对的，一旦 NGSOC 被攻击，如何能够快速而准确地产生预警，以便在最短时间内介入处理就非常重要。除了通用的终端安全检测、网络攻击检测和 APT 检测等攻击检测手段，还引入了 NGSOC 网络白名单机制，非白名单的入站和出站均告警和阻截，最大限度避免 NGSOC 被攻击或攻陷。此外，还给 NGSOC 平台增加了 300 多条自身安全加固和检测规则，让 NGSOC 平台在冬奥会和冬残奥会期间实现零事故。

技术的困难可以靠人力解决，但项目进行过程中遇到的困难不仅仅只是技术难题，比如，从 2020 年 2 月开展 HA 项目研发开始，由于各方面原因，研发人员并不是一成不变的，每一次人员的更迭都需要消耗大量时间去培训和交接。

老尹还提到，除了 NGSOC，冬奥项目在 2020 年几乎都在进行安全产品能力提升和交付部署阶段，直到 2021 年重心开始转向运营。冬奥安全运营中心项目整体做下来也是了了一个夙愿，从加入奇安信开始一直在接触和参与安全运营相关的工作，心里也一直有一个目标和期待，就是通过标准化把常态化安全运营真正做起来，事实也证明了做起来很有必要。冬奥项目经历了一个从极繁设计—不断简化—不断优化—全部标准化的过程。考虑到全面性的同时，又要兼顾效率，过于烦琐的设计会大大降低效率。

下期预告：下一篇将会进一步讲述如何实现冬奥安全运营中心标准化运营。安

以创业者心态投身工作

——走近大禹平台项目经理、架构师邓涛

作者 公关部 孙丽芳

寒窗苦研无人晓，一战成名天下知。这句话放在奇安信大禹平台上再贴切不过。2019 年组件研发，2020 年整体研发，历经千百次锤炼，大禹平台在北京冬奥网络安全保障工作中大显身手。

为什么是大禹？期间，它又经历了什么？带着这些疑问，项目经理及架构师邓涛走进了我们的视线。

邓涛来自湖北仙桃。因为培养出了李小双、李大双等一批体操世界冠军，仙桃被誉为“体操之乡”。而曾经在互联网 toC 行业连续创业的邓涛，2018 年一个“大跳”，跳入了 toB 行业的奇安信，从事研发管理工作。

“当时明显感觉整个互联网 toC 的创业浪潮已经在往下走，基本上没什么太好的机会了，我觉得要去 toB 行业看看。”

通常来讲，创业者重回一个组织内上班会比较不适应。邓涛却没有这个问题。

“因为我本身也是拿创业的心态来看待在奇安信内部的环境和机会。”

创业的心态是什么？就是把工作完全当成是自己的事，积极地吸收和学习，想尽一切办法，去达成工作目标。

有了这种强大的自驱力，邓涛遇到了一次极好的机会——参与建设大禹平台。

大禹治水，大禹平台治什么？

大禹平台是由董事长齐向东决策并命名的平台。面对滔滔洪水，大禹改变了“堵”的老办法，对洪水进行疏导，

最终战胜了洪水。奇安信的“大禹”要治的则是数据洪流，构建一个大数据安全中台，解决态势感知等大数据智能安全检测与管控类产线的产品质量和安全能力不足的问题。

“态势感知是安全领域最复杂的产品。” 奇安信副总裁、大禹平台负责人左文建一言以蔽之。

奇安信的态势感知产品，分为 GA 业务态势感知、网信态势感知、工业互联网态势感知、特殊行业的监管态势感知、安全运营态势感知、数据安全态势感知、车联网安全态势感知、实战攻防态势感知、API 安全态势感知等。以往这些态势感知在奇安信都是独立的产品团队，每一种态势感知都是一套非常复杂的程序和产品，都要运用非常复杂的技术，且研发费用巨大。

那这些态势感知产品有没有共性的东西？答案是肯定的。那就是它们的核心程序是相同的，不同的只是业务逻辑。把核心程序抽出来，做成一个公共的平台，大家用这个公共平台再去做与自己业务相关的安全产品。就像同样的汽车底盘，能做出轿车、货车，还能做出越野车。这个公共的平台就是“大禹平台”。

把设想付诸现实的任务交给了由左文建带领的应用技术研发一中心。

“我们在 2020 年 10 月上旬接到任务，要求在 2021 年 2 月 11 日完成第一个版本的开发。大禹平台的定位是安全中台，要汇聚感知分析类安全数据，集成行业安全能力，能够持续满足客户的建设需要。 这个要求是很高的，也没有先例。”

时间紧，任务重，左文建快速组建起大禹的核心团队。有着丰富研发管理经验的邓涛进入了团队，任项目经理和架构师。

大禹平台怎么建?

大禹的建设涉及到公司内部 10 多个 L3 部门，管理复杂度和技术复杂度都非常高。

既要做系统的总体规划，又要对项目做全程管控，两项关键职责在身，邓涛的压力可想而知。即便如此，邓涛坚持“磨刀不误砍柴工”，在项目初期推动组织了密集的能力提升培训。

“大概用了一个多月，组织大家了解公司各种不同的能力，调研原来在做这个方向的产线的痛点和问题。对应立项的目标，我们对自己的团队人才进行盘点，到底我们有哪些人，缺哪些人，现有的人要达成工作目标，需要具备什么能力，缺什么能力。然后我们就组织进行了相应的培训。我们还做了相关能力矩阵及相关能力提升的培训计划，把它变成了项目管理的标准动作，使团队对这个领域的认知能够快速拉齐。”

面对大禹平台这种非常复杂的项目，除了调研和培训，邓涛还推动大家快速统一了步调和做事规范。

“齐总只是给了一个初步的目标，我们列了一个详细计划，每步到底要做什么。而且我们在一开始就把到底要怎样做进行了规范，包括怎么开会都列得很明确。专项会议怎么开，关键会议怎么开，等等。”

统一了思想、拉齐了认知、明确了步骤，大禹平台正式进入架构设计阶段。

业务成功，必须要有好的架构设计。大禹平台的整体架构阶段共提交了 855 张设计图，93 篇设计文档，经过了 68 次讨论，25 次线上、线下评审，1176 次提交记录。

在这些过程中，邓涛提供了超过 10% 的提交记录，提交的设计数量在架构师团队中排名第一。“我们的架构设计是一个多次迭代的过程。从雏形开始，我们可以看到它越来越丰富，越来越清晰，越来越明确。”

架构设计完成后，大禹平台进入开发阶段。“开发不仅仅只需要写代码的能力。”项目经理邓涛继续采取很有章法的做法。

他牵头拟制了大禹的开发框架（Needle-Framework），其中包含了开发框架、建立持续集成流水线工具、代码提交规范等；编写基于 DDD 的应用开发示例，帮助大家能够快速理解 DDD，能够在实际的开发中使用起来；编写《大禹开发者手册》，其中包括了应用的开发规范、集成平台需要遵循的规范、数据集

邓涛（左二）被评为奇安信集团 2021 年度优秀干部

成规范等；组织架构培训，覆盖大禹团队及态势感知、TSOC、NGSOC、天眼、数据安全态势感知、工业互联网态势感知、系统安全共 7 个产线团队。

有规范、有工具、有开放的开发环境，大禹平台的开发有序且快速。

经过 3 个月的努力，大禹团队达成 211 目标，完成了第一期的开发工作。大禹一期实现了构建联合分析引擎系统，整合 Sabre、天工模型分析引擎和归并引擎；与锡安云端对接，构建客户与集团云端的安全数据能力通道；完成了数据治理体系建设及数据标准 1.0 版本；通过诺亚、玄机完成态势感知数据治理体系；基于 NIST 的资产模型，使用图数据库实现，关联检索百万节点 0.5 秒；统一数据检索引擎，在多数源并行检索；漏洞与脆弱性管理框架。

2021 年 6 月 20 日，大禹 6.0-RC2（内测第 2 个版本）发布。2021 年 7 月 5 日，大禹 6.0-RC3（内测第 3 个版本）发布。2021 年 8 月 6 日，大禹 6.0 Release（候选版本）发布。2021 年 11 月 26 日，大禹 6.2 RC2（内测第 2 个版本）发布。2021 年 12 月 30 日大禹 6.2 Release（候选版本）发布。

大禹平台以肉眼可见的速度，不断成熟、完善。高效的研发速度和严格的过程管理密不可分。项目经理邓涛的架构师思维在这里运用得恰到好处。

“把研发项目解耦出来，本质上就是两大类，一个是计划，一个是变化。我们要保证计划能够顺利地推行，但是要应对变化。而一个项目的变化无非来自几方面，即风险、变更、决策。它们的出现会引起一系列的连锁反应，也会影响原来的一些部署和方案。我们每天都会监控项目里有什么风险，有没有什么变更的东西，有没有新的决策，如果有的话，快速去判断它们对项目计划的影响，然后尽可能地控制影响。”

做研发管理，邓涛不是凭经验，不是靠感觉，而是

最大限度地让一切有章可循。

凭借多年的研发经验，再加上系统性地学习 CMMI 的软件工程的框架并加以实践，邓涛完成了《研发管理工作指南》建设，帮助团队中的各位研发管理者通过指南来应对研发管理中的各种可能影响计划的问题，帮助大家更加规范地对团队和项目经理进行管理。

“我到 toB 领域之后发现它跟 toC 很不一样。toC 要的是速度，你不能错过市场机会，所以要更快速地去决策，把产品推向市场。然后根据市场的反应，要么停，要么去变更。但是在 toB 领域，我们要做的是成功率。所以每一步我们不仅要走得快，更要走得稳。”

大禹的开发是又快又稳的典范，它对于整个奇安信研发体系的影响也是深远的。

“我们除了完成大禹本身的开发和自己团队的规范建设，期间形成的很多成果也进入了《奇安信 - 研发体系》，包括体系在多个实践域的规范和指南，也包括基于大禹的安全设计提炼出来的奇安信的可信架构设计规范和指南及最佳实践。在大禹的项目中，我们先后通过了 CMMI3、CMMI5、华为可信等的认证评估。在研发时间紧、复杂度高的情况下，实战化的完成上述认证评估，没有事后补过资料和文档。这是我特别引以为傲的经历！”

这也就是说，用大禹的建设经验能指导再造一个、两个甚至更多个大禹。

构建安全未来

2022 年 1 月 18 日，大禹 6.2 发布会在奇安信安全中心举行。发布会的名称叫作“构建安全未来”。

“这是大禹的定位，也代表了它现在的能力。”

向来低调的邓涛对于大禹的评价并不低调。

“大禹是全能型实战选手。宙斯身份控制平台、哈迪斯授权平台、达尔文升级平台、锡安云地交互平台、海龙设备兼容平台、海量数据基建平台、“星海”大数据平台、“猛禽”高性能检索引擎全部作为组件，集成进了大禹。这也就意味着大禹具备了面向大数据安全的通用开发平台及配套的内置安全能力，包括安全资产管理和运营、数据接入、数据治理、云地协同、威胁联合分析、事件管理与处理、安全设备接入控制等。”

事实上，就在发布会举办的同时，大禹正在迎接一场史无前例的实战挑战。这就是北京冬奥会的网络安全保障。

作为北京冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，奇安信创新“中国架构”，首次实现系统性、全局性建设冬奥网络安全保障体系，统筹部署安全保障工作。架构采用 APPDAR 安全保障框架，改变了以往的“产品堆砌”模式，将大数据处理、人工智能处理、威胁情报、行为分析等建设成为安全中台，利用中台的优势能力为具体安全产品赋能，覆盖所有冬奥场馆和工作终端。

而大禹正是 “安全中台”能力的核心。态势感知是安全领域最复杂的产品，尤其是冬奥网络安全保障所需要的态势感知产品。大禹被广泛集成在了态势感知等多项安全产品中，其中包括某国家级指挥中心的态势感知指挥平台。

天下武功，唯快不破

既然是实战，最关键的就是快速应对战况的千变万化。

冬奥前夕，临近春节，邓涛在这一年多来第一次请假。高强度的研发管理工作，让他几乎每天晚上十点下班，连周末都在加班。“弦一直绷的很紧，我想稍微调整一下，请两天假陪陪家人，后面肯定没时间了”。

然而，在带着家人出行的路上，邓涛突然接到一通紧急电话。核心内容是按照中央网信办冬奥会网络安全专家研判组组长、中国工程院院士方滨兴的最新研判要求，冬奥网络安全保障系统要增加一些新的功能。这主要是由作为“安全中台”能力核心的大禹平台来予以实现。

邓涛二话不说，立刻中止假期，回到战场。

“相当于上线之后，客户临时要增加新的需求。我们要快速上一些新功能，包括 IP 画像、蜜点等。之所以会这么临时，第一是原来已有功能可能没有考虑到这么大场合的一些分析场景。第二是方院士会有自己的一些

大禹核心团队

分析的思路和想法，但是需要在他看到我们的东西之后，才能具体提出哪些地方缺什么，需要加什么。”

根据不断更新的功能需求，在左文建的带领下，邓涛和团队分成两个班次，24 小时轮流倒班。大家一边讨论产品一边制作原型，然后快速进行测试。两个班次日以继夜，进行接力，以几乎“立等可取”的速度每天迭代一个新版本，发到冬奥网络安全保障现场。方滨兴院士每天早上九点都能在桌上看到新的数据，做出新的研判。

这种高频率的工作状态，持续了三周。

北京冬残奥会于 3 月 13 日圆满闭幕，奇安信实现了奥运网络安全“零事故”。大禹经受住了冬奥实战的考验，也锤炼了自身，正式量产，即能够实现完全标准化，完全能够适配奇安信旗下所有态势感知产品。经过测算，态势感知各条产品线，把中间核心部分全部替换为大禹平台以后，研发效率至少将提升了 30%。

大禹的前景很广阔，而邓涛的想法很平实。

“接下来我的工作重点就是做好大禹和各产线的深度对接。一方面，大禹的复杂度很高。另一方面，为了让整个系统更好地运行，我们实际上还用了很多新的东西，产线可能对它们并不熟悉。我们将想办法在减少人工指导的情况下，提升大禹的满意度和使用度。还有就是进一步做好研发效能的管理，让我们内部研发的流程更快、更流畅、更平滑。” 安

规划快一步

奇安信 | BEIJING 2022

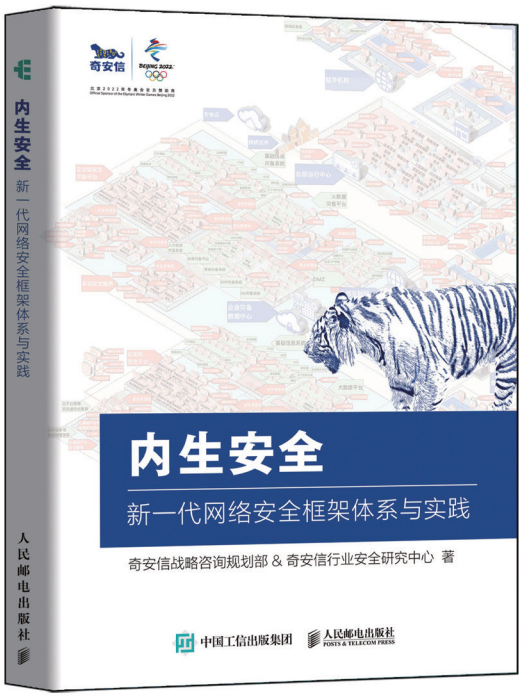
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

比十三香！这份 IT 人“无忧长假指南”有点东西

作者 公关部 王梦琪

“快要到假期了，咋一点儿也高兴不起来，总有一种预感，这个假期和往年一样，不能完整的度过。” 某企业 IT 部门网络安全负责人老张，正纠结要不要全家出去游玩。

时间回到一小时前。

五一假期前夕，眼睛盯着电脑屏幕上的文件，实则在思考长假准备带孩子去哪儿玩的老张，突然接到了上级指示——

“节假日是攻击活动的高发期，我们一定要严防死守，做好网络安全保障工作！安全第一，大家千万不能松懈！”

确实，道路千万条，安全第一条。一边感叹假期难过一边向手下同步消息的老张，陆陆续续听到了同事们的吐槽。

“一大波告警信息马上到达战场……唉，又是一个心惊胆战的假期。”

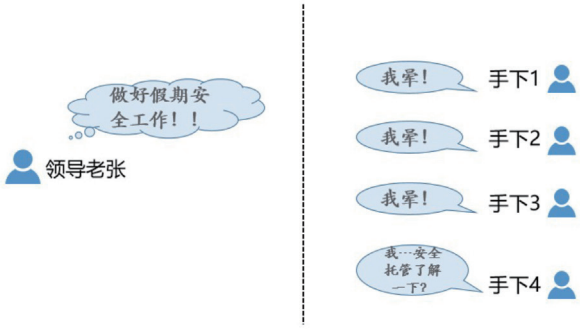
“部门人手不够，平时就一个人当成两个人用，假期正是攻击活动密集的时候，单靠咱们这几个老将，怎么顶得住？”

“就怕深夜突如其来的告警事件，半夜开电话会议，看来五一也得‘夜总会’了。”

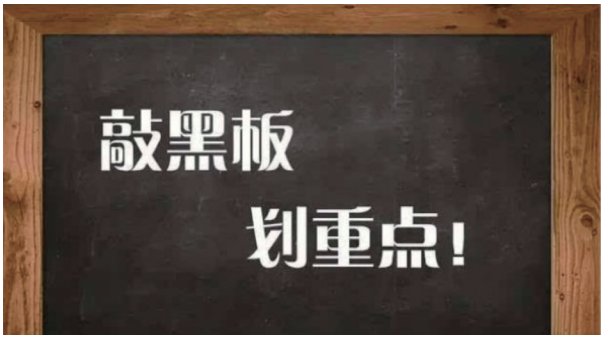
……

听完这些话，老张默默地叹了一口气，这年头，做安全难啊！

叮——新邮件的提示音将老张拉回了现实，出乎意料的是，这并不是来自手下的“求救”邮件，而是一份关于安全托管服务的介绍。



安全托管服务（MSS），即由专业安全公司提供人员、流程、工具结合用户自身的安全相关数据来开展安全运营的“远程托管”模式。老张所看到的邮件内容，介绍的是奇安信安全运营中心打造的安全托管服务，在节假日期间，也可为客户提供 7*24 小时全天候的专业服务。



划重点！奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，通过 7*24 小时持续监测、主动响应，协助客户完成威胁事件的闭环工作，通过运营驱动安全体系建设水平提升。

◆ 远程托管同企业自治的传统运营模式对比

对比项	传统运营	远程托管
基础设备	自购设备	专业公司代建
专业人员	自行招募	购买能力服务包
服务流程	层层汇报	短、平、快
运营时效	5×8 h	可满足7×24 h
运营能力	依赖于自身能力	集众家之长
分析能力	依赖于自身能力	后端专家团队支持
闭环能力	依赖于自身能力	人+威胁情报，持续支撑
小结	投入成本高、建设周期长	投入产出的性价比高、见效快、共享行业知识库

面对老张的公司这种专业人才短缺、分析处置人员能力不足，无法有效处置海量告警日志、及时发现高危安全威胁的情况，以及包括勒索攻击在内的各类安全事件频发，企业自有能力无法应对；客户资产繁多，隐藏的安全威胁难以发现、面对通报难以溯源处置；企业组织“重建设，轻运营”，安全建设难以发挥预期效果；在各种大型重保、攻防演习等重要时期专业人手不足……以上种种企业常见痛点，奇安信安全托管服务均可以有针对性解决安全运营难题。

奇安信安全托管服务类型主要包括威胁监测与响应服务（MSS-TDR）、管理监测与响应服务（MSS-MDR）和远程顾问服务。MSS-TDR，即通过远程对告警数据进行分析研判，并进一步溯源分析，提供专业的处置服务和整改建议； MSS-MDR，即通过远程对 NGSOC（态势感知与安全运营平台）的各类威胁告警数据进行关联分析和研判，在为客户提供综合分析服务的同时，主动响应，提供专业的运营指导、改进建议；远程顾问服务，即资深专家在线对相关报告进行解读或针对疑难问题进行解答。

与天眼、NGSOC 等奇安信明星产品的强强联合，能够更好地协助客户完成各类威胁事件的闭环处置工作，集合联动设备的技术与产品能力优势，打破传统运营模式带来的投入成本高、效果不明显、安全运营难等痛点，让企业安全运营更专业、更高效。总体来看，安全托管服务价值主要体现在以下几方面：

其一，持续监测，服务专家 7*24 小时全天候不间断监测，实时发现问题，快速通告并协助客户进行处置；

其二，深度分析，服务专家结合平台进行深度分析，针对事件提供完整的攻击过程，展现攻击的前因后果，解决客户被通报无法回溯的难点；

其三，主动响应，安全事件快速响应，协助客户联动封禁处置，积极主动防御；

其四，安全闭环，通过云地结合的模式，对发现的问题持续跟踪，确保安全闭环。

支撑安全托管服务的奇安信安全运营中心，拥有网络安全、终端安全、Web 安全、攻防技术、安全分析、应急响应等多元化专业人才，服务团队成员在长期安全工作中积累了大量的实践经验，目前已为政府、教育、企业、卫生、传媒等多行业、多领域的数百家客户提供服务。

在看完奇安信安全托管服务的介绍后，老张心里的石头落了地，这下，自己和伙伴们终于可以放心回家陪陪家人，享受五一假期了！

确实，专业的事情就该交给更专业的人去做！安

大事记

北京市政协主席魏小东一行莅临奇安信调研

按照北京市委统一安排，北京市政协主席魏小东就助推经济社会发展“开门红”到市政协委员所在企业调查研究。3 月 21 日上午，魏小东一行莅临奇安信调研。

魏小东走进奇安信工控展厅、党建室、车联网实验室等地，了解奇安信科研攻关、“红云行动”党建品牌建设等情况，并与委员们座谈交流，详细了解企业发展遇到的困难、需要政府支持解决的问题和对北京经济社会发展的意见建议。

魏小东指出，今年大事多、喜事多，保持经济社会大局稳定尤为重要。要发挥企业生力军作用，以企业高质量发展助推首都经济社会发展“开门红”。希望政协委员在带领企业发展的同时发挥自身优势，架起政府与企业沟通的桥梁，为北京持续优化营商环境积极建言献策。市政协将认真研究梳理企业需求及意见建议，及时向市委市政府报送，推动问题解决，帮助企业实现更好地发展。

北京数十家国资与高新企业齐聚奇安信 交流冬奥网安“零事故” 经验

为管理好、运用好冬奥遗产，4 月 11 日，中关村数字经济产业联盟（简称中数联盟）组织成员单位赴奇安信交流。奇安信在活动中首次公开系统性分享“中国模式、中国架构、中国产品、中国服务”的冬奥网络安全保障“零事故”成功经验。

本次交流是中数联盟成员单位互访活动第 8 站，北京市国资委主任、中关村数字经济产业联盟理事长张贵林主持活动并讲话。

“本次活动，一方面是学习奇安信冬奥网络安全保障的成功经验，另一方面是落实国家有关规划和要求。”张贵林表示，数字经济已经成为全球新一轮产业竞争力的制高点，党中央国务院高度重视数字经济，在今年发布的“十四五”数字经济规划、两会总体报告中，都强调了促进数字经济发展，促进国家网络安全和能力建设。奇安信作为网络安全企业和冬奥网络安全赞助商，不仅拥有很高的技术水平，并且在国家安全方面勇于担当，做出了突出贡献。

张贵林进一步指出，国有企业的网络安全要引起高度重视，全力推动网络安全建设，尤其是公共交通、水力、能源等重点企业，切实提升国有企业网络安全水平。

体系化防御 · 数字化运营 奇安信举办冬奥“零事故”终端安全分享会

4 月 21 日，在奇安信冬奥“零事故”终端安全经验分享会上，分享了“体系化防御，数字化运营”的终端安全新思路。

“体系化防御，数字化运营”以确保各类终端“可信、合规、安全”为核心目标，通过“体系化防御”健全终端安全能力，实现安全能力全覆盖、安全管理全统一、安全响应全协同，运用“数字化运营”保障终端安全效果，实现可量化、可提升、可看见的闭环终端安全运营，从而确保终端安全能力的持续有效和稳步提升。

在这次冬奥安全保障过程中，奇安信成功解决了国内外黑客对各类冬奥终端发起的6641次攻击事件，以“零事故”的佳绩通过了冬奥的实战检验。

中海油走进奇安信 交流冬奥网络安全“零事故”经验

4月20日，中国海洋石油集团有限公司科技信息部总经理周建良一行走进奇安信，并围绕冬奥网络安全保障和央企网络安全建设与奇安信安全专家进行了深入交流和合作研讨。

这是奇安信冬奥网络安全“零事故”宣讲团的首次开讲。在冬残奥会结束的第三天，奇安信就成立了宣讲团，全面梳理冬奥网络安全保障中形成的方案、标准、规范、产品，形成冬奥遗产，形成了网络安全“中国方案”，为我国关键信息基础设施、重要活动的网络安全打造模范样本。

奇安信举办研发平台战略发布会

4月19日，奇安信集团在京举办研发平台战略发布会，奇安信董事长齐向东透露，通过研发平台的量产，可以有效解决行业难题，奇安信已率先尝到甜头，研发平台相关产线增速高于行业平均水平3倍以上。

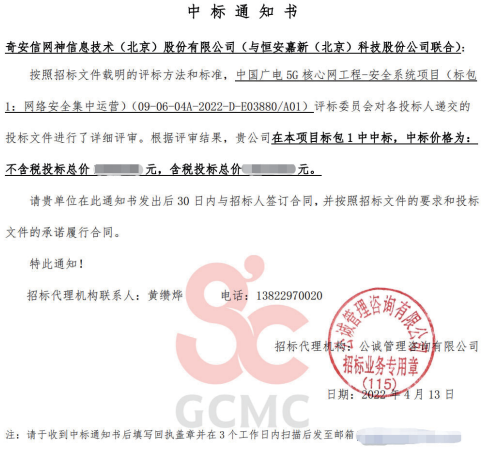
齐向东介绍了“三步走”的平台化战略蓝图。第一步是研发平台化：通过研发平台的成功量产，推动研发人员实现人效比40%左右的提升，为2022年公司盈利打下坚实基础；第二步是产品平台化：真正实现安全产品协同与数据统一管理，全面提升产品竞争力，保持公司营收高增速，持续引领行业；第三步是能力平台化：适应安全行业整合化趋势，带领行业走向集中化，改变“小零同”的现状。

今年的BCS大会上，将会公布详细的生态伙伴认证标准并开放平台接入申请通道。

奇安信中标中国广电 5G 安全大单

近日，中国广播电视网络集团有限公司（简称中国广电）发布了《5G 核心网工程 – 安全系统项目招标》中标候选人公示。

公示显示，该项目包括 6 个标包，奇安信网神信息技术（北京）股份有限公司（与恒安嘉新（北京）科技股份公司联合）中标了中国广电 5G 核心网工程 – 安全系统项目（标包 1：网络安全集中运营），包括软件、硬件，平台建设规模涉及 1 个集中节点的软件和 31 省节点的硬件设备等。



中 标 通 知 书

奇安信网神信息技术（北京）股份有限公司（与恒安嘉新（北京）科技股份公司联合）：

按照招标文件载明的评标方法和标准，中国广电 5G 核心网工程-安全系统项目（标包 1：网络安全集中运营）（09-06-04A-2022-D-E03880/A01）评标委员会对各投标人递交的投标文件进行了详细评审。根据评审结果，贵公司在本项目标包 1 中中标，中标价格为：不含税投标总价 [redacted] 元，含税投标总价 [redacted] 元。

请贵单位在此通知书发出后 30 日内与招标人签订合同，并按照招标文件的要求和投标文件的承诺履行合同。

特此通知！

招标代理机构联系人：黄缵烨　　电话：13822970020

招标代理机构：公诚管理咨询有限公司

日期：2022 年 4 月 13 日

注：请于收到中标通知书后填写回执盖章并在 3 个工作日内扫描后发至邮箱 [redacted]

齐向东：“零事故”应成为网络安全防护新目标推动行业高质量发展

在中国网络安全产业创新发展联盟成立大会上，奇安信集团董事长齐向东结合当前国际网络安全态势，总结了冬奥网络安全保障工作的成功经验和启示，并提出以“零事故”作为网络安全防护的新目标。

齐向东表示，“零事故”是网络安全“中国方案”的胜利，不仅国家重大安保活动、关键信息基础设施安全保护积累了经验，提供了重要实践，更为未来我国网络安全产业的发展提供了全新启示：一是将三级网络安全指挥体系常态化，二是由具有技术能力第三方全权负责安全建设，三是建议明确网络安全投入占比不低于 10%，四是按照统一的框架进行系统性、全局性规划，五是加快研发具有独立知识产权的中国产品，六是用实战攻防检验安全系统的有效性。

奇安信公益基金会向吉林、福建高校捐赠防疫物资

近日，奇安信公益基金会携手爱心企业向福州大学、闽江学院、福建信息职业技术学院三所高校捐赠的第一批防疫物资送抵校园。后续第二批防疫物资，也于 4 月中下旬送达福州外语外贸学院、福建船政交通职业学院。

荣誉证书

兹有 奇安信科技集团有限公司 向长春理工大学教育基金会捐赠420箱泉阳泉矿泉水。助力学校防疫抗疫，特颁此证，以示谢忱！

长春理工大学
教育基金会
二〇二二年三月二十二日

此前，奇安信已向吉林大学、长春理工大学两所高校分批捐赠了口罩、方便面、饮用水等防疫物资，助力吉林高校抗疫。

齐向东出席统战部服务北京冬奥会、冬残奥会工作总结会暨主题教育活动启动会

3 月 31 日，首都统一战线服务北京冬奥会、冬残奥会工作总结会暨“喜迎二十大 · 奋进新时代”主题教育活动启动会召开。北京市委常委、统战部部长游钧出席会议并讲话。奇安信集团董事长齐向东分享了奇安信作为北京冬奥会官方网络安全服务商的心得。

他表示，奇安信能够实现冬奥网络安全“零事故”目标，根本原因在于，始终紧密团结在党的周围，在党的指导下开展各项工作，在北京冬奥会上实现了网络安保的历史性突破。

在全国人民喜迎中国共产党召开二十大之际，齐向东表示，将继续积极参与市委统战部、工商联“民企心向党、奋进新征程”理想信念主题教育活动，坚定发展信心，深入贯彻“稳字当头、稳中求进”的总要求，以服务大局为抓手，在践行国家战略中彰显社会价值，成为新时代北京新产业的排头兵，为首都高质量发展做出新贡献。

十八国驻华国防武官参访 奇安信全面开启国际市场

3 月 30 日上午，来自阿联酋、突尼斯、埃及、科威特、摩洛哥、赞比亚等 18 个中东及非洲国家的 20 位驻华国防武官到访奇安信。

武官团与奇安信集团董事长齐向东、总裁吴云坤就奇安信冬奥网络安全保障成果、俄乌网络战等内容进行交流与讨论，并详细了解了奇安信在能源、金融、工控、关基等领域的国家级网络安全体系建设解决方案等产品与服务。

奇安信已在欧洲、中南亚、南亚、中亚、中东、及非洲开展网络安全业务，并为部分中国“走出去”的大

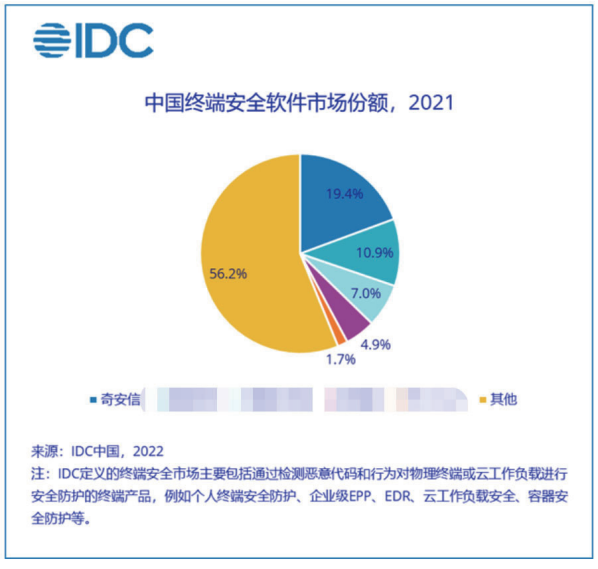
型企业及中国大型银行的海外分支机构提供网络安全服务和解决方案。

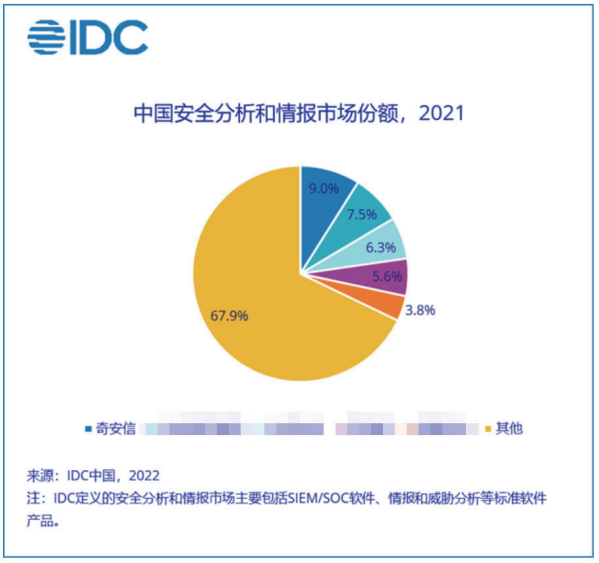
荣誉墙

IDC 报告：奇安信终端安全多赛道领先 连续四年市场份额第一

日前，权威咨询机构 IDC 发布了《2021 年下半年中国 IT 安全软件市场跟踪报告》。《报告》显示，2021 年全年中国 IT 安全软件市场厂商整体收入为 34.2 亿美元（约合 220.4 亿元人民币），较 2020 年增长 31.7%。

奇安信凭借“体系化防御、数字化运营”的终端安全新思路，以及主机终端新赛道云工作负载安全的强劲增长，在终端安全软件史市场，以 19.4% 的市场份额稳居首位，从 2018 年到 2021 年连续四年领跑终端安全软件市场；在安全分析和情报领域，奇安信以 9%的市场份额，连续两年夺得 2021 年该细分领域第一名。





奇安信入选信安标委 “网络安全国家标准 20 周年优秀实践案例”

近日，全国信息安全标准化技术委员会正式发布《关于公布信安标委 20 周年网络安全国家标准优秀实践案例获奖名单的通知》。其中，奇安信集团“工业控制系统安全标准助力城市轨道交通网络安全综合防护平台建设”项目，入选优秀实践案例，充分发挥其示范引领作用，为工业安全相关建设树立良好标杆。

序号	案例名称	申报单位
1	基于国产密码算法的应急广播消息安全保护体系	国家广播电视总局广播电视科学研究院
2	基于国密的国家电子政务外网安全邮箱系统平台网络安全国家标准实践	国家信息中心、国家信息技术安全研究中心、北京国信安邮科技有限公司、深圳奥联信息安全技术有限公司
3	服务器安全技术要求和测评准则应用推广实践	浪潮电子信息产业股份有限公司
4	专网安全管控体系建设应用	浙江省人力资源和社会保障信息中心、浙江远望信息股份有限公司
5	工业控制系统安全标准助力城市轨道交通网络安全综合防护平台建设	奇安信科技集团股份有限公司

奇安信代表顾鑫荣获冬奥会、冬残奥会北京市先进个人

4 月 19 日，北京冬奥会、冬残奥会北京市 · 北京冬奥组委总结表彰大会上，奇安信集团冬奥保障团队技术负责人顾鑫凭借在冬奥会期间保障冬奥网络安全工作的突出表现，荣获“2022 年冬奥会、冬残奥会北京市先进个人”称号。

冬奥期间，3500 多名和顾鑫一样的奇安信网络安全工程师、数百位冬奥网络安全卫士一起，驻守在闭环内外，为冬奥期间提供 7*24 小时不间断的网络安全保障服务，用中国制度、中国产品、中国技术、中国服务构建冬奥网络安全“中国方案”，实现了北京 2022 年冬奥会网络安全“零事故”，为保证北京冬奥会顺利召开和安全运行发挥了关键突出作用，并形成了宝贵的冬奥遗产，为国家关键信息基础设施保护和重大活动安保工作提供实践经验。

奇安信通过全球软件工程领域最高级别 CMMI 5 级评估认证

近日，奇安信正式通过全球软件工程领域最高级别 CMMI – DEV V2.0 成熟度 5 级评估认证。

CMMI 全称 Capability Maturity Model Integration，即“软件能力成熟度模型集成”，是国际公认的衡量软件企业研发能力成熟度和项目管理水平的权威标准，代表着国际上最先进的软件工程管理方法。CMMI 成熟度水平分为 5 个等级，5 级为该体系最高等级评估，是目前国际软件行业对管理成熟度要求最高、申请难度最大、级别最高的评估。

本次认证项目全部由研发尖端平台和技术创新产品的实战项目参与，奇安信研发已将 CMMI–DEV V2.0 5 级的各项标准，应用到软件项目管理及应用开发的各个环节，依托于近年大量的研发项目数据积累，共计创建过程性能基线 70 条、创建过程性能模型 7 个、创建预测模型 7 个，完全满足了 5 级的 19 个实践域、共计 186 条实践的评估要求，从管理到执行，涵盖软件工程

Measures conducted an official CMMI® V2.0 Benchmark Appraisal No. 58397 on Mar 17, 2022 in accordance with the CMMI Institute's Appraisal Requirements for CMMI®. The appraisal team judged

QI-ANXIN Legendsec Information Technology (Beijing) Inc.
Research and Development Center

to be at Maturity Level 5 as defined by the CMMI® V2.0 Development

Pascal Rabbath, Measures Technology LLC
Certified High Maturity Lead Appraiser(0100199-01)

2022-03-17

CMMIDEV/5℠
Exp. 2025-03-17/Appraisal #58397

Measures 2022年3月17日执行了评估号为58397的CMMI V2.0基准评估，满足了CMMI研究所对CMMI®的评估要求，评估小组判定

奇安信网神信息技术（北京）股份有限公司
研发中心

达到了CMMI® V2.0 Development
成熟度等级5

Pascal Rabbath, Measures Technology LLC
Certified High Maturity Lead Appraiser(0100199-01)

2022-03-17

CMMIDEV/5℠
Exp. 2025-03-17/Appraisal #58397

的各个方面。实现了更快、更好、更多、更省的高效软件产品交付，可有效提升研发团队的工作效率与交付质量。

奇安信 SOAR 入选国际权威机构 Forrester 报告

近日，国际权威咨询机构 Forrester 发布《Now Tech: Security Orchestration, Automation, And Response (SOAR), Q2 2022》报告，概述了全球安全编排自动化与响应 (SOAR) 的市场现状及发展。基于市场占有率和功能，奇安信与全球多家厂商共同上榜 Forrester 报告。

作为国内技术先进、功能齐全、操作实用的安全编排自动化与响应系统，奇安信 SOAR 具备区别于其他同类产品的 5 大关键能力——安全能力编排化、安全流程自动化、告警响应智能化、案件管理全程化、系统架构开放化。此外，SOAR 新加入的协同作战室功能，还可以让安全工程师实时沟通、并内置大量自动化剧本和命令，进一步提升人机协同作战效率。

《中国网络安全行业全景图》第九版发布 奇安信蝉联“入选最多企业”

3 月 31 日，国内网络安全权威机构安全牛正式发布《中国网络安全行业全景图（第九版）》。该报告共收录 433 家国产网络安全企业和相关行业机构，包含 14 项一级安全分类，94 项二级安全分类，二级细分领域共收录 2609 项，较第八版增加 486 项。

其中，奇安信本次共入选 13 个一级安全分类，79 个二级安全分类，几乎覆盖了全部一类安全领域和大部分二级细分领域，多年稳居入选全景图细分领域最多企业榜首。

奇安信零信任首批首家通过“Zero Trust Ready” SDP 解决方案测试

近日，在中国信息通信研究院联合各生态伙伴共同发起“Zero Trust Ready”项目中，奇安信零信任安全解决方案顺利通过了该项目 SDP 解决方案基准能力测试评估，成为首批首家获得此项权威认证的企业。

“Zero Trust Ready”项目由中国信息通信研究院算网融合研究团队依托 CCSA TC621（算网融合产业及标准推进委员会）联合各生态伙伴共同发起。奇安信零信任安全解决方案作为第一批次“Zero Trust Ready”SDP 解决方案基准能力测试评估的首个方案，经历了中国信通院和 CCSA TC621 的严格测试，测试内容均顺利完整地通过，获得认证。

NO：2022-04-01-A01-01

CAICT 中国信通院　CCNIS

Zero Trust Ready 证书

SDP解决方案

奇安信网神信息技术（北京）股份有限公司

兹证明奇安信网神信息技术（北京）股份有限公司奇安信零信任安全解决方案，通过了2022年度“Zero Trust Ready” SDP解决方案基准能力测试评估(第一批次，测试报告编号：B22B20135)。测试依据：《Zero Trust Ready SDP解决方案基准能力测试方案》，通过的测试内容包括：

√SDP灵活部署　√身份安全　√动态访问控制　√持续信任评估
√业务访问安全　√自身安全　√业务数据安全　√态势感知
√安全运维管理　√网络安全　√安全扩展能力

云计算标准与测试验证北京市重点实验室

算网融合产业及标准推进委员会

地址：北京市海淀区花园路北路52号

颁证时间：2022年3月24日

奇安信位居“2021年中国网安产业竞争力50强”第一名

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

“2021年中国网安产业竞争力50强”榜单

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

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