奇安信网络安全通讯 • 安全快一步

2021 年 3 月 第 3 期

网安26号院

SECURITY INSIDER

攻守有道

网络安全攻防演习全攻略

P10

规划快一步

奇安信 | BEIJING 2022

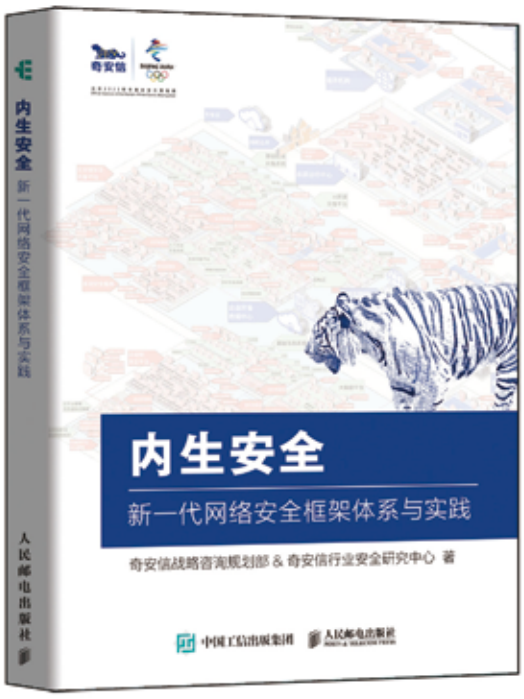
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

双重压力之下
安全能力期待质的飞跃

2021年的网络安全实战攻防演习再度拉开帷幕。

五年间，网络安全实战攻防演习逐渐走向演习规模化、规则成熟化、频度常态化、手段多样化、防御体系化。

在实战攻防演习的推动下，政企机构的网络安全建设从满足安全合规向体系化的能力建设发展，打造”常态化“的安全运行能力成为重要手段。

我们需要清醒认识到的是，历年攻防演习暴露出的政企机构薄弱环节仍有待改善，包括安全意识薄弱，利用社工突破隔离网；互联网存在未知资产，易成为攻击跳板；业务互联出口多，安全管控不严；应用系统常规漏洞多；供应链管控弱，自身安全等级低等。这意味着安全能力真正实现质的变化，提升对网络安全的重视程度和投入，需要更多制度性的安排。

不久前发布的《十四五规划纲要》和2035年远景目标纲要，让网安从业者看到更有前景的未来：安全理念贯穿始终，网络安全继续成为风口。网络安全与人工智能、大数据、区块链、云计算被共同列为5大新兴数字产业，明确要求培育壮大，加快推动。 显然，未来五年，网络安全不差钱。

《十四五规划纲要》将能力建设提到特别重要的地位：专门提出“全面加强网络安全保障体系和能力建设”，并要求“提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力”。网络安全将更加注重其体系特性和能力建设，而且能力范围覆盖更广。

安全工作、意识先行。为了从根本上解决对网络安全重视程度有待提高的问题，《十四五规划纲要》中首次提出了“加强网络安全宣传教育和人才培养”的规划要求。这无疑是要聚焦解决网络安全的思想根子问题。

严峻的安全形势令政企机构面临巨大的现实风险。据 Cybersecurity Ventures 预测，到2021年全球因网络安全事件导致的损失将高达6万亿美元；每分钟造成的损失高达1140万美元。

根据 Gartner 的数据，到2025年，有40%的董事会将会设立专门的网络安全委员会，网络安全已被视为仅次于法律合规的第二大风险来源。国际数据公司 IDC 预测，2020~2024年间，中国网络安全市场年复合年均增长率为16.8%，增速继续领跑全球网络安全市场。

在现实风险和法规要求的双重压力下，国内的政企网络安全能力建设有望实现质的飞跃。

总编辑

李建平

2021年3月1日

CONTEN

目录

安全态势

月度专题

攻守有道

网络安全攻防演习全攻略

2021年国家级网络攻防演习举办在即，现政企机构再度面临严峻考验。 奇安信一直推广并实践实战攻防演习，参与了众多国家级、省市级以及大型企业的实战攻防演习，积累并总结出一套完整的实战攻防演习防守经验及最佳实践，汇编成“网络安全攻防演习全攻略”。

攻防一线

安全之道

TS

奇安信人

奇安资讯

第 3 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
奇安资讯主编	陈冲
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

全球网络安全演习动态

网络安全演习成为各国发现防护漏洞、提升安全能力的重要途径。过去一年来，美国、欧盟、日本、澳大利亚与东盟等国家均举办了例行或新的网络安全演习。

网络风暴 2020

“网络风暴 2020”（Cyber Storm 2020）于 2020 年 8 月 10 日至 14 日举行，由美国国土安全部下属网络安全和基础设施安全局（CISA）主办。美国“网络风暴”演习从 2006 年开始，每两年举行一次，迄今已经举行过七次。本次演习参与单位包括 200 余家联邦机构；州政府和地方政府以及一些重要基础设施领域的合作伙伴，超过 2 万名人员参与其中，达到历届演习活动之最。

演习分为攻、防两组进行模拟网络攻防对抗，攻击方通过网络技术、社工手段、物理破坏手段，攻击能源、金融、交通等关键信息基础设施；防守方负责搜集攻击部门反映的信息，评估并强化网络筹备工作、检查事件响应流程并提升信息共享能力。

网络欧洲 2020

“网络欧洲 2020”（Cyber Europe 2020）演习由欧盟网络与信息安全局于 2020 年 6 月举行，旨在建设网络安全能力，加强欧盟合作并提高医疗健康领域的网络安全意识。“网络欧洲”演习是欧盟网络与信息安全局目前主办的最大规模活动，每两年举办一次，迄今为止已经举办了六次。

演习活动场地分布在整个欧洲的几个中心地带，并由演练控制中心统一协调。参加演习的人员来自欧盟各成员国的网络应急机构、电信、能源企业、网络安全部门、金融机构、互联网服务提供商，以及其他私营公司和公共组织。

北约“网络联盟”演习

“网络联盟”演习由北约组织于 2020 年 11 月 16 日至 20 日举行，此次演习共有来自北约成员国、伙伴国和欧盟近 1000 名官员和专家参与，演习规模创历年新高。由于受到新冠肺炎疫情影响，此次演习首次在线上进行。“网络联盟”演习从 2008 年开始举行，每年一次，具有测试性、实战性等特点，与具有对抗性等特点的“锁盾”演习并称北约两大网络演习。此次演习在爱沙尼亚网络安全培训中心协调下，以常见网络威胁为模板，重点测试对网络攻击事件的实时响应能力，如破坏机密网络、破坏关键基础设施的通信系统、利用智能手机应用程序窃密等，提高北约成员国协调应对网络安全事件的能力。

APCERT 年度网络安全演习

2020 年 3 月 11 日，亚太计算机应急响应小组（APCERT）举办了国际网络攻击模拟演习，参与者包括亚太、中东和非洲的 32 个国家和地区的计算机安全事件响应团队（CSIRT）。本次演习要求各方参与者处理一个本地企业遭受数据泄露及恶意软件感染的案例。

此次演习需要成员和合作伙伴之间的跨边界协作计划，用于测试事件处理过程和每个团队的沟通，例如根据演练场景进行分析、安全咨询、应急响应（包括断网）等。演习组织者需要制定与当前安全形势尽可能接近的网络威胁方案。这将有助于团队为最大程度地缓解现实生活中的网络威胁做好准备。

东盟 – 日本跨国网络安全演习

2020 年 6 月 25 日，由越南网络安全应急响应小组 / 协调中心（VNCERT/CC）与信息和通信部共同举办了 2020 年东盟 – 日本跨国网络安全演习。本次演习在线

上和线下共同举行，参与者包括十个东盟成员国和日本的 200 名专家。此次演习旨在提高专业能力，并建立国家网络安全事件响应网络。除了演习，该网络还计划提供培训课程，进行科学研究以及在预防和控制网络攻击方面进行国际合作。

金融业“量子黎明”演习

量子黎明第 5 次网络安全演习（Quantum Dawn V）由美国证券业及金融市场协会（SIFMA）于 2019 年 11 月举办，美欧日澳加等 9 个国家地区 180 多家金融机构和政府机构的 600 多名人员参与。该演习每两年举办一次。

量子黎明主要考核参与者跨部门、跨领域、跨国家的协调、沟通和危机应对能力。参与者可以在各自国家参与，通过邮件、电话等方式通信，以增强演习的真实性。本次演习演示了全球网络中断情况下，各机构领导者如何共同协作建立响应和恢复能力，测试金融行业在运营弹性上的

表现，着重演练了北美、欧洲、亚洲等地区企业和监管机构之间的跨区域沟通与协调。

澳大利亚电力行业国家网络安全演习

澳大利亚电力行业国家网络安全演习由澳大利亚网络安全中心（ACSC）、电力行业、政府机构于2019年11月联合举办。该演习包括一次为期2天的行动演习、一次战略讨论演习，行动演习有32个机构的560名人员参与，战略讨论演习有23个机构的25人员参与。

本次演习重点演示了8个方面能力：发布警告和报告网络安全事件；沟通与协调；事件响应能力和管理；信息共享（包括威胁情报）；信息技术与操作技术；公共信息协调；恢复；角色与责任。

北美“电网故障”网络安全演习

自2011年开始，由北美电力可靠性公司（NERC）的电力信息共享和分析中心（E-ISAC）主办的北美“电网故障”（GridEx）每两年举办一次，迄今已经举办了5次。

第五次（GridEx-V）演习在2019年11月13日至14日举办，由管理层桌面会议和分布式演习场景执行两部分组成。管理层桌面会议的参与者来自电力行业、跨行业合作伙伴和政府的100多名高管和员工；分布式演习参与者包含526个组织的7000多名参与者，包括天然气公用事业、水公用事业和电信公司等。该演习展示了公共事业是如何对虚拟网络和物理安全威胁与事件做出响应并恢复，如何加强在危急时刻的沟通关系，并为汲取的经验教训加大投入。

中国澳门网络安全事故演习

2020年12月11日，中国澳门举行“2020年度网络安全事故演习”。此次演习由中国澳门网络安全事故预警及应急中心联同负责网络安全监管工作的特区政府部门，以及中国澳门自来水股份有限公司、中国澳门电力股份有限公司等15个机构共同组织，旨在加强各方在应对网络安全事故时的沟通协调和技术处理能力。

此次演习模拟中国澳门发生大型网络安全事故，大量关键基础设施营运者的电脑系统遭受黑客入侵，网络安全事故预警及应急中心、监管实体和各营运者在短时间内共

同做出应对，通过“网络安全事故预警及通报平台”，以电子化方式对事故进行预警、通报及更新处理进展。整个演习历时约 3 小时，参演各机构和部门从演习中评估当前事故通报和应对机制，以便做出优化完善。

美国城市网络安全演习

2020 年 9 月，由美国陆军网络学院及政府和企业联合两座港口城市查尔斯顿市、萨凡纳市共同举办了第三次美国城市网络安全演习（Jack Voltaic 3.0），该演习始于 2016 年，每两年一次。本次演习旨在探究如果同时出现多种灾难性事件，城市该如何继续保持运转能力。

本次演习设计了 Emotet 恶意软件感染、勒索软件传播、货船事故、灌水和报警系统故障等场景。演习测试了两座港口城市在模拟网络攻击下的响应能力，特别是在恶意软件、物理破坏等混合威胁情况下，能否正确应对。

黑掉卫星

“黑掉卫星”（Hack-a-Sat）是在 DEF CON 28 大会上举办的首届天基夺旗竞赛活动。本次竞赛由美国太空部队主办，有超过 6000 名选手自发组织成 2000 多支队伍参加。竞赛分两阶段举行，经过 2020 年 5 月第一阶段之后，到 5 月 24 日，赛事八强陆续确定。第二阶段与 2020 年 8 月 7 日至 9 日举行，八支队伍将在两天内接受五项挑战，包括获得对卫星地面通信站的控制权、尝试与失控自旋的卫星取得联系、团队已经成功夺回控制权，最后需要在实验室中拍下月球图像以证明恢复成功等。

比赛结束后，得分最多的三支队伍 PFS、Poland Can Into Space 以及 Solar Wine 赢得了 5 万美元的奖金。美国空军表示，国防部高度重视“黑掉卫星”网络安全竞赛，因为该竞赛能够帮助美国军方发现其系统中的缺陷，并且可以借此机会发现网络安全人才。

黑掉楼宇

“黑掉楼宇”（Hack the Building 2020）网络攻防演习于 2020 年 11 月 16 日至 19 日举行，本次演习由美国网络司令部赞助、马里兰州创新研究所（MISI）创建的“梦想港”（DreamPort）主办，有来自工业，学术界，民政机构和国防部的 45 个攻防团队参加。本次演习分为三个阶段，第一阶段是 11 月 16 日、17 日对目标建筑的进攻；第二阶段为 11 月 17 日下午的楼宇自动化和控制系统网络安全虚拟会议和小场地比赛；第三阶段为 11 月 18 日、19 日举行的攻防对抗活动。

总体而言，“黑掉楼宇”演习活动凸显了关键基础设施网络安全对于商业和政府机构的重要性。该演习展示了信息技术、物联网和运营技术网络攻击对目标建筑物自动化和任务运营的影响。

奇安信
新一代网络安全领军者

“天眼+安服”创新安全运营服务

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。

奇安信
新一代网络安全领军者

www.qianxin.com
kefu@qianxin.com
4009-303-120

奇安信

新一代网络安全领军者

奇安信营销体系

招募精英

党政大客户部总经理

1.负责中央部委及二级单位市场的全年销售任务达成；
2.制定年度销售计划及预算，分解销售任务，推动并确保相应计划、目标的达成；负责团队的建设、管理、指导与激励；
4.重要客户中高层关系维护，项目运作与把握；潜在客户的市场拓展，制定增量目标，计划并达成；
5.进行市场调研与分析，研究同行业界发展状况，为公司战略制定、产品规划等方面提供相应建议。

大客户销售经理

党政/网信/电子政务/审计行业

1.根据公司及本行业销售任务开展销售工作，完成各项销售指标；
2.开拓、积累、夯实客户基础；
3.挖掘客户需求，为客户提供整体解决方案；
4.负责组织开展行业市场活动，加强公司在行业内的品牌影响力；
5.挖掘、反馈所负责行业的市场信息及客户需求，促进产品体系优化，构建有竞争力的市场策略。

售前技术专家

党政大客户部

1.负责国家党政机关头部客户的售前技术工作，协同党政大客户部销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求
2.负责党政大客户部客户技术交流、项目技术文档编写、项目招投标等售前支撑工作；
3.负责党政大客户部技术策略梳理、技术资料整理，并能在党政机关头部客户进行技术和解决方案推广。

解决方案专家

党政/网信/电子政务/审计行业

1.协助行业技术负责人完成行业级解决方案、营销技术策略、行业技术资料整理，并能在行业进行技术和解决方案推广；
2.协同行业销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求；
3.完成行业市场典型客户调研，不断提升解决方案竞争力，能洞察行业趋势、参与行业规范制定。

扫码联系我们

攻守有道

网络安全攻防演习全攻略

2021 年国家级网络攻防演习举办在即，现政企机构再度面临严峻考验。 奇安信一直推广并实践实战攻防演习 , 参与了众多国家级、省市级以及大型企业的实战攻防演习，积累并总结出一套完整的实战攻防演习防守经验及最佳实践，汇编成“网络安全攻防演习全攻略”。

网络安全实战攻防演习的五大演变

作者　公关部 周丹 庞悦宁

2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上发表讲话指出，“网络安全的本质是对抗，对抗的本质是攻防两端能力的较量”。

同年 11 月，《网络安全法》颁布，要求关键信息基础设施运营者定期进行网络安全演习。中国网络安全实战攻防演习的大幕就此拉开，五年时间，网络安全实战攻防演习飞速发展，逐渐向演习规模化、规则成熟化、频度常态化、手段多样化、防御体系化演变。

演变一
攻防演习向规模化演变

我国实战攻防演习的发展分为两个阶段，第一阶段是试验阶段，以学习先进实战经验为主，参演单位少，演习范围小；第二阶段是推广阶段，实战演习发展飞速，参演单位数量暴增，演习走向规模化。

2016 年《网络安全法》的颁布，标志着我国的网络安全攻防演习进入试验阶段。当年，我国举行第一场实战攻防演习后，迅速将我国网络安全实战演习推上日程，为日后发展打下了坚实基础。试验阶段，世界上著名的“网络风暴”“锁盾”等一系列网络攻防演习行动，为我国实战攻防演习发展提供了参考。

在各部门的高度重视下，演习范围越来越广，参演单位数量和涉及行业逐年增多。五年里，我国实战攻防演习走向规模化，参演单位与组织不断增加。2020 年，监管机构和各行业都开展了实战攻防演习，在实战演习中诞生了一大批网络安全尖兵。

演变二
演习规则向成熟化演变

随着国内实战攻防演习的规模逐渐扩大，演习规则也在逐年完善，覆盖面更全，内容更贴合实战，在发展过程中渐渐成熟。

从规则设置看，数量逐年增加，规则进一步细化，要求更严。对攻击方而言，要尽可能地找出系统中存在的所有安全问题，穷尽所有已知的攻击方法，达到让终端、边界、目标系统失陷的目的；对防守方而言，要进行网络安全监测、预警、分析、验证、处置等一系列工作，并在后期复盘总结现有防护工作中的不足之处，为后续常态化的网络安全防护措施提供优化依据。

从具体内容看，规则制定紧贴网络安全发展形势，向实战化倾斜。比如，针对 APT 攻击，要求防守方做到在攻击发生后，不仅要保证损失降到最低，更要掌握是谁、通过何种方式、进入我们的系统做了什么。同时，针对网络安全“一失万无”的特性，除了保护目标系统外，也要保护相关的业务安全运营，在演习中培养从业者的全局意识。

演变三
演习频度向常态化演变

在监管部门、政企机构的高度重视下，实战攻防演习影响力进一步扩大，逐渐走向常态化。一年一度的实战攻防演习周期逐渐拉长。同时，更多政企机构开始利用攻防演习检测自身的网络安全能力，从而为后续网络安全建设指路。

网络攻击突破空间限制，攻击速度快，随时可能发生，因应实战要求，攻防演习对抗周期逐年拉长。在贴合实战的攻防博弈中，防守方必须进行全天候、全方位的网络安全态势感知，增强网络安全防御能力和威慑能力。

实战攻防演习成为政企机构网络安全防御能力的常态化检查手段。只有打一遍，在攻防对抗中发现问题解决问题，才能针对特定问题进行建设规划，全面提升网络安全能力。现在很多大型政企机构都希望专业的网络安全服务商，先给他们做一次实网攻防演习，之后再通过演习结果来进行定制化的网络安全规划与设计服务。只有不断进行网络攻防演习和渗透测试，安全防御能力才能不断提升，从而应对不断变化的新型攻击和高级威胁。

演变四
攻击手段向多样化演变

随着演习经验的不断丰富和大数据安全技术的广泛应用，攻防演习的攻击手段不断丰富，开始使用越来越多的漏洞攻击、身份仿冒等新型作战策略，向多样化演变。

2016 年，网络实战攻防演习处于起步阶段，攻防重点大多集中于互联网入口或内网边界。从演习成果来看，从互联网侧发起的直接攻击普遍十分有效，系统的外层防护一旦被突破，横向移动、跨域攻击，往往都比较容易实现。

2018 年，防守方对攻击行为的监测、发现能力大幅增强，攻击难度加大，迫使攻击队全面升级。随着部分参与过演习的单位防御能力大幅提升，攻击队开始尝试“更隐蔽”的攻击方式。比如，身份仿冒、钓鱼 WiFi、供应链攻击、邮箱系统攻击、加密隧道等攻击手段，攻防演习与网络实战的水平更加接近。

2020 年，传统攻击方法越来越难取得成效，攻击队开始研究应用系统和安全产品中的漏洞发起攻击。比如，大部分行业都会搭建 VPN 设备，可以利用 VPN 设备的一些 SQL 注入、加账号、远程命令执行等漏洞开展攻击，也可以采取钓鱼、爆破、弱口令等方式来取得账号权限，绕过外网打点环节，直接接入内网实施横向渗透。

网络安全实战演习是攻防对抗的过程，攻击手段的多样化，最终目的是为了提升网络安全防护能力，应对不断变化的网络安全威胁。

演变五
安全防御向体系化演变

习总书记在中央政治局第二十六次集体学习时强调，“要坚持系统思维，构建大安全格局”。近几年的实战攻防演习充分证明，没有攻不破的网络，没有打不透的“墙”。面对多样化的网络攻击手段，不能临阵磨枪、仓促应对，必须立足根本、打好基础，用系统思维开展体系化的网络安全建设。

网络安全防护思路，亟需从过去的被动防御走向主动防御。被动防御可以理解为“事后补救”，采用的隔离、修边界等技术方法，是局部的、针对单点的，安全产品之间缺乏联动。这种“头痛医头脚痛医脚”、“哪里出问题堵哪里”的防御思路，已经不再适应当前的网络安全形势。

主动防御，可以理解为“事前防控”，将关口前移，做到防患于未然。在实战演习完成后，应对现有安全架构进行梳理，以安全能力建设为核心思路，重新设计企业整体安全架构，通过多种安全能力的组合和结构性设计，形成真正的纵深防御体系。

结语：

未来，随着云计算、大数据、人工智能等新型技术的广泛应用，信息基础架构将变得更加复杂，网络攻击面不断扩大，带来更多新型威胁。在这样的趋势下，只有更好地提升实战攻防演习水平，建立全面完善的纵深防御体系，才能真正具备有效应对高级威胁的防护能力。安

攻防演习暴露十大薄弱环节

作者 公关部 李建平
安全服务团队顾鑫

实战攻防演练已成为检验参演机构网络安全防御能力和水平的“试金石”、照妖镜，成为应对网络攻击能力的“磨刀石”。

近年的实战攻防演练中，针对大型网络的攻击一般会组合利用多种攻击方式：0day 攻击、供应链攻击、进攻流量隧道加密等各种招数齐上……面对此类攻击时，传统安全设备构筑的防护网有些力不从心，暴露出诸多问题。

总的来看，实战攻防演练中主要暴露出以下十大薄弱环节：

薄弱环节一

互联网应用系统常规漏洞过多

在历年的实战攻防演习期间，已知应用系统漏洞、中间件漏洞以及因配置问题产生的常规漏洞，是攻击方发现的明显问题和主要攻击渠道。

比如，攻防演习期间发现了较多的通用中间件未修复漏洞，其中 Weblogic 应用比较广泛、存在反序列化漏洞，常被作为打点和内网渗透的突破点。

此外，针对所有行业基本上都有的对外开放的邮件系统，可以针对邮件系统漏洞，譬如跨站漏洞、XXE 漏洞来针对性开展攻击。

2020 年曝出的安全漏洞大幅增加、再创新高，其中 Web 应用是漏洞的“主力军”。根据国家信息安全漏洞共享平台（CNVD）的数据，收录安全漏洞数量同比增长了 28.0%，共计 20,704 个，2016 年以来年均增长率为 17.6%。

薄弱环节二

互联网敏感信息泄露明显

网络拓扑、用户信息、登陆凭证等敏感信息在互联网大量泄露，成为攻击方突破点。针对暗网的调查发现，与政企机构网络登录凭证等相关信息的交易正在蓬勃发展。2019 年第四季度，暗网市场网络凭证数据的交易数量开始有所上升，出售的数量就相当于 2018 年全年的总和。2020 年第一季度，暗网市场销售的网络登录的帖子数量比上一季度猛增了 69%。暗网出售的网络登陆凭据涉及政府机构、医疗机构以及其他社会组织。

实际上，2020 年是有记录以来数据泄露最糟糕的一年。根据 Risk Based Security 的报告，2020 年第一季度公开报告的泄露数据量同比增长了 273%。2020 年，公开报告的数据泄露事件总量达 370 亿条，比 2019 年数据泄露数量增长 141%，达到历史新高，其中仍有 1923 起数据泄露事件 (49%) 没有确定的数据泄露量。

大量互联网敏感数据泄露，为攻击者进入内部网络和开展攻击提供了便利。

薄弱环节三

互联网未知资产 / 服务大量存在

在攻防演练中，资产的控制权和所有权始终是攻防双方的争夺焦点。互联网暴露面作为流量的入口，攻击方重要的攻击对象，降低互联网资产风险是防守方最主要的工作。

资产不清是很多政府单位面临的现状。数字化转型带来的互联网暴露面不断扩大，政企机构资产范围不断外延。除了看得到的“冰面资产”之外，还有大量的冰面之下的资产，包括无主资产、灰色资产、僵尸资产等。

在实战攻防演习中，一些单位存在“年久失修、无开发维护保障”的老 / 旧 / 僵尸系统，因为清理不及时，容易成为攻击者的跳板，构成严重的安全隐患。根据奇安信安全服务团队的统计，在实战攻防演习前期对机构的体检中，经常能够发现未及时得到更新的老旧系统。因为历史遗留的原因，以及管理混乱的问题，攻击队可以通过分析老旧系统的已知漏洞，成功攻入内部网络。

政企机构可以采取减少互联网连接通道、归拢外网访问出口，关闭容易被利用的高危端口、下线非必要的未知资产、整改不安全的已知资产等做法，尽量减少风险的暴露面。从提升安全性来看，建议政企机构推动老旧 IT 资产升级、修复问题资产。

薄弱环节四

网络及子网内部安全域之间隔离措施不到位

网络内部的隔离措施是考验企业网络安全防护能力的重要环节。由于很多机构没有严格的访问控制（ACL）策略，在 DMZ 和办公网之间不做或很少有网络隔离，办公网和互联网相通，网络区域划分不严格，可以直接使远程控制程序上线，令攻击方可以很轻易的实现跨区攻击。

大中型政企机构还存在“一张网”的情况，习惯于使用单独架设专用网络，来打通各地区之间的内部网络连接，不同区域内网间也缺乏必要的隔离管控措施，缺乏足够有效的网络访问控制。这就导致攻击方一旦突破了子公司或分公司的防线，便可以通过内网进行横向渗透，直接攻击到集团总部，或是漫游整个企业内网，进而攻击任意系统。

在实战攻防演习中，面对防守严密的总部系统，攻击方很难正面突破，直接撬开进入内部网络的大门。绕过正面防御，尝试通过攻击防守相对薄弱的下属单位，再迂回攻入总部的目标系统，成为一种“明智”的策略。

薄弱环节五

第三方 / 专网接入安全防护措施过于单薄

互联网出口和应用都是攻入内部网络的入口和途径。目前政企机构的接入防护措施良莠不齐，给攻击者创造了大量的机会，给防守工作带来巨大压力。

针对 VPN 系统等开放于互联网边界的设备或系统，为了避免影响到员工使用，很多政企机构都没有在其传输通道上增加更多的防护手段；再加上此类系统多会集成统一登录，一旦获得了某个员工的账号密码，攻击方可以通过这些系统突破边界直接进入内部网络中来。

此外，防火墙作为重要的网络层访问控制设备，随着网络架构与业务的增长与变化，安全策略非常容易混乱，甚至一些政企机构为了解决可用性问题，出现了“any to any”的策略。防守单位很难在短时间内梳理和配置几十个应用、上千个端口的精细化访问控制策略。缺乏

访问控制策略的防火墙，就如同敞开的大门，安全域边界防护形同虚设。

薄弱环节六

内网安全检测能力不足

攻防演习中，攻击方攻击测试，对防守方的检测能力要求更高。网络安全监控设备的部署、网络安全态势感知平台的建设，是实现安全可视化、安全可控的基础。部分企业采购部署了相关工具，但是每秒上千条报警，很难从中甄别出实际攻击事件。

此外，部分老旧的防护设备，策略配置混乱，安全防护依靠这些系统发挥中坚力量，势必力不从心。流量监测及主机监控工具缺失，仅依靠传统防护设备的告警去判断攻击、甚至依靠人工去翻阅海量的日志，导致“巧妇难为无米之炊”。

更重要的是，精于内部网络隐蔽渗透的攻击方，在内部网络进行非常谨慎而隐蔽的横向移动，很难被流量检测设备或态势感知系统检测。

网络安全监控是网络安全工作中非常重要的方面。重视并建设好政企机构网络安全监控体系，持续运营并优化网络安全监控策略，是政企机构真正可以经受实战化考验的重要举措。

薄弱环节七

内网主机 / 应用漏洞大量存在，集权系统管控不严格

主机承载着政企机构关键业务应用，需重点关注、重点防护。但很多机构的内部网络的防御机制脆弱，在实战攻防演练期间，经常发现早已披露的陈年漏洞未修复，特别是内部网络主机、服务器以及相关应用服务补丁修复不及时，成为攻击队利用的重要途径，从而顺利拿下内部网络服务器及数据库权限。根据 2020 年实战攻防演习总结来看，内部网络的隐患占到 47%，排名第一，其大多数表现为内网大批漏洞不修复。

集权类系统成为攻击的主要目标。在攻防演习过程中，云管理平台、核心网络设备、堡垒机、SOC 平台、VPN 等集权系统，由于缺乏定期的维护升级，已经成为扩大权限的突破点。 集权类系统一旦被突破，整个内部的应用和系统基本全部突破，可以实现以点打面，掌握对其所属管辖范围内的所有主机控制权。

薄弱环节八

安全设备 / 系统自身安全性不够

安全设备作为政企机构对抗攻击者的重要工具，其安全性应该相对较高。但实际上安全产品自身也无法避免 0Day 攻击，安全设备自身安全成为新的风险点。每年攻防演习都会爆出某某安全设备自身存在某某漏洞被利用、被控制，反映出安全设备厂商自身安全开发和检测能力没有做到位，给攻击人员留下了“后门”，形成新的风险点。2020 年实战攻防演习中的一大特点是，安全产品的漏洞挖掘和利用现象非常普遍，多家企业的多款安全产品被挖掘出新漏洞（0day 漏洞）或存在高危漏洞。有人戏称，2020 年实战攻防演习实际上主要是检验安全设备的安全性。

历年攻实战防演习中，被发现和利用的各类安全产品 0Day 漏洞，主要涉及安全网关、身份与访问管理、安全管理、终端安全等类型安全产品。这些安全产品的漏洞一旦被利用，可以使攻击方突破网络边界，获取控制权限进入网络；获取用户账户信息，并快速拿下相关设备和网络的控制权限。

根据 2010 年至今 CNVD 共发布 2097 个有关安全产品的漏洞，其中涉及国外安全产品的漏洞有 1459 个，占比达到 70%，涉及国内安全产品的漏洞有 428 个，占比为 20%，通用型漏洞（涉及多品牌）210 个，占比为 10%。根据 CNVD 公开数据整理安全产品漏洞中，截止 2020 年 10 月份披露的高危漏洞数量达到 122 个，已超过历史年度最高值。

薄弱环节九

供应链风险管控不到位

在攻防演习过程中，随着防守方对攻击行为的监测、发现和溯源能力大幅增强，攻击队开始更多地转向供应链攻击等新型作战策略。

攻击方会从 IT（设备及软件）服务商、安全服务商、办公及生产服务商等供应链机构入手，寻找软件、设备及系统漏洞，发现人员及管理薄弱点并实施攻击。常见的系统突破口包括：邮件系统、OA 系统、安全设备、社交软件等；常见的突破方式包括软件漏洞，管理员弱口令等。

由于攻击对象范围广、攻击方式隐蔽，供应链攻击成为攻击方的重要突破口，给政企安全防护带来了极大的挑战。从奇安信在 2020 年承接的实战攻防演习情况来看，由于供应链管控弱，软件外包、外部服务提供商等成为迂回攻击的重要通道。

薄弱环节十

员工安全意识淡薄，专业安全人员短缺

很多情况下，“搞人”要比“搞系统”容易得多。利用人员安全意识不足或安全能力不足，实施社会工程学攻击，通过钓鱼邮件或社交平台进行诱骗，是攻击方经常使用的手法。

钓鱼邮件是最经常被使用的攻击手法之一。即便是安全意识较强的 IT 人员或管理员，也很容易被诱骗点开邮件中钓鱼链接或木马附件，进而导致关键终端被控，甚至整个网络沦陷。在历年攻防演练过程中，攻击队通过邮件钓鱼等方式攻击 IT 运维人员办公用机并获取数据及内网权限的案例数不胜数。

人是支撑安全业务的最重要因素，专业人才缺乏也是政企机构面临的挑战之一。在攻防演习期间，大量防守工作需要开展，而且专业性较强，要求企业需要配备足够的专业化网络安全人才队伍。安

奇安信
新一代网络安全领军者

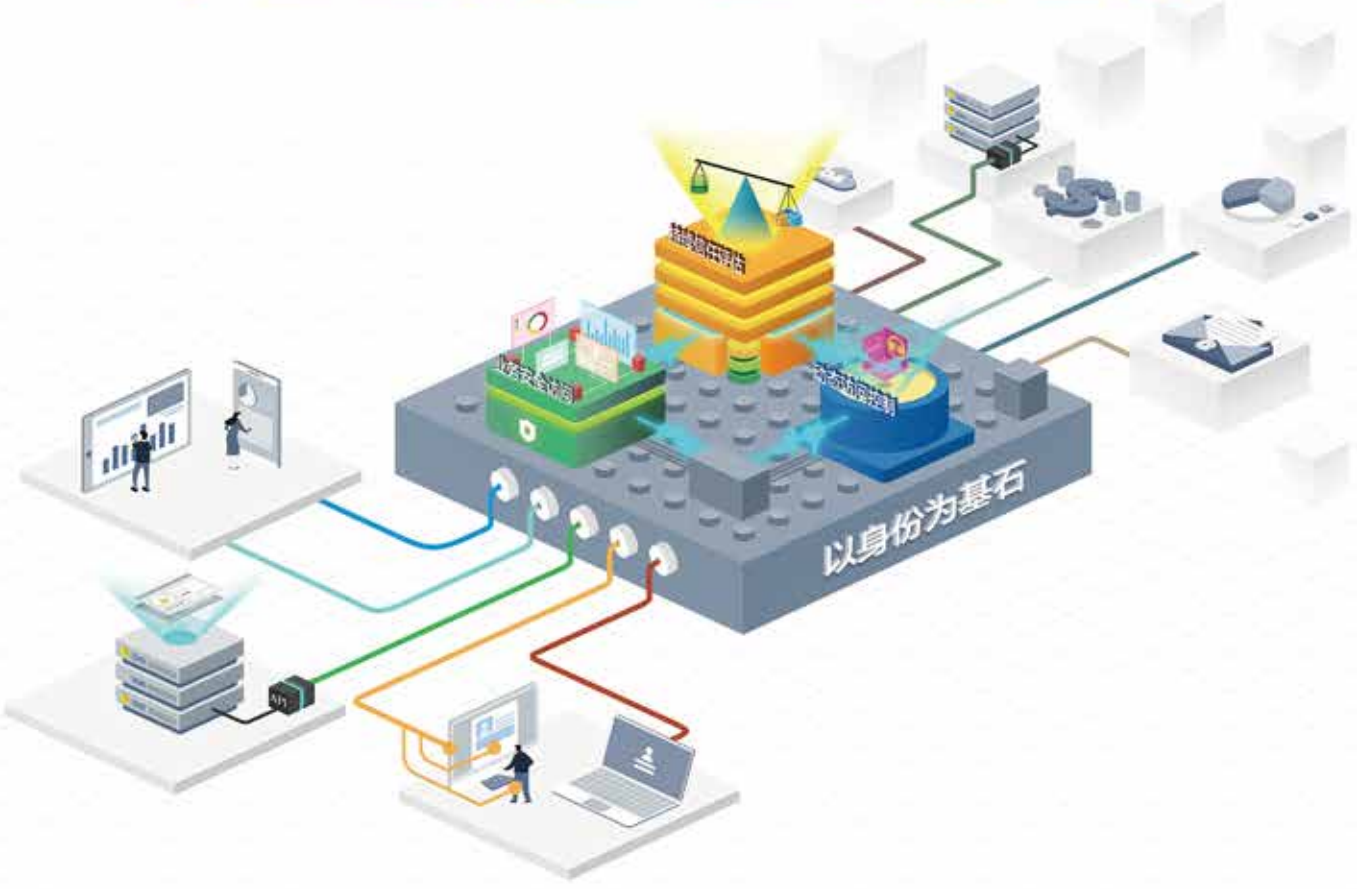
让网络更安全 让世界更美好

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

九大措施应对网络攻击“七十二变”

作者 公关部 魏开元

从近两年的实战攻防演习来看，攻击队使用的手法可谓是“七十二变”，包括 0day 漏洞的广泛利用、软件以及服务供应链的攻击、基于人性弱点的社会工程学攻击、WiFii 钓鱼攻击甚至是物理攻击纷纷登场，着实让防守队感到“压力山大”。

在 2020 年某次实战攻防演习期间，多次出现因安全产品的 0day 漏洞或者不当配置被攻击队成功打穿的情况，也出现了针对防守队的攻击溯源行为，攻击队反向部署欺骗诱捕系统（蜜罐），从而获取了防守方部分系统登录口令，实现二次渗透的反转案例。

对此，奇安信基于多年实战攻防经验，针对防守方的战前准备、攻防对抗和事后溯源总结三个阶段，提出了建立基于可持续监测分析和响应的协同防护模式，具体而言包括九大举措。

举措一

梳理资产，知彼先知己

近几年，各大政企机构的信息化建设非常迅速，IT 资产数量也成倍提升，使得内部资产管理变得更加困难。但在实战过程中，每一台直接或间接暴露在公网的资产，都有可能成为攻击队的目标。因此在战前准备阶段，防守方必须清楚掌握防守目标所有的在线资产，其目标在于明确资产归属，下线无主、没必要且高风险的资产。

资产主要包括三大类。第一类是 IT 硬件资产，主要包括内外部应用系统、PC/ 服务器资产、网络设备、安全设备、IP 资产特权终端；第二类是软件资产，包括但不限于操作系统、中间件、数据库、开源组件、大数据 / 虚拟化平台；第三类是互联网链路资产，主要包括总部、分支机构以及各大业务网点的互联网出口。

值得注意的是，在梳理资产的同时，需要和供应商相对应，在发现漏洞或其他不当配置时，可快速响应处置。

举措二

防微杜渐，收缩攻击面

很多时候，防守方失陷的原因，在于一些很小的目标，甚至可能是某位员工在社交网站的一次发帖或者一个开放的打印机端口。在实战过程中，攻击队对于目标的情报收集能力是惊人的，他们往往能从最不起眼的信息或者资产开始寻根溯源，最终找到目标的关键信息，如组织架构、登录口令、重要源代码等等。

因此在战前准备阶段，防守队通过网络扫描、网络爬虫等多种技术，主动探测用户在互联网上暴露的资产和敏感信息，协助用户梳理出互联网资产全景图，对暴露信息进行清理或隐藏，降低被攻击队利用风险十分必要。另外在条件允许的情况下，还可充分利用部分暴露信息制作“陷阱节点”，在部署欺骗诱捕系统（蜜罐）时配合使用，达成对攻击队欺骗诱捕的目的。

另外，在正式的攻防演习开始之前，防守队内部还可开展一次预演。结束后，参演人员对演习过程中发现的问题进行总结，包括是否存在系统漏洞、安全设备策略是否有缺陷、监测手段是否有效等，针对性提出整改计划和方案，并为后续工作积累经验。

举措三

完善纵深防御体系

在攻防对抗阶段，防守方需尽量避免发生这样一种现象，即攻击者一旦突破内网边界，便能够肆意在内网横向移动。这就要求防守队必须构建起多批次、大纵深的防御体系，让攻击者每前进一步，都需要付出更高的成本，甚至迫使攻击者放弃攻击行为。

对此，奇安信提出了基于威胁情报的检测能力 + 核心资产防御 + 人的纵深防御体系，除了在网络边界部署入侵检测系统、防火墙和 VPN 网关等边界防护产品外，还应在网络侧部署天眼，实现高级威胁和异常流量的检测与分析；在服务器侧部署椒图，实现服务器加固和针对服务器内部的检测与响应；在终端侧部署天擎，实现终端安全的统一管控和检测与响应；在邮件服务器部署邮件威胁检测系统，实现对鱼叉邮件、带毒邮件、钓鱼邮件的精准检测；部署 NGSOC，对所有安全事件进行统一管理，监测企业内部整体网络安全态势……在此基础上，引入威胁情报，强化监测能力。

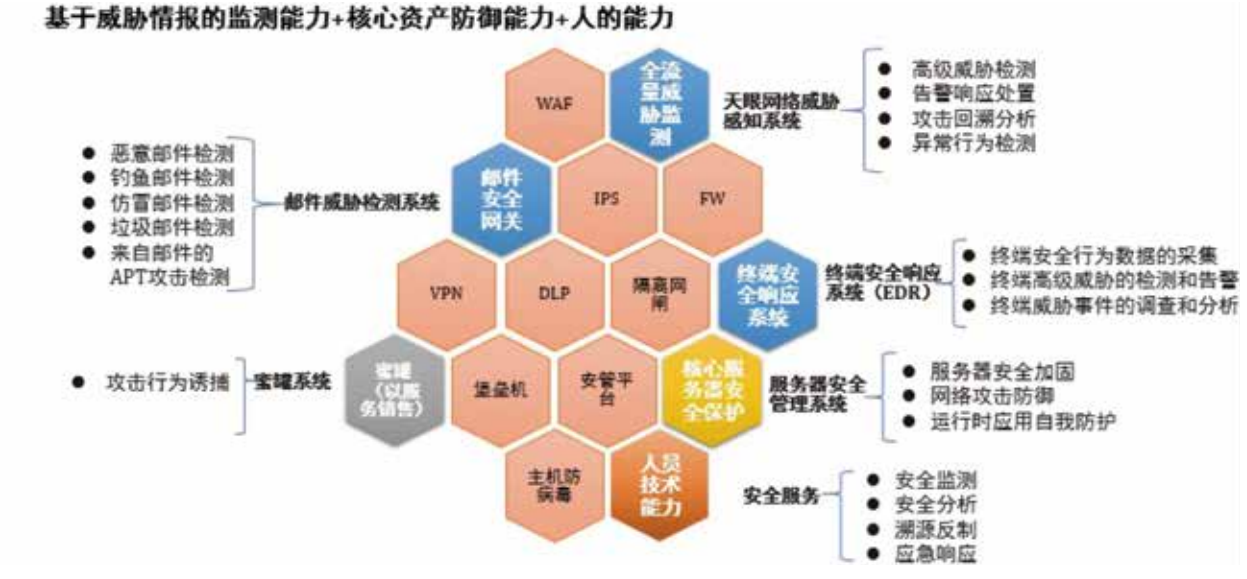
举措四

构建内网的主动防御能力

只有防御纵深还不够，防守方依然处于一个“被动挨打”的局面。在真正的战争中，有利条件下局部的反冲锋，往往能带来非常积极的防御效果。对于网络安全实战而言，防守队在内网实施主动出击，同样十分重要。

通常而言，构建内网的主动防御能力，需要全面覆盖互联网接入、办公网接入、分支机构接入、第三方供应商接入、专网接入、VPN 接入和关键系统，收集内网全量数据（包括流量数据和日志数据等），利用大数据技术、关联分析引擎，找出内网中可能存在攻击事件和异常行为。

例如在流量侧，奇安信天眼能够采集全流量进行拆包检测，并将所有网络会话，如 DNS、URL 等信息都记录下来，可用于针对攻击队伍的溯源分析。同时，天眼针对加密流量的检测也有很好的效果。而在服务器侧，椒图能够主动采集内网服务器东西向流量进行统一检测，针对 Webshell、SQL 注入甚至 0day 攻击，都有很好的检测效果。一旦发现内网服务器失陷，还可通过微隔离技术，主动隔离失陷服务器，防止进一步扩散感染。



举措五

提升基于情报的精准防御能力

情报通常包括两个方面，一方面是描述攻击行为的威胁情报，另一方面是描述漏洞行为的漏洞情报。无论是哪种情报，都能够降低安全设备的误报率和漏报率，从而提升防守队的处置效率。

在威胁情报方面，对于经过分析已经确认的攻击事件，防守队可将攻击事件涉及的IP地址、攻击方式、域名、攻击者相关信息、攻击行为和相关威胁情报上传至云端威胁情报平台，平台会自动将该情报与其他防守队提交的情报进行关联，再下发至所有安全设备，并进行统一分析工作。

在漏洞情报方面，防守队可将每日收集到的漏洞相关情报提交至补天漏洞平台，由补天后端小组等奇安信二线实战攻防专家进行统一研判后，再实时发布给前端项目经理及漏洞提交者，同时推动安全设备进行统一规则更新，实现对漏洞利用的精准检测。

举措六

重点守护核心资产和数据，坚守最后一道防线

除常规武器外，防守队还应针对重点目标进行重点加固，以防“漏网之鱼”。

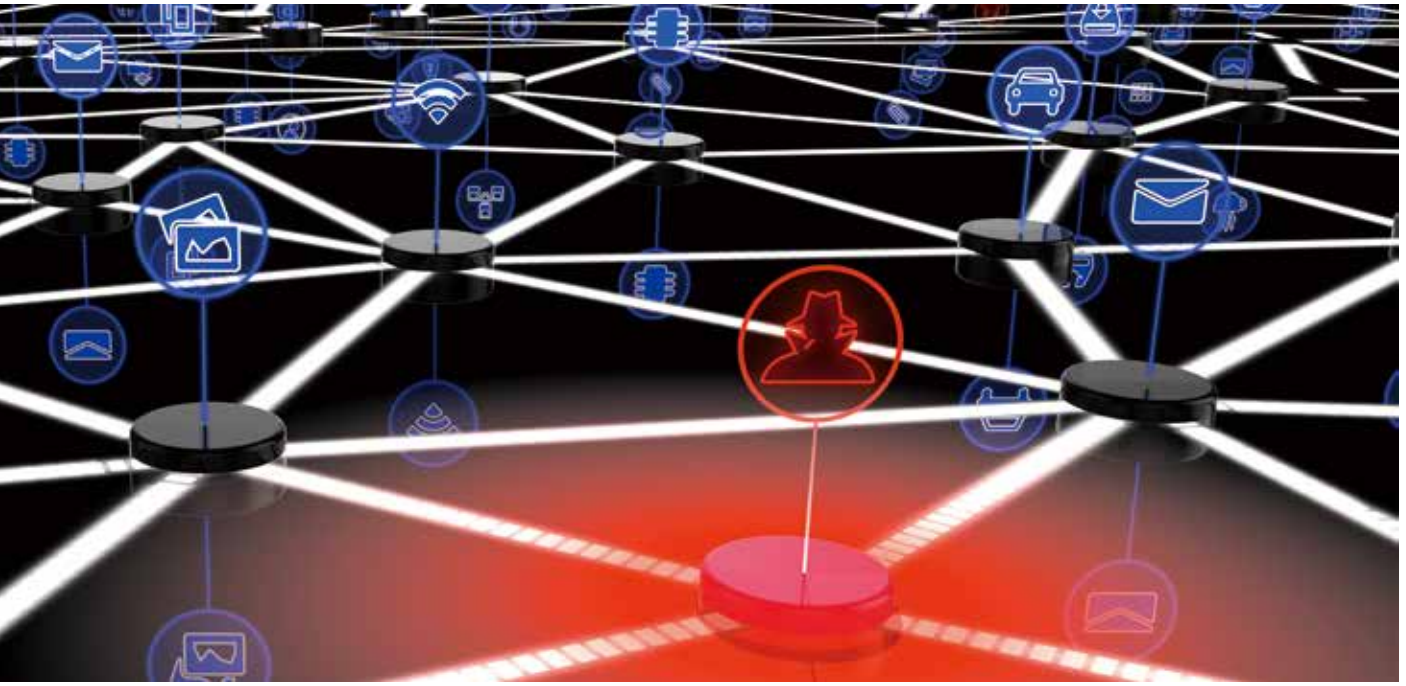
第一点是针对内网的集权系统（域控、OA、云平台、大数据平台）等系统开展安全评估及安全加固；第二点是针对报备的核心目标系统，加强内部网络隔离和主机防护，并采用白名单措施保障其安全性；第三点是针对重点安全产品（包括防火墙、杀毒软件等）进行重点加固，尤其是远程代码执行等漏洞的修补工作。

举措七

加强专业化的分析研判与响应处置

网络安全实战攻防演习的本质还是攻击队与防守队之间的对抗，因此在武器之外，防守队的技战术水平，能够很大程度决定结果走向。在防守队伍支持方面，奇安信除派出一线驻场专家外，还设置了大量的威胁分析师、安全运营工程师提供远程支持。2020实战攻防演习期间，奇安信投入一线、二线专家超过3000人，为超过50%的参演单位提供了防守服务。

在攻防对抗期间，驻场防守队伍能够根据告警信息，针对攻击行为的具体特点实时制定攻击阻断的安全措施，详细记录攻击阻断操作，同时配合甲方业务主管单位对业务稳定性进行监测。如遇到可疑样本、0day漏洞等疑难杂症时，二线专家还可提供远程的样本分析、漏洞复现等支持。



举措八

改进联防联控能力，实现高效协同

过去实战攻防演习曾经流行过这么一个段子：通信基本靠吼，处置基本靠手。这个段子在一定程度上反映出了防守队伍在协同联动方面的缺失。

为了弥补短板，防守队应当遵循以下“四化”。第一是防守组织化，总部领导挂帅，总部安全、网络、开发、业务和分支机构联合成立工作组；第二是处置流程化，明确应急预案流程，同时借助自动化工具（SOAR），在值守期间采用电子化流程保证事件处置运转；第三是沟通工具化，采用 IM 通讯工具，在 IM 上工作组细分小组，加强内部沟通，解决沟通靠吼的现状；指挥平台化，使用统一的攻防演习指挥平台、实战化威胁运营平台等工具，实现监控、分析、处置平台一体化管理。

举措九

构建溯源反制能力

在实战攻防演习中，针对攻击队溯源反制是防守队重要的加分项目之一，对接下来的防守部署也具有非常重要的意义。奇安信认为，构建完整的溯源反制能力应该包括以下四个步骤：

1、事前埋点：部署蜜罐系统，在公开渠道（如社交网站）散布虚假消息（代码、账号）和伪装应用；

2、事中监控：监控虚假账号异动、监控蜜罐告警；

3、溯源追踪：攻击 IP 定位、域名反查、域名注册信息查询、恶意代码分析；

4、对抗反制：攻击 IP 的漏洞发现、攻击 IP 漏洞利用、人工溯源信息，甚至利用蜜罐等技术手段，实现对攻击队主机的反向控制。安

“为了和平，我们需要武器。” ——中国原子弹之父邓稼先

2021 实战攻防演习“兵器谱”

作者 虎符智库

无论是战争还是和平年代，武器都是国家安全的重要保障。在网络空间也是如此，习近平总书记曾指出，“网络安全的本质是对抗，对抗的本质是攻防两端能力的较量”。而技术硬核的产品装备，无疑是防守能力的重要保障。

本期《网安 26 号院》重磅推出《实战攻防演习“兵器谱”》，一共精选了奇安信旗下天眼（新一代威胁感知系统）、云锁（服务器安全管理系统）、NGSOC（态势感知与安全运营平台）、天擎（终端安全管理系统）、邮件威胁检测系统、蜜罐（网神攻击诱捕平台）、SOAR（安全编排自动化）、开源卫士等九款产品及解决方案，旨在为每位安全从业人员提供最实用的装备指南。

其中，天眼被誉为实战攻防“标配武器”，物如其名，任何异常流量、网络攻击、高级威胁等都逃不过它的“法眼”；云锁帮助客户构建面向实战化的服务器安全防护能力，为核心业务及数据提供一个固若金汤的防护；NGSOC 凭借强大的安全感知能力、一流的大数据分析技术和安全可视化能力，成为实战场景下的防守“司令部”；天擎作为奇安信安全家族的老大哥，集防病毒、终端安全管控、终端准入、EDR 等功能于一体，在实战化场景下不可或缺。

邮件威胁监测系统虽一向低调，但可以抵御“老生常谈”却屡试不爽的钓鱼邮件攻击，避免让防守方在阴沟里翻船。攻击诱捕平台（蜜罐）将“欺骗防御”演绎到极致，完美诠释“兵不厌诈”的军事哲学。SOAR 在实战中如同一位交响乐指挥大师，让各种安全产品构成的乐队各施所长，协作演奏出一曲曲优美乐章，并可安全处置效率提升十倍以上。开源卫士实现了“正本清源”，从源头阻断来自软件供应链攻击的隐患。

“沙场秋点兵，演习验真功”。从被动防御到主动防御，从事后补救到事前防控，从单兵作战各自为阵到产品协同无缝联动，新的攻击手段、防护技术层出不穷，防守方和攻击方的对抗交锋更加激烈。“兵器谱”上的主角们有更出色的表现。

1 实战攻防演习标配利器：奇安信天眼

在安全服务圈流传着一种说法，“无天眼，不实战！”充分体现了天眼在实战化攻防演习中的重要地位。那么，天眼为何被认为是攻防演习中必不可少的标配，并被列为本次“兵器谱”之首呢？本文就来看看天眼在实战中能发挥哪些作用。

天眼的全称是奇安信新一代安全感知系统，它以攻防渗透和数据分析为核心竞争力，聚焦威胁检测和响应，为安全服务和分析人员提供一套在监测预警、威胁检测、溯源分析和响应处置上得心应手的威胁检测平台。

图：天眼威胁感知系统

和安服组成“最佳 CP” 攻防演习屡立奇功

好武器，用起来才是关键；而好不好用，一线人员说了算！在天眼在攻防演习中之所以拥有优异口碑，注重实战效果，注重一线人员的操作是重要原因。

从 2018 年开始，天眼与安全服务体系进行了整合，奇安信内部将这次调整戏称为这是天眼与安服的联姻。事实证明，这次联姻非常成功，它让天眼最快的速度，

渗入到了广大政企客户攻防对抗的现场一线，产品的实战化水平和防守效果迅速迈上大台阶。天眼、安服可以说是一对“最佳 CP”，两者联袂，立下战功无数。

在 2020 年某部委的实战攻防演习中，通过天眼的日志和流量分析，防守方快速溯源了整个 APT 攻击行为，最终确定是海莲花。在某银行单位的实战攻防演习中，防守方反馈，天眼的全流量检测模式比其他同类产品更加彻底，很好解决漏报难题。更重要的是，天眼的威胁狩猎图非常直观，攻击方何时攻进，访问哪些服务器，对哪些设备攻击，都可以一目了然。

更精准的威胁检测 破解“误报”、“漏报”两大难题

长期以来，让安全人员最头疼的难题，莫过于“误报”和“漏报”。IDC 的最新报告调查了 350 位内部人士、MSSP 安全分析师和管理人员，结果显示，由于广泛的“警报疲劳”导致警报被忽略，以及担心漏报（遗漏安全事件），安全分析师的压力不断增加，而生产力则在下降。在攻防演习中，防守方面临海量“误报”会忙的焦头烂额，而“漏报”更让攻击方有机可乘、轻松攻入。

与传统检测产品基于自身流量发现威胁不同，天眼基于自主研发的 QNA 大数据人工智能威胁检测引擎，创新性的从互联网数据进行发掘和分析，极大提升未知威胁和攻击的检出效率，达到更高的准确率和更低的误报率。

随着攻防演习的不断进阶，新型攻击手法层出不穷，利用 0Day 漏洞攻击屡见不鲜。为此，天眼特别增强了行为分析功能，通过多年积累的成功经验对行为分析进行分类，主要包括 DNS 分析、非常规服务分析、邮件行为分析、登录行为分析等超过 30 种场景，显著增强了未知威胁的检测准确性。

为了提升防守方效率，天眼采用了双向会话 WebIDS 检测引擎，只对攻击成功进行告警，从而大大降低了无效报警数量，让管理人员可以集中应对有效的告警事件。同时，天眼对沙箱技术进行升级，从操作系统层升级到 CPU 指令层级，强大的细粒度检测能力让沙箱逃逸无所遁形。

更全面的溯源分析 实现威胁狩猎可视化

在攻防演习过程中，防守方必须要知道几个答案：谁攻击了我的什么？使用了什么手法？窃取了什么信息？因此，安全人员需要基于攻击链的视角，通过可视化方式，重现整个攻击过程。

对此，天眼具备强大的告警关联分析能力，可以告警和日志进行关联产生精准攻击事件，为精准封禁提供依据，告警和流量日志智能关联分析引擎。同时，它具备全包存储和分析的取证能力，并提供线索可视化图谱拓线分析能力（威胁狩猎），能为企业用户呈现一次攻击的完成过程，帮助防守方对网络攻击进行回溯和深度分析。

图：天眼威胁狩猎可视分析系统

天眼还内置了 ATT&CK 模型，显著提升威胁分析能力，从而能够更加精确、快速的发现和定位攻击者在系统内部的非法活动。

更快速的响应处置效率提升 10 倍以上

实战攻防强调“兵贵神速”，一旦发现威胁告警，防守方需要最短时间能完成处置，避免攻击得手。天眼率先将 SOAR 技术应用于告警的闭环处理，通过自动化编排，让响应处置效率获得了 10 倍以上提升，对

于需要重复性持续性的操作，提升的效率更是数以百倍计。

同时，天眼还能和其他安全产品实现无缝联动，提高响应效率。其中包括通过与防火墙进行 NDR 联动，及时在边界阻断威胁；通过与终端进行 EDR 联动，及时处置失陷主机；通过与流量传感器联动，及时阻断异常流量；与邮件威胁检测系统联动，及时处置异常邮件等等。

图：天眼威胁事件态势呈现

更好用的产品体验 小白也能看得懂、用起来

天眼结合了一线分析人员的操作习惯，将整个界面逻辑和交互进行持续优化，进行了重新调整，引入了极其便利的工作台概念，易用性方面基于一百多条的场景需求，通过多达 50 多次的原型设计和不断打磨，使得整个产品的交互和易用性得到大幅提升。

天眼还通过对系统底层的优化来提升用户体验。如原来的仪表板页面在处理超过 30 天大数据量情况下页面响应速度从平均 10 几秒降低到 2-3 秒，页面响应速度提升 5-6 倍。

2020 年天眼获得多项荣誉，在数世咨询中获得应用创新力和市场执行力“双第一”，并荣膺全球权威咨询机构 Frost&Sullivan 的“2020 年中国威胁检测与响应 (TDR) 市场领导奖”，以及美国知名权威网络安全杂志《Cyber Defense Magazine》(简称 CDM) 颁发的“Next Gen (下一代) ”大奖。

在实战攻防演习规模不断扩大、走向常态化的浪潮之下，在公安部提出了的“三化六防”新思想的背景下，为实战而生的天眼，已经成为各大政企单位攻防演习中不可或缺的标配。

2 服务器安全“守护神”：奇安信椒图云锁

在历年实战攻防演习期间，云锁就多次帮助防守队发现 0day 攻击。

服务器作为承载数据资产和业务管理的基础设施，其安全防护的重要性日益凸显。服务器安全防护已经成为网络安全的“最后一道防线”。

与此同时，有公开调研显示，服务器的漏洞修复不及时、端口管理不当、账户弱口令、过高权限、系统或应用配置不合规等问题，都有可能造成严重的主机安全事故，例如企业业务中断、数据被窃取、加密勒索或意外宕机等，带来不可估量的经济损失。

为帮助客户构建面向实战化的服务器安全防护能力，奇安信集团椒图事业部旗下云锁服务器安全管理系统 (简称云锁)，能够从战前准备、攻防对抗、回溯分析三个阶段构建服务器端防护体系。

产品简介

云锁基于服务器端轻量级软件 Agent，安全加固服务器操作系统及应用，通过 IN-APP WAF 探针、RASP (应用运行时自我保护) 探针、内核加固探针能有效检测与抵御针对服务器的黑客攻击和恶意代码；同时云锁融合资产清点、漏洞 & 补丁检测、恶意代码检测、进程行为清点 、基线检查等强大功能，帮助用户构建服务器端事前加固、事中防御、事后追溯的闭环管理体系。

产品架构

产品采用 B/S 架构，分为服务器 Agent 端、Web 管理端及管理中心三部分。

服务器 Agent 端：提供产品安全检测能力，实现对

部署服务器的资产收集，风险扫描，行为监控，入侵检测，攻击防御，系统加固，风险处置等多种安全能力。

Web 管理端：产品管理、报告查看、权限配置

管理中心：采用微服务架构，实现服务器统一管理及数据分析，具备资产分析引擎，Webshell 沙箱，EDR 行为分析引擎，事件分析引擎，弱口令分析引擎，行为学习引擎，威胁情报以及 SSK（Server Security kernel）核心引擎。

战前准备：全面梳理服务器资产风险点与暴露面

随着企业 IT 规模的不断扩大，各类服务器数量成倍增长，其管理和防护难度可想而知。防守方如不能明确掌握各类服务器资产以及相关行为的状况，对危险端口暴露、漏洞未修复、账户弱口令、白应用被黑利用等安全风险不能实时掌控，则很难部署具有针对性的防护方案，给攻击队伍留下可乘之机。云锁能够通过以下几项能力帮助防守方梳理在线资产，找出风险点，缩小黑客攻击面。

第一，自动化资产梳理及风险检测。云锁能够自动化识别进程、账户、端口、网络连接、内核模块等重要资产信息，并基于发现的服务器资产可以实现补丁漏洞检测、Webshell 检测、弱口令检测，帮助防守队伍提前发现资产安全风险，做好安全加固工作，减少黑客攻击面。

第二，暴露端口梳理。云锁能够自动识别出暴露在互联网中的业务端口，帮助用户快速梳理整个业务信息系统的暴露面，支持用户自主添加端口进行入站 IP 的学习，形成可信 IP 列表，从而对异常访问进行告警或阻断。

第三，主机外连管控。云锁可自动分析服务器应用的外部访问日志，梳理外网 IP 和域名连接清单，用户可根据实际情况，创建访问规则并将其应用到服务器上。当连接非白名单 IP 或域名时，则产生事件告警并记录为异常外连。

第四，行为学习与白名单机制。除常规的资产、配置、漏洞和补丁管理外，云锁还能够利用机器学习技术，学习服务器内各项服务的命令执行、文件创建、网络连接等各类行为的时序图，建立应用白名单和行为基线。在对抗时期，一旦发现执行了不在白名单内的应用、相关进程或者其他偏离行为基线的行为，即可产生告警，能够在不依赖具体漏洞的情况下，发现利用未知漏洞（尤其是 0day）的攻击行为。

攻防对抗：持续检测与响应，威胁无所遁形

无论战前的准备如何充分，攻击队总是能够利用各种各样的手段如（0day 攻击等）突破外围防御。此时，针对服务器内部的持续检测与响应，就显得至关重要，这也是云锁的核心优势所在。云锁能够从攻防角度出发，通过内核探针、RASP 探针、IN-APP WAF 探针、Webshell 沙盒、无文件攻击检测引擎等多项检测技术，构建服务器异常行为检测模型（知彼）。

第一，IN-APP WAF 探针。云锁 IN-APP WAF 探针是嵌入在 web 中间件中的流量过滤插件，通过代理 http 请求来匹配 WAF 规则，针对加密流量的检测和过滤能力更强，可以有效防御已知类型的 Web 应用攻击。

第二，RASP 探针。工作于 ASP、PHP、Java 等脚本语言解释器内部，通过 HOOK 函数的方式，可以细粒度的监控应用脚本的行为及函数调用上下文信息，及时发现恶意代码和漏洞利用行为。RASP 能有效防御新型 SQL 注入、任意命令执行、文件上传、任意文件读写、Weblogic 反序列化、Struts2 等基于传统签名方式无法有效防护的应用漏洞，是对 IN-APP WAF 的有效补充。

第三，内核加固探针。通过内核驱动增强操作系统自身对抗黑客攻击和恶意代码的能力，限制漏洞利用后下一步行为。内核加固探针工作于系统层，会对文件篡改、反弹 shell、进程自我复制、监听原始套接字等黑客在入侵产生的多种异常行为进行监控及防护。

第四，Webshell 动态检测。对于服务器上可执行的 Web 脚本类型文件，会进行本地扫描，并上传至云中心沙盒（脚本虚拟机）进行检测，基于沙盒虚拟执行和污点追踪技术，可以有效检测各种加密、变形的 Webshell，并将检测结果返回服务器本地的 WAF 和 RASP 引擎。

事后：精准溯源分析

网络攻击的溯源分析从来不是一个简单的事情，它

依赖于全量日志的记录与分析，其价值在于了解攻击者的意图、实力等，针对性采取合适的对策。正如有专家所说，溯源可使防守队了解攻击者的意图，也就能采取合适的对策。而从漏洞修复的角度看，知道是谁在攻击，确定漏洞修复的优先级会更容易。

云锁可实现服务器上进程、文件、网络行为的全量监控，并通过管理中心的 EDR 行为引擎 & 威胁情报引擎进行分析匹配，实现 APT 攻击的检测，并可为威胁狩猎平台、大数据分析平台提供服务器行为数据支撑。

总而言之，云锁作为国内领先的服务器安全产品，在国际上率先达到 Gartner 定义的 CWPP（云工作负载保护平台）标准、EDR（终端检测与响应）+EPP(Endpoint Protection Platform) 标准，兼容多种虚拟化架构和操作系统，可以说是实战环境下，实现服务器端事前加固、事中防御、事后追溯闭环管理的安全利器。

3 实战防守“司令部”：奇安信 NGSOC

历届实战攻防演习排名靠前的防守机构中，多家使用奇安信 NGSOC 作为主力监控平台。

实战攻防对抗形势日趋激烈，安全管理者难以有效地摸家底、识风险、控态势，安全运营人员缺乏深度检测、持续监测、精准预警、趋势研判、追踪溯源、运营保障等方面能力。政企机构亟需提升实战化安全能力，加强安全运营人员能力和持续的运营体系建设。

图：NGSOC 安全监测大屏

奇安信网神态势感知与安全运营平台（简称 NGSOC）具备强大的实战能力，结合奇安信专业的安全运营团队，可以有效强化政企机构实战化安全能力。在往届国家级实战攻防演习中，奇安信 NGSOC 曾发现多起 0day 攻击事件和大量新型攻击手法，协助防守方取得优秀的成绩。历届演习排名前十的防守机构中，多家使用 NGSOC 作为主力监控平台。

下面介绍 NGSOC 在实战化中的应用场景。

图：NGSOC 实战攻防演习作战策略

战前准备：自查整改，强化安全基线

战前阶段，防守方的主要工作是自查整改，清查被防护业务系统涉及的资产及其暴露面，并进行修补整改。

图：资产和脆弱性闭环管理

第一，资产和脆弱性梳理。自查整改工作的重点是对被防护业务系统的资产与脆弱性进行梳理，NGSOC

能够提供一个完整的闭环管理工具，包括资产梳理、脆弱性梳理、闭环处置、持续监测等。

第二，快速接入日志数据。NGSOC 拥有丰富的数据理解能力、可视化的交互式解析配置、灵活的部署方式，可以快速接入日志数据，为战中的集中监测、分析、溯源提供数据支撑。

战中阶段：攻防对抗，监测异常与 0day 攻击

实战演习期间，核心工作是攻防对抗，对威胁的监测、发现及快速处置成为关键。

第一，超前威胁预警和指挥。在攻防对抗中，发生大规模重大攻击时，防守方需要第一时间了解是否遭受到攻击？首个被攻击的资产？影响了哪些部门？攻击的范围有多大？影响面趋势情况？事件整体处置情况？NGSOC 具备威胁超前预警功能，在发生重大攻击时，第一时间通过平台下发威胁预警包，快速解决以上问题，对已发生和有可能发生的威胁态势进行全面掌控。

图：威胁预警态势大屏效果图

第二，攻防态势统一指挥。NGSOC 预置了众多维度的态势监测大屏，其中针对实战攻防场景专门推出了攻防演练监控态势大屏和攻击者态势大屏，包含安全部署情况、攻击源监控、威胁监控、目标资产监控等信息。安全管理人员能够从宏观态势纵览整个战场，掌握当前的攻防情况并作出指挥决策。

图：攻防演练指挥大屏

第三，威胁快速建模。攻防对抗过程中，如攻击方使用了新型攻击手法或 0day 漏洞，绕过现有的检测措施，实现对失陷主机的远控。这时，防守方分析人员通过流量或日志回溯掌握攻击手法及过程后，可利用 NGSOC 的日志关联分析能力，通过图形化配置界面快速构建检测模型，实现对新型威胁的检测告警。

第四，一键处置。这个场景在攻防对抗过程中非常常见，是威胁应急响应的一种必要手段。当 NGSOC 检测到威胁并产生告警后，经分析人员确认后，可通过联动处置功能模块，对天擎（终端安全系统）、防火墙或上网行为管理网关等产品直接下发一条指令，对告警中的恶意 IP、域名或 URL 进行封禁。

战后复盘：总结汇报

战后阶段，将把本次攻防演习的工作成果及不足进行汇报总结，为后续改进、完善安全运营体系提供依据。

数据与报表的支撑。演习结束后，安全运营或安全管理人员在编写此次演习的工作总结时，可通过 NGSOC 上记录的监测、分析、处置等工作成果数据，形成丰富的可视化报表，直接插入到工作总结中。

同时，安全分析人员可通过 NGSOC 的调查分析、日志搜索等功能模块，结合平台接入数据，可对攻防演习中的攻击事件进行调查回溯，分析现有监测防护体系的薄弱点，提供整改建议。

图：NGSOC 拥有丰富的可视化报表模版

经过多年打磨，奇安信 NGSOC 凭借强大的安全感知能力、优秀的使用体验、权威的威胁情报、一流的大数据分析技术和安全可视化能力，已经成为实战场景下的防守“司令部”，在部委、地市政府、央企、金融机构、高校等各行业超 600+ 政企机构落地实践。

4 守好网络攻击的“着陆点”：奇安信天擎

奇安信天擎终端安全管理系统可满足防守队从备战到实战不同阶段的差异化防守需求，助力防守队攻克终端安全防御难题。目前，天擎已助力国内 5 万余家政企单位部署终端安全工作，是防守队守好终端安全的利器。

在实战攻防演习过程中，终端历来是攻防双方的必争之地。终端安全防御难，一方面受到终端数量庞大、操作系统各异、用户安全意识薄弱等问题牵制；另一方面，终端又是所有网络攻击的“着陆点”，针对终端系统的攻击手段复杂、多样。在这一背景下，防守队该如何在攻防演习中守好终端安全？

作为奇安信面向政企单位推出的一体化终端安全产品解决方案，终端安全管理系统（以下简称“天擎”）集防病毒、终端安全管控、终端准入、EDR 等功能于一体，在实战攻防演习中全面发挥防御能力，从演习的三个不同阶段入手，助力防守队攻克终端安全防御难题。

下面具体来看，天擎在演习过程中为防守队献上的锦囊妙计。

阶段一：盘清资产、识别风险

在实战攻防演习正式启动前的第一个备战阶段，核心目标是梳理全网终端资产的状态，识别高风险资产，从而确定网内的风险点和暴露面。

这一阶段，防守队可利用天擎“终端发现”的扫描、监听等能力，并结合网络准入设备，首先对全网资产进行全面扫描，并重点识别未确认、不活动中高端。

未确认终端主要包括近期新入网尚未进行资产识别的终端、未进行实名认证及登记的终端、以及系统无法准确识别的终端等。由于此类设备在网运行期间缺乏有效的资产识别和信息获取，使其成为不折不扣的“黑户”，给安全策略落地、安全责任到人带来了较大阻力，是实战演习前需要解决的首要风险点。

不活动终端通常包括临时启用的业务服务器、长期开机但不常态使用的计算机终端等，此类终端犹如“幽灵”般存在，往往长期不受关注并疏于管理，给防守留下了较大的暴露面。演习前夕，需全面识别此类终端，并结合业务实际需求，及时采取关停或纳入统一管理等安全措施。

在消除了“黑户”和“幽灵”后，防守队已经基本做到了“盘清资产”。接下来，防守队需针对终端列表进行深入分析，并利用天擎的“综合评估”模块，识别并标记相关安全配置不符合基线要求的终端、保存大量敏感数据的终端、重要部门核心人员使用的终端、停服系统终端等高风险终端。

“综合评估”模块共包含三项能力，分别为：

1. 配置脆弱性评估

天擎通过检查终端身份鉴别、安全审计、访问控制、资源控制、入侵防护的配置状态，评估其配置脆弱程度，并判断其是否符合实战攻防演习背景下的终端安全管控标准。

2. 数据价值评估

防守队可自定义“高价值数据”的典型特征，并针对全网终端指定路径下的各类文件进行内容扫描，基于检测到的高价值数据情况，将在网终端划分为普通数据终端、敏感数据终端、核心数据终端等，并进行分类标记。

3. 沦陷迹象评估

沦陷迹象评估主要针对主机的系统帐号变化、终端 U 盘使用、IE 浏览器访问、文档打开、搜索、共享访问等记录进行分析评估，确定可能已被侵入并受到恶意控制的终端。

至此，在天擎的协助下，防守队就可以达成“盘清资产、识别风险”的目的，第一阶段备战结束。

阶段二：加固战壕、精准防控

第二个备战阶段，则以缩小网络暴露面，最大程度消除隐患为核心目标。

防守队可利用天擎的“一体化”特性，再次评估终端漏洞修补、全盘病毒查杀、开启实时防护、使能主动防御、部署运维管控措施等防护管理手段效果，并进行必要的策略优化和调整，以加强“战时”的总体防控强度。

除此之外，针对上一阶段所识别出的关键风险点，则需重点加强其防控措施，实现精准防控，建议防守队采取的主要措施包括：

1. 停服系统加固

通过启用天擎的“XP 系统加固”和“Win7 系统加固”模块，基于内存指令控制流检测技术、智能权限分析与设置技术，重点防护针对停服系统进程的远程代码执行漏洞攻击、针对浏览器漏洞的网页挂马行为攻击、针对常用文档编辑程序漏洞的钓鱼攻击等。

2. 软件安装统一控制

通过天擎内置的“软件管家”，建立统一的软件管理中心。在演习期间，全网终端仅可安装经过软件中心安全鉴定的程序，禁止运行其他未被鉴定、授权或非可信来源的安装文件，从而规避常用软件夹带恶意程序植入的风险。

3. 移动存储管控

随着利用 U 盘等移动存储设备传播恶意程序的新型攻击出现，天擎可对所有企业自用 U 盘进行登记管理，并对文件存储进行高轻度加密，非可信的移动存储设备则无法在终端设备上使用。

4. 违规外联管控

针对隔离内网用户，开启违规外联监控及告警措施，重点监控无互联网访问权限终端通过自建网络连接互联网，或使用不可信互联网连接访问互联网的情况。

至此，第二阶段备战结束。

阶段三：持续监测、及时响应

经过了以“拉伸防线纵深、缩小暴露面”为目标的前两阶段备战工作后，攻防演习将进入实战阶段。这一阶段，天擎终端检测与响应（EDR）优势凸显。具体而言，在演习期间，防守队可利用 EDR 实现以下几方面的工作：

1. 基于告警信息进行分析和调查

EDR 系统可基于持续的 IOC 和 IOA 检测，对恶意行为进行识别并发出告警，防守队则通过 EDR 提供的威胁调查工具，对线索中的可疑事件、IP、文件等进行信息检索及关联分析，从而快速洞察威胁全貌，是对传统防护手段的有力补充。

2. 对确定的威胁事件进行快速定位

在演习期间，防守队会持续获取各类通报信息。对于一些已确定的攻击事件，防守队往往已经掌握了攻击的部分特征，需要在最短的时间内查清威胁全貌并确定受影响范围，以采取响应措施。此时，EDR 可以作为调查工具，把终端上发生的所有行为以元数据的形式记录下来。在此基础上，防守队可快速检索出与威胁相关的 IP、主机、进程、命令参数等，这一过程类似于使用“搜索引擎”。

3. 加强战时的“机动巡逻”

基于“战时”的需要，部分用户还可利用 EDR 所支持的高级查询规则，自定义与业务相关的威胁行为特征，并在全网终端大数据中检索。此类应用是在一系列自动化告警机制之外的补充，主要起到了“机动巡逻”的作用。

4. 终端威胁集中处置

当威胁及其影响范围被确定后，防守队可通过 EDR 的统一控制台，针对全网或限定范围的终端进行进程中断、网络隔离等操作，从而在短时间内遏制威胁的破坏。值得强调的是，天擎 EDR 可与奇安信旗下的天眼、NGSOC 等产品实现联动处置，防守队则可借此特性，

实现网络侧、终端侧的协同响应。

以上就是天擎在攻防演习三个阶段所发挥的防御能力，满足防守队从备战到实战不同阶段的差异化防守需求。在网络实战攻防演习的常态化趋势下，越来越多的政企单位加入其中，攻防双方的演习程度不断白热化，想要守好终端安全，天擎这个制胜武器每一个防守队都值得拥有！

防守指挥中心利器：奇安信安全编排自动化（SOAR）

每年实战攻防演习都会聚集多支顶尖攻击团队。面对攻击方远超日常的攻击手段和强度，政企机构往往力不从心：大量人员值守，但靠人工进行安全处置，安全设备缺乏协同联动，严重影响处置效率。

奇安信推出的 SOAR 3.0，有望扭转攻防演习中防守方的被动局面。作为真正整合人员、流程和工具的安全运营平台，奇安信 SOAR 基于自动化、智能化的网络安全检测和响应能力，可将安全处置效率提升 10 倍以上，少量告警仅需 10 ~ 30 秒，显著提升安全响应的效率。

时长缩至分钟级 安全处置效率提升十倍

SOAR 是安全编排、自动化与响应的简称，正是针对防守方面临的诸多运营挑战而生：很多防守方依赖安全设备规则，需大量安全运维人员进行值守。安全设备扩容流程复杂、效率低。安全设备协同依靠人工，操作耗时费力，严重影响效率。

作为面向实战化安全运营的安全编排、自动化及事件响应产品，奇安信 SOAR 将安全运营相关的团队、工具和流程通过编排和自动化技术整合在一起的，有序处理多源数据，持续进行安全告警分诊与调查、威胁猎捕、案件处置、事件响应，最终实现高效、有效的安全运营。

奇安信 SOAR 可以大大提高处置效率。根据实际检测，在一键封禁 IP 场景下，对于少量告警，人工处置要 20 分钟甚至更长，利用 SOAR 仅需 10~30 秒；如果在告警量数以万计的条件下，依靠人工更加难以处置，而 SOAR 可以全量处置，时长锁减至分钟级别。

五大关键能力提升协同作战效率

区别于其它同类产品，奇安信 SOAR 是基于自身丰富的实战化安全运营经验，依托具有丰富安全管理与运维技术积累的技术团队，经过了长期调研和潜心研发，使其实战性全面领先于同行。

奇安信 SOAR 具备 5 大技术特点及关键能力：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。

安全能力编排化能够将实现团队、工具和流程的整合与协同联动，减少人工干预。

安全流程自动化可以实现告警分诊、安全响应、剧本执行、应用执行、案件处置，以及服务调用的自动化，

节约时间和人力成本，并确保能够持续达成预期的效果。

告警响应智能化能对海量告警信息进行智能分诊，提升了告警响应的精准度和有效性，方便工程师进行下一步研判。

案件管理全程化可帮助用户对一组相关的告警进行流程化、持续化的调查分析与响应处置，并不断积累该案件相关的痕迹物证 (IOC) 和攻击者的攻击战术等指标信息。奇安信 SOAR 具有目前国内仅有的、真正符合国际共识的、独立且完整的案件管理功能。

系统架构开放化确保友好便捷地集成各类安全工具和产品，无缝融入现有安全体系。

此外，协同作战室功能可以实现安全工程师的实时沟通，内置大量编排好的自动化剧本和命令，实现了人机间的协同处置，改变了“通讯基本靠吼，操作基本靠手”的局面，提升了协同作战的效率。

借助奇安信 SOAR，政企机构可以有效应对攻防演习期间的人员不足、响应不及时、安全设备缺乏协同且联动性差等严重影响安全处置效率的问题。奇安信 SOAR 可以帮助客户在事前制定预案以逸待劳、事中自动响应快速处置、事后复盘总结积累经验，全方位提升实战化能力。

具备整合资源、自动运营、告警分诊、快速响应、动态对抗、提升人效等六项价值，奇安信 SOAR 就像防守队作战指挥中心的操控台，可以让所有安全设备实现协同作战，并实现了团队、工具和流程的真正整合，提升安全运营和响应处置的效率。

防好供应链攻击源头：奇安信开源卫士

开源软件的应用非常广泛，在金融、运营商、电力、航空、汽车等行业客户的信息系统底层架构中，均有开源软件的影子。据 Gartner 调查报告显示，99% 的组织在其 IT 系统中使用了开源软件。

作为支撑信息系统的源头，在实战攻防演习中，开源软件极易成为红队利用软件供应链攻击的“源头” 和突破口。

如何快速盘清开源软件资产？如何发现开源软件中的安全风险？如何及时掌握相关的漏洞情报？

为此，奇安信发布了国内首个成熟的商用开源软件安全治理产品——奇安信开源卫士系统。

奇安信开源卫士是一款集开源软件识别与安全管控于一体的软件成分分析系统，该系统通过智能化数据收集引擎在全球范围内获取开源软件信息及其相关漏洞信息，利用自主研发的开源软件分析引擎为企业提供开源软件资产识别、开源软件安全风险分析、开源软件漏洞告警及开源软件安全管理等功能，帮助用户掌握开源软件资产信息，及时获取开源软件漏洞情报， 降低由开源软件带来的安全风险，保障企业交付更安全的软件。

奇安信开源卫士具备四大能力：

开源软件资产发现功能

奇安信开源卫士通过软件成分分析，可以识别企业软件中使用了哪些开源软件以及开源软件间的关联关系，自动生成开源软件资产信息清单。目前开源卫士能够识别 C、C++、Java、Python、JavaScript、.NET、PHP、Swift/OC、Go/Golang、.Net、Erlang、Scala、Ruby、Perl、R 等多种语言开发的 4000 多万个开源软件版本的信息。

开源软件安全风险分析功能

奇安信开源卫士通过开源软件信息，能够匹配对应的漏洞信息，自动生成开源软件漏洞信息列表，目前开源软件漏洞情报信息兼容了美国国家通用漏洞数据库（NVD ）、国家信息安全漏洞库（CNNVD）、国家信息安全漏洞共享平台（CNVD）及多个开源社区漏洞信息等数据源。

开源软件漏洞情报推送功能

奇安信开源卫士通过云端分析中心在全球范围内获取开源软件漏洞信息，然后经过一系列自动化数据分析处理后，通过邮件、站内信等方式将开源软件漏洞情报

信息及时推送给企业客户。

开源软件关联分析功能

开源软件中的安全漏洞，在影响该开源软件安全的同时，也会给使用该开源软件的其他开源软件带来安全风险。奇安信开源卫士可以对开源软件间的关联关系和相互影响进行分析，帮助企业全面跟踪溯源开源软件漏洞可能的影响范围。

奇安信开源卫士应用场景：

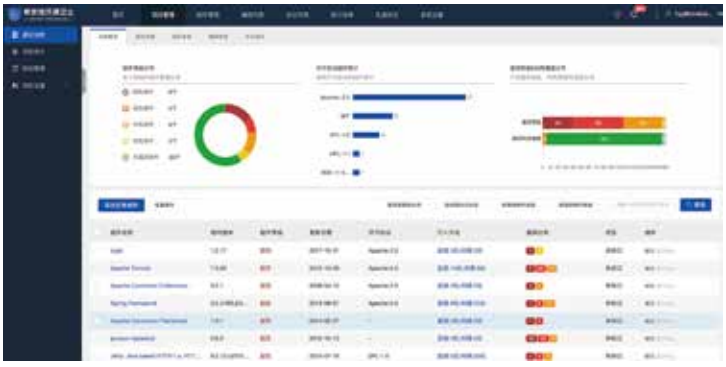
软件设计阶段：可通过奇安信开源卫士开源软件查验功能检索预使用的开源软件的版本是否存在已知漏洞和协议风险，在技术选型时，及早规避引入有漏洞的开源软件，从源头把控开源软件的风险。

软件开发阶段：软件开发部门使用奇安信开源卫士与软件版本管理系统、持续集成系统等开发工具链进行集成，针对研发项目进行周期性自动化开源软件安全扫描，及时发现引入的开源软件是否存在已知漏洞和协议风险，便于开发人员对有风险的开源软件进行及时整改。

软件测试阶段：软件研发（包括自主开发和外包开发）完成后，分析软件中包含了哪些开源软件资产，形成开源软件资产清单，分析开源软件中是否存在已知安全漏洞和协议风险，评估漏洞危害等级及整改建议。

软件运行阶段：奇安信开源卫士针对上线前形成的开源软件资产清单，通过云端安全分析中心持续监控开源软件漏洞情报信息，当有新的漏洞被发现，系统会通过邮件、站内信等方式通知客户，帮助客户及时获取到影响自身安全问题的漏洞情报信息，及时采取应对措施。

目前，奇安信开源卫士团队运营着国内规模最大的“开源项目检测计划”，收集了 4000 多万个开源项目版本的信息，积累了大量的开源软件安全基础数据。奇安信开源卫士的漏洞信息兼容了国家信息安全漏洞库(CNNVD)、国家信息安全漏洞共享平台（CNVD），能够满足行业用户相应的监管要求。同时，当用户使用的开源软件不能通过升级软件版本进行漏洞修复时，奇安信开源卫士依托奇安信代码安全实验室专业的漏洞研究能力，可以为用户提供开源软件漏洞危害评级、漏洞补丁分析、漏洞补丁方案等高端漏洞修复咨询服务。



图：开源软件分析结果

7 主动防御利器：奇安信网神攻击诱捕平台

在 2020 年国家级实战攻防演习中，奇安信网神攻击诱捕平台曾成功溯源到攻击者的信息，协助客户提交溯源报告，得分取得佳绩。

在往年国家实战攻防演习中，防守方一直处于被动防守困境，任何防护措施上的疏漏都会导致防守失败。2020 年防守方引入攻击诱捕技术后，成功扭转了攻防不对等的状况。攻击诱捕技术有效提高了攻击者的攻击难度、延缓攻击进程，增加了防守方主动溯源和反制能力，为防守方赢得主动权。

奇安信集团连续 4 年深度参与国家实战攻防演习，基于丰富的实战对抗经验研发了奇安信网神攻击诱捕平台。该平台基于欺骗诱捕技术和精心构造的漏洞陷阱、混淆攻击目标，对所发现的攻击威胁流量进行牵引、隔离，以及攻击特征的取证、溯源及反制，有效保护内部真实的资产，实现主动安全防御。

攻击诱捕平台是奇安信天眼从被动威胁检测到主动威胁防御的有效补充，极大增强了实战攻防演习过程中的体系化对抗能力。在去年的实战攻防演习中，奇安信网神攻击诱捕平台曾成功溯源到攻击者的信息，协助客户提交溯源报告，得分取得佳绩。

五大产品价值，构建实战化防守金钟罩

1. 早期突破后检测

没有任何安全解决方案可以阻止网络上所有攻击的发生，但是攻击诱捕平台利用欺骗技术使攻击者相信已经在组织的内部网络上立足，使其产生一种错误的安全感。平台可以从容监视和记录黑客的行为，这些攻击者行为和技术信息可用于进一步保护网络免受攻击。

2. 减少误报和风险

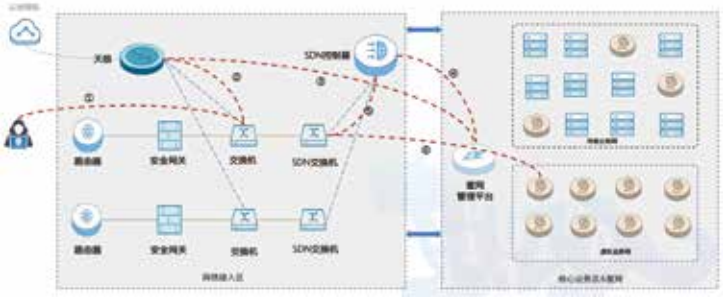
大量的误报会阻碍安全工作，过多的噪音可能导致 IT 团队忽略了潜在的真正威胁。攻击诱捕技术理论上不会产生任何误报，可以做到触碰即告警，告警即发现，减轻用户安全运维的负担。

3. 从传统被动防御向主动防御演进

攻击诱捕平台基于实战攻防演习、重大安全保障活动的最佳实践，采用欺骗伪装技术，联合奇安信云端威胁情报、天眼未知威胁检测系统，对流量实施动态的诱骗捕获，并根据行为进行溯源、分析，推动了企业安全体系从被动防御向主动防御的进化。

4. 降低企业攻击诱捕系统的建设成本

攻击诱捕平台创新的提出攻击流量检测 +SDN 的方式进行流量牵引，根据攻击行为进行智能的分发和应答，主动仿真等技术，降低了蜜罐系统对业务仿真的依赖，在较低的覆盖率的情况下也能保证诱捕的效率，极大程度降低了企业攻击诱捕系统的建设成本。



5. 协助企业在实战攻防演习防守中获得佳绩

多协议、多场景化的攻击反制以及攻击行为的分析，可以协助防守方在实战攻防演习防守过程中追踪到黑客的自然人身份，从而获得更好的战绩。

八大使用场景，更主动、更智能、更具反制能力

1. 公网、内网探测场景

用于探测攻击者的端口扫描行为。

2.WEB 漏洞型蜜罐场景

用于发现攻击者利用特定 Web 系统漏洞的攻击行为。

重保初期，可以对探测行为的告警列表进行导出，对攻击 IP 采取封禁措施。

3. 堡垒机蜜罐场景

模拟奇安信堡垒机系统界面，诱导在内网横向移动的攻击者访问，输入个人相关信息用于反制溯源。

4. 反钓鱼蜜罐场景

用于模拟企业的 PC 办公终端。在办公终端蜜罐运行钓鱼木马，造成肉鸡上线假象，攻击者拉取诱饵文件后，可在攻击者主机运行进行反制。

5. 数据库反制蜜罐场景

数据库反制蜜罐内置 mysql 服务器，当攻击者使用低版本存在漏洞的 mysql 客户端进行连接时，mysql 反制蜜罐可以获取攻击者主机信息。

6. 中间件蜜罐场景

模拟常用的一些 WEB 中间件，用于测试或进行反制。

7. 操作系统模拟蜜罐场景

用于操作系统模拟，可在上面进行自定义修改，定制安装程序。

8. 开源蜜罐场景

开源蜜罐，主要用于内网监测、SSH 登录模拟。

守好最易突破环节：网神邮件威胁检测系统

实战攻防演习中，钓鱼邮件成为攻击队频繁使用、非常有效的攻击手法。例如，在一次实战攻防演习中，某证券机构遭到攻击队邮件钓鱼，内部账号控制权限被获取。

普通的邮件检测系统在针对具有全自动化、大规模执行、单次成功率低的标准技术的电子威胁具有较好检

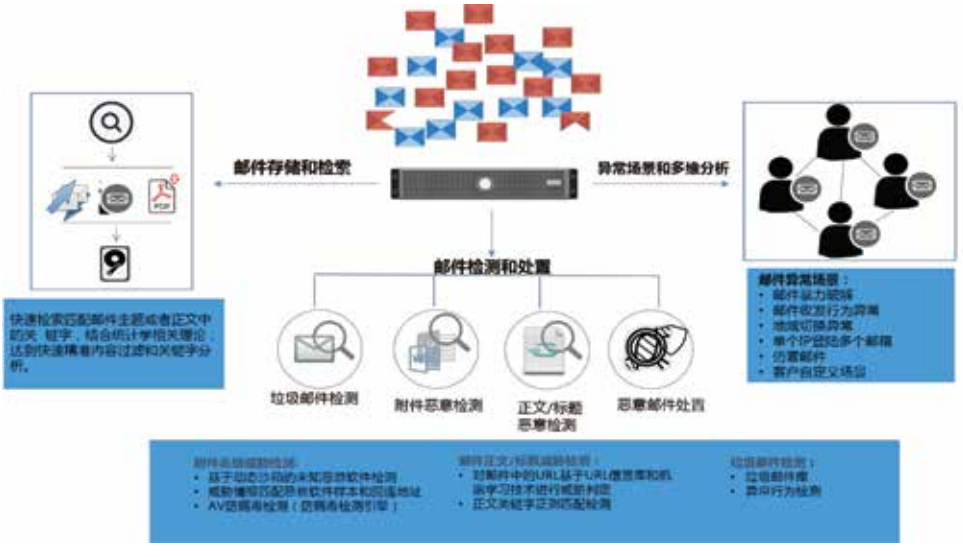


图 1 邮件威胁检测系统功能介绍

测效果，但是针对具有特殊目标、小规模执行、长期持续性网络攻击的高级威胁显得力不从心。因此奇安信集团推出专门针对高级邮件威胁检测的网神邮件威胁检测系统，可以在实战攻防演习时帮助客户更好的防范钓鱼邮件攻击。

强大的侦测手段，提供全面的邮件安全防护

奇安信网神邮件威胁检测系统是奇安信集团面向政府、企业、金融、军队等大型企事业单位推出的针对邮件场景的高级威胁检测及处置的解决方案。

邮件威胁检测系统采用多种病毒检测引擎，结合威胁情报以及 URL 信誉库对邮件中的 URL 和附件进行恶意判定，并使用动态沙箱技术、邮件行为检测模型、机器学习模型发现高级威胁及定向攻击邮件。通过对海量数据建模、多维场景化对海量的邮件进行关联分析，对未知的高级威胁进行及时侦测。强大的侦测技术和全面的处置手段，对电子邮件系统进行全面的安全防御。

六大核心功能为实战攻防保驾护航

网神邮件威胁检测系统依据对邮件数据的采集、结合行为特征检测、分析以及云端数据关联分析挖掘和可视化展示，实现对威胁邮件的快速检测和持续分析。

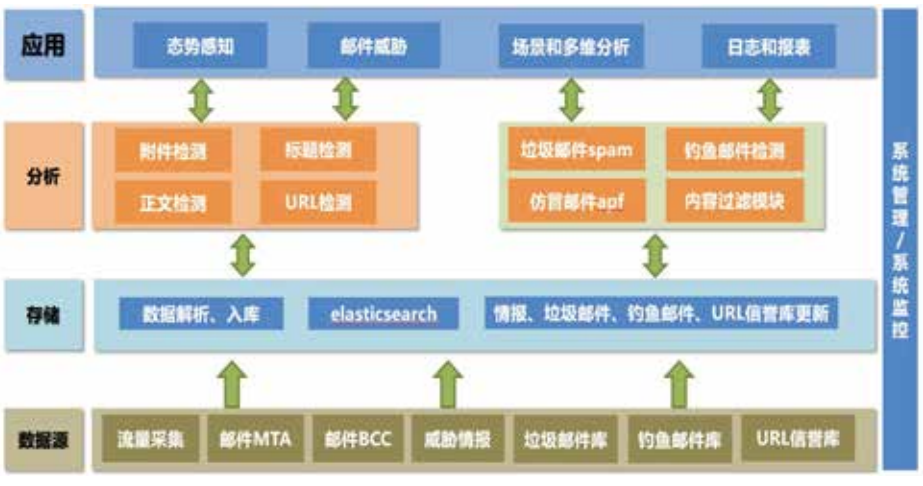


图 2 邮件威胁检测系统的核心模块

图 3 邮件威胁检测能力

（1）强大的威胁情报

邮件威胁检测系统结合了奇安信强大的威胁情报数据，使产品对邮件威胁的检测能力如虎添翼。

（2）高效的沙箱分析模块

邮件威胁检测系统沙箱模块可针对文件进行深度检测，采用静态检测、漏洞利用检测、行为检测多层次手法，构建基于沙箱技术的文件深度检测分析能力。静态检测模块通过多种检测引擎互为补充增强静态检测能力。动态检测模块以硬件模拟器作为动态沙箱环境，分析过程中所有的数据获取和数据分析工作都在虚拟硬件层实现，全面分析恶意代码恶意行为，细粒度检测漏洞利用和恶意行为。

（3）智能的钓鱼邮件识别

奇安信网神邮件威胁检测系统对包含 URL 的钓鱼邮件检测，除了实时的 URL 信誉库和威胁情报，还有在大量数据训练的基础上，利用随机森林、GBDT 等机器学习集成算法，自研的一套基于机器学习的检测系统。

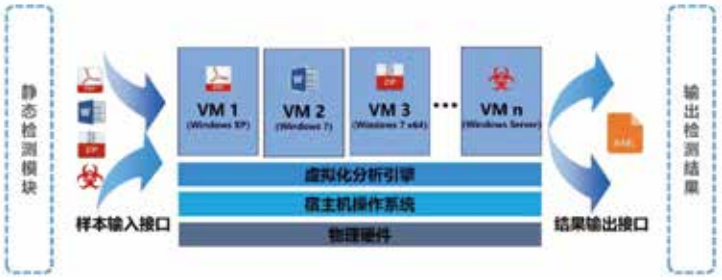


图 4 动态沙箱优势

（4）丰富的邮件异常场景

异常场景包括：发件异常、收件异常、暴力破解、单个 IP 登陆多个邮箱、异地登陆等，并可根据需求自定义异常场景的检测条件。且支持全面分析仿冒邮件场景。

图 5 机器学习技术特点

（5）多维的邮件分析功能

产品提供基于联系人之间的收发关系的多维分析模块以及基于恶意文件 /URL 的传输路径的多维分析模块。

图 6 邮件异常场景检测

用户根据通过关键信息进行检索，实现数据之间的多维关系网。所有复杂的关系通过多维的分析的展现，数据一目了然。

（6）海量的数据存储和检索能力

奇安信网神邮件威胁检测能够快速检索匹配邮件主题或者正文中的关键字，结合统计学相关理论，达到快速精准内容过滤和关键字分析。并配套了大量的检索和分析软件以对数据做到高效分析。

钓鱼攻击已经成为实战攻防演练中的一个重要且常见的攻击方式。人永远是最大的弱点，未知攻，焉知防。对于参与攻防演习的甲方，可以利用邮件威胁检测系统来防范钓鱼攻击，同时可以组织内部钓鱼项目，提高员工安全意识。

9 实战演习的“安全底板”：奇安信实战攻防演习平台

在奇安信天眼、天擎、云锁、安服等重磅武器的加持下，网络安全实战攻防演习活动已经可以交出一份不错的成绩单。但在以政务、能源、金融、广电、交通、民航等关键信息基础设施为攻击目标的演习过程中，如何保证全流程安全管控能力，如何通过对攻防演习活动的及时总结和复盘，为演习单位的网络安全体系建设提供改进方向？如何为攻防双方提供更好的对抗体验？奇安信实战攻防演习平台为监管部门和企业用户组织开展网络安全实战攻防演习活动提供了一整套解决方案。

基于多年实践经验和科研成果，奇安信自主研发而成的实战攻防演习平台，具有安全性、可靠性、可视性、多样性和可追溯的特点，可以提供与实战效果一致的仿真预演，更具科技感的演习观赏视角、强大的实战攻击团队服务，以及一站式整体解决方案。

基于“安全可靠的全程保障机制”理念，实战攻防演习平台采用多种手段确保演习过程安全可控，包含账号身份认证机制、攻击流量全留存、攻击行为实时分析、终端违规行为实时监控并告警、攻击目标圈定可控等，

配合堡垒机、虚拟攻击终端、天擎、天眼等产品，可针对攻击行为进行审计，对违规行为进行告警和阻断，保障演习过程安全可控。

在可视化方面，实战攻防演习平台可提供战况总览维度、攻击方维度、防守方维度、指挥调度维度、违规行为实时监控维度等共 8 个视角的大屏组合，并可根据客户需求提供定制化服务。大屏体系在数据统计实用详尽的同时，采用先进的数据可视化设计理念，形成了具备高观赏度、高可读的全角度立体可视化体系，方便组织者及时了解攻防动态。

作为一套完整的攻防演习整体解决方案，实战攻防演习平台还能提供包括演习平台、演习平台运营服务、演习过程及成绩汇报服务、演习结束后报告服务、攻击队和专家裁判组织服务等一整套攻防演习解决方案，支持管理员、进攻方、防守方、裁判员、专家等多种角色完成演习工作，为演习组织者和各方参与者有更好的参赛和使用体验。

在演习后，实战攻防演习平台可提供攻防总览视角、攻击方 / 防守方成果统计视角、行业视角、实际攻击流量、有效攻击成果等多种攻防统计维度，提供维度丰富、排版专业的汇报素材，并可用于复盘演习过程，为提升演习单位抵御网络威胁能力、优化网络安全体系提供详实可靠资料。而攻击终端安全监控和终端日志、流量数据留存，也可为事中事后审计工作保留完整资料。

强大的能力来源于多年来丰富的“实战”经验，连续 4 年深度参与业界最权威的网络安全攻防演习活动，奇安信实战攻防演习平台将丰富的经验固化为产品并快速迭代，保持平台全方位领先，已形成了不可复制的优势产品壁垒。

针对数据涉密、有信息保密需求的特定项目，实战攻防演习平台还可提供本地化部署方案。相较于云端 SaaS 方案下演习后及时删除数据、回收攻击资源，本地化方案可满足用户本地化部署，运维自动化需求，保留多次演习数据，以便于分析攻击手段演进、防守手段变化，关注整改效果等。2020 年，实战攻防演习平台已为多家客户提供了本地化方案服务，帮助其顺利完成实战攻防演习。

一场安全、可靠、有效的实战攻防演习检验的并不是单纯的业务系统是否安全，更重要的是以人为核心的安全意识和抗风险的能力。依托于奇安信实战攻防演习平台和其他“利器”配合，将人员与技术有效融合，为演习单位提供 " 全流程保障、全环境支撑、全风险可控 " 的一站式服务，堪称实战攻防演习的不二之选。安

客服小姐姐能有什么坏心思呢？竟然对她进行社工钓鱼

作者 公关部 魏开元

2020 年年末，某大型特种设备制造企业生产车间内，集团领导正在视察，有那么几分钟，他望着安全生产的横幅有些出神。

“你负责采购的网络安全设备怎么样了？”老板扭过头去看向了网络安全负责人老汪。

“上个月最后一批工控防火墙已经到位了，他们交付现场做了部署调试，暂时没有发现问题。”

“嗯。”老板略微思考了几秒钟，“这样吧，有没有问题你们说了不算，我说了也不算，我们来一次实战攻防演习就知道了。这个事情老汪你来安排，网络安全也是安全生产的一部分，绝不能只停留在标语上。”

精心构造“鱼饵”，准备钓鱼

“Hill 哥（奇安信 Z-TEAM 负责人），来活了。刚销售给我打电话说，某特种装备制造商找到了我司，说是想做一次渗透测试。”

“来就来了呗，你第一回当攻击队啊，这么激动。”

“嘿嘿，听说他们刚买了全套的安全设备，还请了安全服务人员提供驻场运营，这不想拉出来遛遛，看看现在到底是个啥水平么。”

“有点意思。这样吧，你们攻击队 6 组准备一下，跟我一起去客户现场。关于这次攻防演习，我就提一点要求，不能给我们 Z-TEAM 丢人。”

没过多久，Hill 就拿着客户的授权回来了。和往常一样，Z-TEAM 所开展的攻击渗透，主要目标是取得生产网内抛光、电镀、传送等工控系统的控制权限，除此之外不得影响工厂设备的正常运转，不得爬取敏感数据。

“开个会吧，大家简单分一下工。”Hill 说，“这次渗透从明天上午十点正式开始，总共两周时间。我们还是按照老规矩分成两组，一组负责从他们官网渗透，另一组负责钓鱼邮件。行了，今天早点下班回去休息吧。”

另外一边，老汪在办公室里可没有这么轻松。这几天他累坏了，不停地在给系统打补丁。同为白帽子出身的他，和 Hill 在全球最大的男性交友网站（Github）上，可是老网友了，经常会在一起切磋攻防实战技巧。这个奇安信 Z-TEAM 的老大哥，还不知道会给他带来什么“麻烦”。

第二天上午，队员们全部早早就位，为这次行动做着最后的准备。负责 Web 渗透的雷子不停地翻看着这家

特种装备制造商的官网，似乎已然成竹在胸；负责邮件钓鱼的 Hill，也在为钓鱼邮件做最后的伪装，一切早已准备就绪。

“Hill，这次你准备钓谁啊？”雷子突然问了一句。

“HR 吧。我看前两天他们公众号刚发了一条消息，要招两个网络安全运营工程师，我这简历都弄好了，没准他们还真会给我打电话约我面试呢。”

外围防守十分严密，试探性攻击一无所获

“叮叮叮，叮叮叮……”，一阵清脆的闹铃声让 Hill 他们为之一振，十点钟到了。

攻防演习开始后，Hill 并没有急着把钓鱼邮件发出去，这样就显得太假了。他知道，老汪肯定跟各部门提前叮嘱过，不要随便打开不明邮件，所以 Hill 决定浑水摸鱼。上次 Hill 去拜访客户的时候就了解过，人力部下午两点钟上班，Hill 打算趁着 HR 中午睡醒后迷迷糊糊的那几分钟时间，抛出“鱼饵”。

因此这会儿 Hill 正不紧不慢地正琢磨着，怎么能让自己编译的木马文件，躲避防病毒软件的检测呢。

一旁的雷子倒是忙的不亦乐乎。借助奇安信自研的代码审计工具（代码卫士），雷子很快就从源代码中，发现了两个文件上传漏洞，触发后可以上传 Webshell（一种网页后门，用于控制网站服务器）文件。

“这么常见的漏洞都没补？”雷子心里有些犯嘀咕。不管了，先搞一下再说。

“汪总，我们官网服务器上部署的 WAF 产生异常告警，应该是 Z-TEAM 那边上传了 Webshell。”

老汪一下子从椅子上站了起来，如临大敌一般：“尽快定位清除后门文件，另外注意随时更新 WAF 规则，这应该只是他们的一次试探性的渗透动作吗。”

看到自己上传的后门文件被删除，雷子并没有感到过多的惊讶，事实上，他也没有指望一击必中，“Hill，他们果然是有准备的啊，部署了 WAF，我这边再更新一下后门文件配置，看看能不能绕过防护规则，不过需要一点时间，下午就看你钓鱼了啊。”

Hill 不动声色，只是向雷子比了一个 OK 的手势。

转眼时间来到了下午两点。Hill 看了看时间，顺手点击了邮件发送的按钮。

这回轮到 Hill 有些小小的失望了。尽管他精心构造的木马附件骗过了邮件安全网关的检测，但负责招聘的同事并没有掉以轻心，而是将邮件转发给了网络安全部。果然，云沙箱检测结果显示，Hill 投递的简历包含以远程控制为目的的木马文件。

“人力部门的同事安全意识不错，在大家的共同努力下，我们的网络安全防线并没有失守。”在晚上举行的第一天攻防演练总结会议上，老汪没有吝啬自己的赞美之词，“各个部门要强化安全意识，今后各部门收到的邮件，统一先转到网络安全部处理，检测正常后再转发到各个业务部门。”

“防守挺严密的，还真是那么回事儿。”另外一边，Z-TEAM 也在开着总结会，雷子率先发了言，“Hill，看来我们不费点功夫，这回还真不好弄，我后来又修改了一次 Webshell，但他们 WAF 规则更新也非常快，又把我拦截了。”

“常规操作。”Hill 笑了笑，想缓解缓解略显紧张的气氛，“我这边钓鱼不也还没成功么，他们那个老汪跟我也算是老网友了，是有两把刷子的，哪能这么简单就搞定了。这样，从明天开始，我们的策略要变一下，必须重新寻找突破口，这方面我亲自来负责。雷子你那边暂时先不变，继续尝试 Web 渗透，看看有没有可以利用的 WAF 漏洞。”

二次伪装，成功骗过客服小姐姐

接下来的几天，Z-TEAM 似乎略显沉闷。负责 Web 渗透的雷子一直未能突破防守方的防线，“Hill，

这次我觉得 Web 渗透的路子这次可能走不通，防守方 WAF 运营非常专业，不管是在规则更新方面，还是产品本身的漏洞，响应非常及时，我尝试利用了一些过去的老旧漏洞，发现都打补丁了，要重新挖掘 0day 的话，我估计剩下的一个星期时间也打不住。”

Hill 挠了挠下巴，他也明白了这个情况，正在思索着怎么才能找到防守方的弱点，一边反复浏览着防守方的官方网站。

突然，他眼睛一亮，目光停留在了在线微信客服的传送门上。“在线客服？对啊，还是得通过社会工程学的方法。既然他们 HR 不收钓鱼邮件，那就钓他们的客服。”Hill 心里想。

“雷子，你那边 Web 渗透别停，什么 Webshell、SQL 注入这些手法，给他们全来一套。噢，对了，记得重新写 Webshell 文件，他们 WAF 要是拦截了，就不停的修改，让他们安全团队不停地配置规则去。”

“那 Hill 你这边？”雷子不禁问到。

“我这儿还是老办法，社工钓鱼，不过这次我决定钓他们的售后客服。所以，你的主要任务就是吸引他们安全团队注意力。”

“得嘞。”

说着，Hill 就把木马文件重新做了伪装，默默点开了他们的微信客服页面。

“你好，我们是某某公司，我在咱们家买的设备出了点问题，机械臂上面有一道裂痕，能走售后吗？”Hill 嘿嘿一笑，率先向客服发起了攻势。

大约 5 分钟后，客服小姐姐有了回复：“您好，如果不是人为故意的，是可以走售后的。您能提供几张照片吗？我发给售后师傅看看。”

“好的，稍等一下，我拍几张照片发给你哈。”说着，Hill 就把早已准备好的远程控制木马，打了一个压缩包，发给了对面客服。

“抱歉啊，您这边能单发图片吗？我这儿打开压缩文件不方便。”

“什么意思？”Hill 有点意外，没想到对面客服安全意识也这么强，只好假装不明所以。

“我的意思就是您这边别用压缩包，就直接把照片一张一张发过来就行，这样看起来也方便。”

“图片有点大，还有一段视频，压缩包方便一点，再说我都打包好了，你就解压一下不就行儿了么。”Hill 佯装不耐烦。

“不好意思啊，我们这边有规定……”客服耐心解释道。

就这么着，和客服僵持了大约半个小时，突然，Hill 似乎失去了耐心，语气一下子加重了许多：“不就是解压缩么，有必要搞这么复杂啊。你们公司就这么对待客户需求的么，你再这么不耐烦我给你们李总打电话投诉退款了。”

对话框一下子静默了三分钟时间。

“那好吧。”客服小姐姐终于妥协了，对话框的另外一边，Hill 会心一笑，雷子他们也不约而同地比了一个“耶”的手势。Z-TEAM 的队员们知道，木马文件精心做了

伪装，逃过对方杀毒软件的检测应该不成问题。

果不其然，过了不大一会儿，控制台显示，木马程序已经成功运行。

持续扩大战果，成功获取工控设备控制权

“咱们总算是成功迈出了第一步，大家这几天都辛苦了，晚上我请大家吃点好的，就当提前庆祝一下。雷子，你那边得找个嘴巴利索的，就渣渣吧，专门对应付他们客服，别让他们再看出破绽了，其他人就注意盯着控制台，准备开始下一步的渗透，争取提前拿下。”Hill 在会上布置了下一阶段的重点工作。

尽管成功入侵客服小姐姐的办公电脑只是成功的第一步，但 Hill 明白，在目前绝大多数机构仍然使用的以边界防御为核心的传统安全架构面前，内网防御肯定相对较弱，因此后面只会越来越容易。

第二天天刚蒙蒙亮，Hill 就迫不及待的来到了办公室，查看木马收集到的信息。这一看，收获颇丰。木马程序探测到了某个文件目录下，以明文形式存储的办公系统账号和登录密码。

在成功登录对方办公系统后，Hill 第一时间翻看了该公司的组织架构。Hill 想来，由于客服工作的特殊性，需要和公司内部多个部门保持沟通，应该有权限可以看到相对完整的公司组织架构。而想要成功获取该公司工控系统的控制权，必须要找出工控系统运维人员使用的工控主机，植入远程控制木马程序。

果然在组织结构目录下，Hill 他们定位到了工控系统运维人员及相应的工控主机序号，随即针对该主机进行信息搜集和弱口令暴力破解攻击（类似于穷举法，不停地变换登录口令直到成功登录）。

幸运的是，有两台工控主机（主机 A 和 B）使用了类似的的弱口令（姓名首字母缩写 + 出生年月日），Z-TEAM 不费吹灰之力就控制了这两台工控主机。

Hill 他们大喜。

经过两天时间的监控和弱点分析，Z-TEAM 的队员们发现主机 A 使用了双网卡，但是两个网卡之间没有采取任何隔离措施，不巧的是主机 A 并没有连接关键工控设备；主机 B 也是一台双网卡主机，其上部署了隔离卡软件进行双网卡切换。

“雷子，发动人手找一下主机 B 双网卡之间隔离软件的漏洞。”Hill 说到。

最终，Z-TEAM 发现了 B 主机上隔离卡软件的一个重大设计缺陷，并利用该缺陷成功绕过双网卡的隔离机制，成功拿到了工控设备的操作权限，可以随意停止、启动、复位相应的工控设备，某些操作可对设备的生产过程造成直接且严重的伤害。

Hill“顺手牵羊”，推销安全方案

攻防演习结束后，Hill 和老汪线下约了顿饭。

“老汪，还是棋差一招吧，没想到我从客服这里渗透进去。”

“哈哈，我能说我想到了吗，我还专门交代了，尤其是人力、行政、财务、销售、客服这些部门，不要接收来路不明的文件。没想到……Hill，这次你们从客服这里进来以后，后面开展的太快了。你得给我出点招，从你们攻击队的视角来看，我们这个网络安全体系该怎么建设，上面下了 KPI 的。”

“没问题啊，我司能给你们设计一套完整的内生安全架构……”

关于 Z-TEAM

奇安信 Z-team 团队是一支在实战攻防演习中扮演重要角色、擅长进攻型的队伍，团队成员大多来自攻防渗透研究出身的高级技术专家和渗透工程师，多次参与省部级网络安全实战攻防演习，取得了出色的成绩。团队在实网对抗的不断锤炼中，研发相关技术工具，在 Web 攻防、社工渗透、内网渗透、模拟 APT 攻击等方面，技术实力扎实，技战法灵活，攻防实战能力受到业内广泛认可。（根据 Z-TEAM 实战攻防演习真实案例编写）安

如何组织一场安全、可靠、高效的网络实战攻防演习

作者 奇安信安全服务团队

为什么需要实战化能力?

当前网络空间面临的安全问题与过去不同，从原来只攻击传统的网络设施和应用系统，到开始面向“云大物移工”等新技术领域的应用系统，攻击的目标系统逐步转向核心业务数据和承载核心数据的业务应用；从普通的个人网络犯罪，到有组织的攻击甚至有境外背景的国家级对抗，攻击工具的武器化、攻击手段的战术化，均对防守者提出了更高要求。

在 2017 年 6 月颁布的《网络安全法》中，明确提出“应定期组织关键信息基础设施的运营者进行网络安全应急演练，提高关键信息基础设施应对网络安全事件的水平和协同配合能力”。正所谓讲一百遍不如打一遍，为了能有效检测行业或本单位的网络安全事件应对状态，应急演练必须向常态化与实战化迈进。

网络安全的建设不是单纯的业务系统是否安全，也不是安全设备是否全面，面对错综复杂、不断进化的网络空间攻防战，如何才能真实、有效的检验实战化监测、响应、处置能力呢? 一场安全、可靠、有效的实战攻防演习检验的并不是单纯的业务系统是否安全，更重要的是以人为核心的安全意识和抗风险的能力。奇安信结合数百场组织实战攻防演习的经验，总结分析如何协助各单位组织一场实战攻防演习。

组织实战攻防演习的四大核心要点

实战攻防演习通常以实际运行的信息系统作为演习目标，通过有监督的攻防对抗，最大限度地模拟真实的网络攻击，以检验信息系统的安全性和运维保障的有效性。演习在保障业务系统安全性的前提下，明确目标系统，不限制攻击路径，以提权、控制业务、获取数据为演习目的。

实战攻防演习包含攻击方、防守方、组织方三方，并配备实战攻防演习平台。

组织方负责演习整体工作的组织协调，主要包括以下几个部分：演习组织、演习过程监控、演习技术指导、应急保障、演习总结、防守技术措施与策略优化建议等。实战攻防演习一般可分为准备、演习、收尾三个阶段。

核心点一、明确的组织架构与职责分工

在正式演习开始之前，应以监管（主办）单位为核心，成立演习指挥部，下设演习组织机构，形成相应的工作组，

如领导组、协调组、专家组、裁判组、应急组、技术支撑组等，并明确各组职责分工，做到工作到组、责任到人、分工有序、密切配合。

核心点二、攻防演习环境准备

为保证演习顺利开展，各工作组应以指挥部为中心，集中办公，为各工作组准备单独的场地，各场地应具备电力、网络、办公桌椅等基础设备及后勤保障资源。

演习指挥大厅应有大屏展示设备，用来动态展示演习过程和结果，并进行演习风险管控。攻击人员使用专用笔记本电脑，系统环境统一初始化，安装录屏、终端管控软件。

奇安信提供可视化演习平台，对攻击行为全程监控全程审计，对演习态势与成果进行大屏展示，对演习过程和成果进行长期持续管理，实现演习的全程监控、全程审计、全程可视、全程管理。所有参演人员如有攻击操作、防守成果提交、裁判评分等动作都须在实战攻防演习平台上进行，便于事中事后的审计。

核心点三、演习过程风险管控

可控是实战攻防演习任务应该遵循的的基本原则，演习过程应做到人员可控、过程可控、环境可控及成果可控。例如，在演习开始之前，需向攻击人员明确提出禁止使用和谨慎使用的攻击方式，并在演习过程中通过终端录屏、终端管控、现场录像、平台流量审计等技术手段进行监控溯源；对于突破重要边界及核心业务系统的行为，需要有专家组及用户予以研判和审核，关注业务状态决定是否可以进行下一步突破。

核心点四、演习总结与问题整改

攻击队上报的攻击报告除包括攻击成果外，需要包含完整的攻击路径、木马及恶意程序上传位置、代码修改情况等信息。在演习结束后，通过平台记录的流量信息对攻击队提交成果的真实性进行审计；同时，组织方应及时通知各防守单位清理战场。避免已有攻击线索及遗留风险造成二次伤害。

演习的目的是为了掌握安全状态，指导防守单位后续开展针对性安全整改，因此需要组织方对本次演习的

成果做好总结、汇报，防守方需根据演习暴露出的问题及时进行整改、加固和复测，问题比较突出的单位，需要采用实战化的方式审视现有安全体系的有效性，开展专项安全规划、设计，将已有安全体系升级为可抵御实战化攻击的安全体系。

结语

组织一场安全、可靠、有效的实战攻防演习依托于人员配合和技术支撑，奇安信实战攻防演习服务可以有效的将人员与技术融合，在每一场演习开始之前都能做到心中有数。奇安信于 2019 年起，正式推出实战攻防演习服务，采用演习组织服务 + 演习平台的形式，为客户提供“全流程保障、全环境支撑、全风险可控”的全程管家式服务，保障演习的顺利进行。安

实践经验分享

大型企业的网络安全实战攻与防

作者 奇安信安全服务团队

根据奇安信参与实战化攻防演习的经验来看，随着攻防演习推广不断深入，涉及单位数量逐年增多，攻击手段逐年多样，防守方难度也在不断加码。实战化攻防演习在即，各大型企业最为关心的问题聚焦在如何有效应对实战化攻防演习。下面，奇安信从大型企业所面临的困境与建议两个维度出发，助力企业顺利开展攻防演习活动。

一、问题与困境

1、组织经验欠缺

从以往经验来看，参加防守的企业在演习前 2 个月才会接到通知并开始准备工作。企业工作人员需要注意实战化攻防演习与传统的渗透测试、合规检查的区别，以及企业需要部署的重点工作。

2、技防准备不足

参考历年来协助各大央企开展实战攻防演习的经验，下述几项内容往往会成为企业的防守薄弱环节：

（1）攻击面过多暴露

互联网出口和应用都是攻入内网的入口和途径。然而目前，仍然有部分集团型企业存在大量的互联网出口，分散发布了大量的互联网应用，防护措施良莠不齐，给攻击者创造了更多机会。

（2）资产情况不明

集团内有多少个互联网出口？这些出口 IP 有多少个？发布的互联网应用与 IP 端口的对应关系是什么？为这些应用开放的端口是否有必要？这些开放的服务是否存在安全漏洞？上述问题中任何一环的疏漏，都会造成互联网边界被突破、攻击者进入内网的严重后果。

（3）内网安全难以应对

部分企业内网存在“一张网”的问题，各子网间没有隔离和防护手段，少数企业甚至出现过从地区办事处的办公电脑可直接访问总部数据中心核心交换机的情况。

（4）访问控制不严

随着网络架构与业务的增长与变化，企业的安全策略非常容易混乱。防守单位很难在短时间内梳理和配置几十个应用、上千个端口的精细化访问控制策略。缺乏访问控制策略的防火墙，就如同敞开的大门，安全域边界防护形同虚设。

（5）安全态势未知

部分企业虽然采购部署了网络安全监控设备与网络安全态势感知平台相关工具，但是很难从每秒上千条报警信息中甄别出实际攻击事件。

（6）新型应用带来新的挑战

以远程办公为例，视频会议系统软件漏洞、VPN 密码爆破、远程连接通道被恶意利用等问题层出不穷，为网络安全带来了新的挑战。传统的企业安全防护架构能否满足新型应用和新型业务模式的安全防护需要，如何做好特殊时期、特殊应用的防护工作，同样是各企业网络安全人员需及时解决的问题。

3、人防队伍欠缺

由于种种约束和限制，部分企业在网络安全人才队伍建设上存在实际困境。其中包括人力资源缺乏导致企业难以建立健全的安全组织架构、缺乏支撑安全业务的各项能力；高级网络安全人才确实导致企业网络安全工作与防御体系难以与时俱进。

二、奇安信的建议

面对不断升级的网络安全威胁和严格的监管政策，

企业想要做好实战化网络安全工作需要从两个方面入手，一是深入完善网络安全体系建设，围绕规划、建设和运营三个阶段，不断深化开展企业网络安全域的划分、安全域边界的隔离和监控、安全计算环境安全的提升以及态势感知平台的建设。二是持续优化提升安全实战能力，在资产基础信息管理、资产全生命周期安全、安全防护体系全局评估、集团级应急响应体系等几个方面开展持续深入的安全运营工作。

企业在开展上述工作的过程中，建议重点关注以下几个方面内容：

1、安全运营工作的优化提升

安全运营工作水平体现在“全面、高效”两个方面。“全面”指资产信息掌握要全，“高效”指安全事件响应效率要高。

多数企业都已经部署使用 NGSOC 平台，基于 NGSOC 平台已有能力，深化开展基于流量的资产探测、资产漏洞发现、资产配置缺陷发现等工作。在监测问题得到良好解决的基础上，企业还可以通过深化应用 NGSOC 平台的自动化编排功能，简化安全事件处置操作，压缩企业响应处置安全事件的时间，提高企业响应安全事件的准确性，提升总体安全事件响应效率。

2、服务器安全的关键防护举措

首先需对服务器进行深入的威胁排查以及安全加固工作，包括病毒、后门、Webshell 的扫描删除、补丁更新、基线检查与配置等内容。同时，对服务器基本信息进行全面的收集和管理，例如端口、服务、应用、账户等，在这些信息的基础上，还需与主机安全加固产品结合，基于微隔离技术、HIPS 技术、Webshell 拦截技术等，对核心服务器做好精细化防护。最后，将上述内容统一做好详细记录，集中、安全存储与管理，供分析和溯源使用。

3、威胁发现能力的深入挖掘

企业需不断提升和完善未知威胁发现能力。威胁发现不仅仅是告警事件的分析与处置，而是结合网络流量信息、终端安全防护数据、服务器防护信息等多维度数据，进行综合分析研判，对照业务逻辑与日常规律，发现异常行为，定位未知威胁，描绘威胁攻击链、攻击时序、攻击范围以及攻击来源信息，为企业做全面的事件处置及采取加固手段提供真实、严谨的依据。

4、社工攻击防护的探索建设

在不断深化加强安全意识教育的基础上，企业需要组织钓鱼邮件、鱼叉邮件、交友诈骗、水坑攻击、WiFi 钓鱼、问卷调查、虚假活动等社会工程学评估活动，进行持续宣传教育。

5、工业控制系统的重点防护

在“安全分区、网络专用、横向隔离、纵向认证”的基础上，还要重点做好精细化访问控制和即时集中监控工作。若某工控系统被选定为演习目标系统，建议提前对该系统做详细的安全评估工作，摸清工控网现状，做好针对性防护。

“实战演习”中各单位集中力量、突击建设、调动一切内外部资源迎战，显然不是一种常态机制。然而，时时都在发生的网络空间安全对抗却是常态化的。上述建议取之于实战演习、用之于实战演习，希望能对企业从容面对攻防演习、切实降低安全风险有所帮助。安

实践经验分享

电网大集体企业实战攻防演习应对之策

作者 奇安信安全服务团队

为适应电力行业信息化和产业化发展的大趋势，电网大集体企业通过强强联合、充分发挥技术和资源优势，业务范围覆盖电力生产、调度、营销、信息管理等领域。随着电网大集体企业对网络的依赖程度越来越高，网络攻击也对企业的安全运转带来非常大的威胁，但企业对网络安全的重视程度并不相同，部分企业存在安全管理不细、安全技术措施不全、终端内外网访问控制不严、资产台账不清、弱口令屡禁不止、私搭网络、代码违规托管在第三方开源平台、违规外联等问题。

在实战攻防演习任务中，存在通过收集大集体企业敏感信息，并以大集体企业系统和网络作为跳板进入到管理信息大区的攻击尝试。如何在常态化、覆盖全网的实战攻防演习背景下，提升实战化网络安全保障能力是大集体企业网络安全管理者的重大挑战。经过奇安信在电力行业多年的实战化运营经验积累，建议在传统安全建设、运维体系的基础上，着重开展以下五方面工作。

一、互联网资产暴露面梳理

对互联网应用进行梳理，形成明确的资产清单，杜绝私搭私建行为，避免 IT 资产脱离管控。资产清单信息包括不限于所属单位、应用名称、访问方式、所属单位、内容描述、接入方式、域名、域名方式、外网 IP、外网端口、内网 IP、内网端口、上线时间、部署位置、服务器信息、中间件信息、数据库信息、运维信息、资产责任人等。要确实做到资产“底数清、情况明”，尤其对长期不维护不使用的“僵尸”系统务必确保全量关停下线，确保资产风险被发现和加固。

可采用 web 漏洞扫描技术、系统漏洞扫描技术、操作系统探测技术、端口探测技术、服务探测技术、Web 爬虫技术等各类探测技术进行资产发现。

二、敏感信息泄漏探查

情报收集是攻击队开展工作的必要基础手段，其会通过搜索引擎、学术类网站、网盘、代码托管平台、招投标网站、文库、社交平台、漏洞通报平台等地，探查与目标系统相关的资料、信息，作为防守单位有必要定期清理互联网上存在的敏感信息，包括系统技术方案、系统架构、软件源码、网络拓扑图、各类账号及口令等。

三、内网终端安全管控

针对部分大集体企业终端基数大、内外网访问未隔离、终端准入管控不严、违规外联的情况，可借助全流量分析和威胁情报能力进行全网终端病毒治理，把威胁域名进行逐一核实，依靠安全设备的威胁检测、终端安全管控系统的日志管理分析，结合对多个情报来源进行对比后，在安全设备和终端上阻断确认的恶意域名链接。

随着实战攻防演习对抗模式升级与变化，终端已经逐渐成为攻击的首选，终端对鱼叉攻击、系统文件白利用等攻击手段的精确检测发现变得尤其重要。通过持续终端行为采集、安全风险告警、威胁深度调查、多维度响应等手段，做好内网终端安全管控，尽可能压缩攻击者对内网终端的攻击时间，降低威胁通过内网终端达到攻击目的可能性。

四、社会工程学攻击防范

提高员工与第三方安全厂商人员保密意识，所有电网行业内部文件、信息（账号、密码、业务系统源代码、漏洞情况、系统域名、IP等）一律不得外泄；提高其网络安全意识，所有通过邮件、电话索要电网行业文件和信息的，一律不给；加强对电网行业数据的安全保护，梳理并彻底删除所有开发人员、运维人员、服务人员工作邮箱、个人邮箱（139、126、163、QQ邮箱等）中与电网行业相关的邮件；落实办公和生产场所安全护卫工作，严格履行进站联系单审核制度，发现可疑人员，立即汇报区域安全代表，并主动实施行为管控。

由定期开展信息安全意识培训升级为信息安全意识实测，真实检验员工信息安全意识水平，检验各部门、各单位信息安全意识工作开展成效和应急处置能力；潜移默化地让员工接受信息安全观念，帮助员工减轻数据泄密、病毒攻击、违规操作等困扰，构筑牢固的信息安全意识防火墙、构建信息安全文化氛围；积极推进信息安全防御体系建设、执行企业信息安全防护标准要求，为提升网络与信息安全防范能力提供教培依据。

五、持续开展技术检测

制定年度网络安全工作计划，持续开展技术检测，尤其是要开展日常全流量威胁分析即查即改，确保安全设备策略有效，树立安全措施不到位是失职、安全设备用不好是渎职的理念，克服设备一买、万事大吉的倾向。网络安全整改通知单要责任到人、查缺补漏、稳步推进、落实保障形成闭环。

网络安全工作讲一百遍不如“打”一遍，要通过实战化场景审视电网大集体企业的网络安全体系。网络安全管理与运营水平的提高，离不开电网公司网络安全归口管理部门的指导和帮助，电网大集体企业应继续在电网公司网络安全归口管理部门的指导下，有效落实网络安全工作责任制，坚决把网络安全抓紧、抓细和抓实，坚持“科学发展、安全运营”的原则，进一步加强信息基础设施的网络安全建设，完善安全运营管理体系，完成年度网络安全管理目标任务。安

实践经验分享

中小型银行实战攻防演习经验分享

作者 奇安信安全服务团队

受银行业务发展需要的影响，银行在通过互联网为用户提供便捷业务的同时，原本相对封闭的金融系统在互联网侧的受攻击面不断加大。尤其是以城商行、农信银行等机构为代表的中小型银行，由于体量等方面的因素，网络安全建设方面投入跟不上业务发展的需求变化，导致无法应对当前复杂的网络安全形势。对此，中小型银行该如何做好实战攻防演习的准备工作，奇安信总结了如下几方面的经验参考。

1、易受攻击的系统与设施需要重点关注

通过多年来的实战攻防演习分析发现，银行客户在实战中容易被攻击的系统主要集中在门户网站、信用卡系统、网银、电子商城等应用系统，除了这些核心业务系统外，一些非业务类的应用、中间件、平台等都可能作为主要攻击路径成为攻击者突破的重点。常见的攻击路径包括客服系统、教育培训系统、邮件系统等，也包括分支机构、开发测试网、金融云平台、第三方接入区、VPN、集权类系统、可以接入内部网络的个人终端等基础支撑环境。

2、以协同优先为原则，组织实战攻防演习工作

实战攻防演习是一个多军种作战、高频对抗的过程，在实战过程中，中小型银行可以考虑由行内高层领导挂帅，协调整体工作；网络安全部门作为主责方，牵头实战攻防演习的整体工作落实；数据中心作为主防单位，负责安全设备部署、安全监控等工作的落实；开发中心作为重要的处置单位，配合安全部门和数据中心整改已发现的应用系统问题。

3、强化积极防御能力，降低被攻陷的可能

在防守过程中，除了传统的防护设备之外，建议采用网络安全滑动标尺模型中的叠加演进理念，既要审视与补充原有纵深防护体系中对内网防护能力的不足，又要构建全面的安全监测能力，例如通过部署流量层面的威胁检测手段以及主机侧行为监测手段，并结合专业人员的威胁分析能力，及时发现进入到内网的攻击行为，并采取有效的处置措施，降低攻击带来的影响。

4、吸取大行经验，细节决定成败

演习过程中，攻击队会高度模拟黑客攻击的模式，攻击的范围可能会被无限延伸，对于中小型银行，需要在有相对完善安全防御体系的基础上关注细节，经过与各大银行实战攻防演习的经验总结，提供细节关注点示例如下：

（1）掌握真实的资产信息。在日常安全工作中以及在前期筹备阶段可以进行内、外部的资产梳理，如在实战中发现异常，可以快速定位，及时处理。

（2）梳理边界，汇总网络出口。尽可能地将出口归束在总行出口，减小暴露面、缩小攻击面，避免网络存在太多或不掌握的互联网出口。在此基础上结合攻击场景，梳理防范措施，并部署全流量威胁监测设备，提升安全监测能力。

（3）口令与权限管理。利用流量监测或主机防护等设备，对弱口令等问题进行发现，并及时让相关部门 / 中心对发现的弱口令问题进行整改。

（4）建立业务红线机制。攻击者的很多攻击并不能被传统的防御设备 / 系统所监测到，这需要针对演习中报备的目标业务系统建立安全红线机制，一旦发现异常，就

进行告警，常见主要的红线手段有：流量异常、严格访问 IP 白名单（只要不是白名单中的访问 IP，触发安全红线告警）。

5、通过实战攻防演习推动安全防护能力建设

实战攻防演习是阶段性的，但是安全工作是持久的。除了定期进行安全评估和渗透测试，有必要常态化组织开展本机构的实战攻防演习工作，评估当前安全防护状况，加强组织内部协调。同时将实战演习时开展的安全工作下沉到日常工作中，避免在演习前期短时间的突击，才能达到更好的效果。

6、提升内部人员防护能力才是根本

通过场景化安全运营培训，利用虚拟化平台，模拟实战化场景，采用创新的分组轮循式实操教学方式，为客户单位培养优秀的网络安全防护岗位人员，有效提升本单位发现和处置当前多种网络攻击的防护能力。

近年来，奇安信参与了众多国家级、省市级以及大型企业的实战攻防演习，积累并总结出一套完整的防守经验及最佳实践，实战攻防演习防护框架如下：

结合上述框架内容，为了更好地应对实战攻防演习工作，中小型银行需要经历如下几个过程：

筹备阶段：中小型银行在接到通知后，应首先成立实战攻防演习指挥工作小组，并明确分工；其次，指挥小组要合理地制定演习目标，围绕目标完善现有防御体系；最后，指挥小组需要协同内部、外部资源，制定实战攻防演习过程中各类方案及流程。

检查阶段：检查阶段的目标是收缩行内的暴露面、减少行内互联网侧敏感信息。安全检查需要从互联网侧和内网侧开展重点内容的检查，降低互联网侧的暴露面和敏感信息，同时加强内网侧弱口令、常规漏洞的整改，提升集权系统安全基线，限制攻击者在内网快速渗透和移动。

预演练阶段：中小型银行客户在此阶段可以组织一次或者两次预演习，采用互联网、内网等不同的攻击场景和路径，检验现有防御体系的有效性和安全运营团队协同的有效性。

值守阶段：在正式实战攻防演习阶段，指挥小组采用协同安全的理念，加强合作，协同内部部门之间、外部安全厂商之间通力合作、明确分工，一起做好正式实战攻防演习的攻击监测、分析和处置工作，尽量保证演习期间少丢分、不丢分。

总结阶段：组织复盘，针对过程中的不足，予以优化；针对演习过程中的优点，总结提炼并固化到日常的安全运营工作中，从而提升整体的安全防御能力。安

实践经验分享

政府单位网络安全实战攻与防

作者 奇安信安全服务团队

近年来，经过实战化网络攻防演习的洗礼，部分政府单位的防守工作捉襟见肘。在演习过程中，有时会出现关闭业务系统、封锁 IP 进行过度防守的情况，这种做法不仅违背了实战演习的原则，且对自身业务开展也有较大的影响。一旦攻击侧的战线拉长，这种不成熟的防线将显得脆弱无力，极易被撕破。

总结部分政府单位通过实战攻防演习发现的安全问题，主要集中在人、管理、意识、资产和工具几个层面。具体而言，很多单位存在没有专注网络安全岗位，没有从体系化、可持续的角度来培养与使用网络安全人员的情况；网络安全层面的组织架构不清、职责不明、相关制度难落地等管理问题，直接导致了安全事件监测、预警、分析和处置效率低；工作人员网络安全意识薄弱给了攻击者可乘之机；资产不清、资产管理不善、轻视边缘业务系统也是重要的安全隐患；已有安全产品的防护能力、安全策略有效性也亟待考量。

针对上述问题，奇安信根据以往经验，以攻击方的视角来看防守方常见的弱点，并列举有组织的攻击所采取的攻击手法，如下图所示：

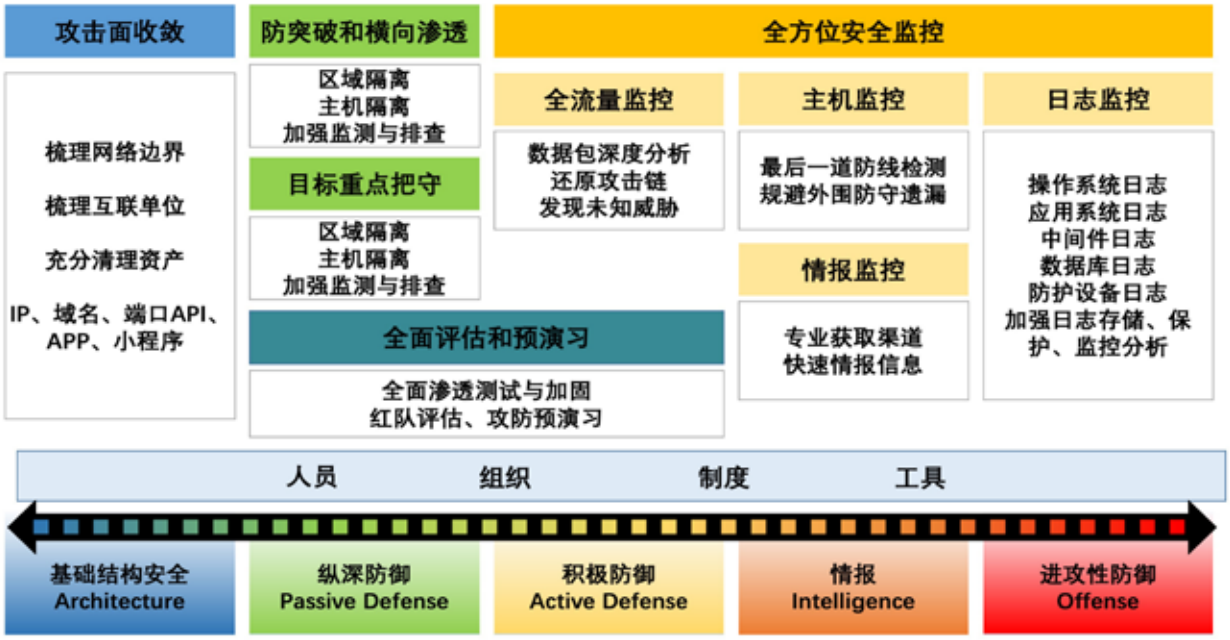
在了解了防守方的常见弱点和攻击方可能会采用的攻击手法后，政府单位该如何建立体系化的安全防护？

首先，最重要的是对自己的系统有掌控力，对于系统的资产情况、安全状态要有明确认知，并且有针对性的对缺陷做加固和修补。

其次，要有体系化的组织，要合理部署职责明晰、覆盖全面的安全专职队伍，并要有对应能力的人员匹配到相应岗位，技术人员应当具备攻防理论、威胁分析、应急处置等能力。

最后，要解决工具问题，要保证所有流量可见、全量日志可查、有可靠的情报输入，只依靠传统防护设备的被动防护是远远不够的。

下图将安全防护工作与滑动标尺模型进行对应，以



阐述安全防护的体系化：

1、攻击面收敛

“点的突破”会加大面防守的难度。对外暴露的资产越多，安全工作开展越困难。这就要求系统运营者必须充分了解自己的资产情况，要定期梳理自己的网络边界、可能被攻击的路径，尤其是有省－市－县多级网络架构的单位和外联接入的单位。如果正面攻击不成，攻击者往往会选择攻击下级单位、供应商等与目标系统有业务连接的单位，通过这些单位绕至目标系统内网。

2、全面评估和预演练

系统运营者对资产的安全状况也必须有充分的了解，周期性系统渗透测试是必须开展的工作，发现隐患，及时修补。通过自主开展演习工作（以红蓝对抗的模式）来检验安全加固工作的有效性，进行防护体系的动态评价。

3、防突破和内网横向渗透

一旦外层防线被撕破，攻击者会迅速进行内网横向移动，如果没有纵深防御体系，攻击方将如入无人之境。内外部访问控制（安全域之间，甚至每台机器之间）、主机层防护、重点集权系统防护、无线网络防护甚至物理层面的防护，都需要考虑。同时要加强内部的监测手段，从网络流量，主机日志、进程、文件等层面进行排查。

4、目标系统重点把守

核心目标系统是攻击方的最终目标，是整个系统的大本营。对关键系统进行定期的评估检查、渗透测试、整改加固是必要的，同时要保持安全监测工作的常态化开展。

5、全方位安全监控

攻击者会尽量隐藏痕迹，而防守者恰好相反，需要尽量提前发现攻击痕迹，并通过分析攻击痕迹，调整防护策略、溯源攻击路径。所以建立全方位的安全监控体系是安全防护的最有力武器，监控工作应当从网络层面的全流量监控、主机监控、日志监控、情报监控等多个维度开展。安

实践经验分享

运营商省级机构的网络安全实战攻与防

作者 奇安信安全服务团队

经过多年的安全建设，虽然多数运营商省级机构的主要安全防护手段已经逐步齐备，但是在面对有组织、特别是有国家背景的网络安全攻击时，依然会暴露出安全建设与运维过程中存在的一些不足之处，例如：

1、风险识别覆盖不够

其中包括资产管理不当、系统带病上线、敏感信息泄露、互联网暴露面大等问题，为攻击方提供更多突破口。

2、安全防护存在缺失

展开来说，人员安全意识薄弱、供应链防护不足，都会导致其中任一环节成为攻击方的重要目标，以及网络隔离策略粗放、终端安全管理薄弱、已知漏洞难以修复、集团系统防护脆弱等问题，也让部分省 / 专业公司网络安全防护难以抵御攻击。

3、安全检测能力不足

比如，难以发展强隐蔽性的 APT 攻击，部分省 / 专业公司只部署的基础特征检测的传统手段，APT 的检测、响应、溯源能力存在不足。

4、安全响应效率不高

其中包含响应效率需要优化和追踪溯源困难两个重要问题，部分省 / 专业因人工交互多、跨系统平台多、人员能力达不到要求等问题，导致响应速度慢，处置流程复杂、恢复周期长。在响应处置过程中，由于日志记录缺失、入侵痕迹被清除等原因，部分省 / 专业公司即便完成安全事件处置，也很难对攻击方进行高效追踪溯源。

针对运营商省级机构在面对有组织、特别是有国家背景的网络安全攻击时暴露的一些不足之处，除了建立有效的安全防护体系外，还应该重点关注以下六个关键点。

1、防止被踩点

省 / 专业公司首先应避免系统带病上线；其次应尽量理清本单位资产情况，清理泄露在公共信息平台敏感信息，加强全员（尤其是未参与信息化建设人员、第三方厂商人员）安全意识教育；同时应重点加强供应链的安全防范。

2、收缩暴露面

攻击者往往不会正面攻击防护较好的系统，而是找一些可能连省 / 专业公司自己都不知道的薄弱环节下手。这就要求省 / 专业公司应充分了解自己暴露在互联网的系统、端口、后台管理系统、与外单位互联的网络路径等信息，从攻击路径梳理、互联网攻击面收敛、外部接入网络梳理、隐蔽入口梳理等方面开展互联网暴露面的收敛工作。

3、开展纵深防御

在前期工作基础上，省 / 专业公司暴露在互联网上的资产必然会成为攻击者的首要目标。一旦一个点突破后，攻击者会迅速进行横向突破，争取控制更多的主机。所以省 / 专业公司应建立纵深防御体系，通过层层防护，尽量拖慢攻击者扩大战果的时间，将损失降至最小。

4、守住关键目标

上述所有工作都做完后，省 / 专业公司还应重点梳理目标系统及其相关系统的业务流和数据流、目标系统开放的服务及 API 接口、目标系统与其相关系统之间的数据传输方式和加密手段等。同时还对重点目标系统进行交叉渗透测试，对目标系统的进出流量、中间件日志进行安全监控和分析，充分检验靶标系统的安全性。

5、监控要全覆盖

建立全方位的安全监控体系是防护单位检测、响应、溯源最有力的武器，基于多年实战经验，有效的安全监控体系需在重点在全流量威胁监控、主机威胁安全监控、安全日志监控、情报预警监控几方面开展。

6、高效协同响应

借助全流量威胁监控和自动编排技术，辅以人工的分析研判，省 / 专业公司能够针对网络高级威胁的及时检测、响应、溯源，实现从以往出现安全事件的个案应急响应到实时全流量检测、实时自动响应处置、实时人工分析的持续响应的转变。安

实践经验分享

实战攻防演习终章：如何正确的复盘？

作者 网络安全部总经理 聂君

近年来，国内网络安全实战攻防演习飞速发展，已被广泛应用于检验防守方安全水平。实战攻防演习之后，收尾工作是复盘。通过复盘，仔细检视我们安全工作短板，提出改进加强点。本文介绍了如何进行一次“问题不会再犯”的复盘。

第一步：复盘方法论

1、复盘目的

同样问题不再重复；同类问题尽量避免；不要在低级错误上失败；从“复盘”到“复仇”。

解释下最后一点：复盘一般意味着防守方被找到了安全问题，“复仇”是指同类问题不会再犯。我们鼓励通过复盘分析，确定事件的根本原因，找到最终解决方案，并落地执行，防止此类事件再次发生，实现完美“复仇”。

2、复盘本质

复盘的本质是跳出事件本身，对问题进行有效管理。

我们经常提到：安全要像可用性一样运维。可以借鉴运维领域 ISO20000 的问题管理，通过问题管理流程，分析事件的根本原因，找到最终解决方案，并落地执行，防止此类事件再次发生。

问题管理流程将问题拆解为问题定义、关键角色、关键步骤三个基础项，对于复盘的结果需要设置衡量指标，对复盘的整个过程技巧进行提炼，以令其可以快速实现我们想要达到的目的。（见图 1）

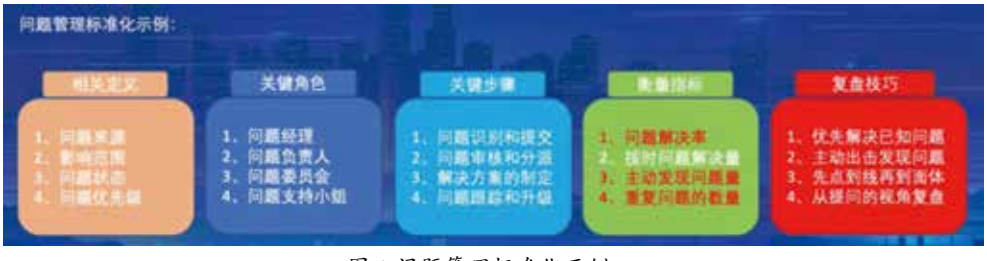


图 1 问题管理标准化示例

总而言之，就是从闭环、解决问题的角度出发，从提问的视角进行复盘，多问几个为什么，能不能做到，主动发现问题中潜在的问题或问题背后的根本问题，将问题一步步扩大到线、面、体，梳理出所有问题之后，先解决至关重要的已知问题。

复盘质量好坏，我们可以看几个衡量指标：

a） 问题解决率，指安全问题的解决比率，按照行业的问题关闭标准，我们的问题解决率能够到什么水位？

b） 主动发现问题数量，指安全问题中，哪些是被动发现，哪些是主动发现，主动发现问题数量和比例是多少？

c） 重复问题数量，指安全问题中，哪些问题是重复发生？

还有几个复盘注意事项：优先解决已知问题；主动发现问题，主动解决问题；先点到线再到面体；提问式复盘，鼓励思考，多提好问题。

3、提问式复盘

多问几个为什么，然后去追寻原因和答案，顺藤摸瓜就能彻底解决问题，实现正确复盘。（见图 2）

人员方面：

企业团队和员工清楚自己的安全职责吗？各角色员工具备安全意识和承担安全职责所需的安全技能吗（特别是安全团队没有安全意识和安全技能不足）？正向和负向安全激励对各团队和人员有效吗？

技术方面：

如何从技术层面，点状的防范这个问题？

复盘矩阵				
1、人员	责任	意识	激励	单兵技术
2、技术	测试	检测	防护	代偿措施
3、机制	有无	执行	验证	持续优化
4、资源	政策	支持	绩效	总体投入

图 2 复盘矩阵

有没有解决这一类问题的技术方案？技术手段是否可以被绕过？所有管理措施和流程是否有技术手段做落地保障？如果这个问题无法防护或者说无法 100% 防护，有没有安全检测方案？如果技术角度无法有效防护和检测，是否有管理措施代偿？能不能从其他维度降维解决这个问题？是不是我们解决这个为的技术方案不是最佳？有没有新技术方案解决这个问题？

机制方面：

安全事件发生，突破了我们哪些安全机制？突破的原因是什么？我们还缺乏哪些机制？机制足够的话，落实执行是否有效？安全管控是否被业务旁路掉？如果有人不遵守这个流程，我们安全团队能发现吗？安全运营持续改进流程运转情况？

资源方面：

安全团队是否资源足够？安全资源的分配顺序是否合理？除了人员编制和预算，安全政策的支持是否足够？

第二步，提出好的问题

1、我们怎么防御投递路径？

· 邮件监测，怎么保证邮件 100% 过沙箱？

· U 盘管控，怎么保证防护策略 100% 生效？

· 我们怎么保证没有未知的终端资产？

· 事中监控效果如何？

· 对终端提权监控 / 防御能力如何？

2、对凭证提取监控 / 防御能力如何？

3、对持久化行为监控 / 防御能力如何？

· 能不能发现攻击者的下一步行为？

· 横向移动？

· 反向隧道外连？

· 内部信息搜集爬取？翻看敏感信息？

4、安全运营

· 是否有数字化指标来实时显示覆盖率？正常率？怎么维持高覆盖率？

· 是否制定一线运营人员处理告警的 SOP？SLA？

· 能否快速溯源？

· 怎么复盘告警能发现安全隐患？

· 安全隐患如何解决？

5、更多

· 新攻击手法的发现跟踪（例如 C# Assembly）

· 新安全技术的调研使用（例如零信任、SOAR）

第三步，人员、技术、机制、资源，四维要素深入分析

1、人员

在复盘时，可以从人员的安全意识、安全职责、安全技能进行分析：

人员安全意识是否足够？分三个层面：公司全体员工、信息技术部门员工、安全团队。公司全体员工的安全意识，需要通过实战化的安全意识攻击测试来提高。信息技术部门员工安全意识，需要结合开发、运维的不同特点来针对性设计提高方案。安全团队的安全意识，主要看是否具备对安全风险的感知能力。

是否清楚知道自己的安全职责。研发认可自己需要在 12 个小时内确认并修复高危漏洞并发版吗？运维认可自己需要在 Windows 月度补丁推出后一天内批准补丁，并在 3 天内完成高危漏洞在生产服务器上的修复吗？公司全体员工认可自己感知到网络安全异常后应该反馈异常给信息技术部门吗？安全团队大部分时候一厢情愿的认为其他团队的安全职责划分，但实际安全事件发生后才发现分歧，并花了大量时间在管控分歧。

人员安全技能是否足够？研发人员是否具备修复漏洞的知识和技能，运维人员是否具备实施基础架构安全的技

能，安全人员是否具备足够的处理告警的安全技能等等。安全事件的背后深层次原因，可能是人员的技能不足，导致无法胜任其所承担的安全职责。

2、技术

技术维度复盘，讲究点、线、面、体。（见图 3）

点：在终端上的攻防对抗领域，单个技术点包括：常见权限维持工具 CobaltStrike 检测、无文件攻击、终端插 U 盘等物理攻击方式，提出单点技术防护和检测方案。

线：同一类问题构成了技术线。除了 CobaltStrike，我们还应该具备针对同类型的渗透测试和权限维持框架（如 Nishang、Empire）进行防护和检测。

面：技术点和线构成了技术面，这个技术面就是：终端安全的攻防对抗。其他技术面还有：终端安全之基础架构安全（身份认证、可信）、终端安全之数据安全等。

体：技术面构成了体。除了上述技术面之外，终端安全这个体还包括去 AD 化、网络安全域划分和隔离、零信任体系等等。比如复盘时考虑网络二层隔离，所有终端和终端都无法在二层通信，只能访问公共应用（OA、Mail、CRM、Git...）。

除了点线面体，技术维度还可以考虑是否引进新技术，从底层进行改造，从根源上解决问题，比如 Google BeyondCorp、BeyondPod 的引入和实践。

3、机制

复盘的时候，我们要追问一下：这个事件的发生，是不是机制有缺失？机制有的话，是不是执行落地没有保障？以及灵魂发问：如果有人不遵守这个流程，我们安全团队能发现吗？

安全运营持续改进流程则是对安全事件的闭环管理，每笔安全事件的处理结果最终必须为误报、属实，二选一。如果是误报，必须改进 SIEM 安全检测规则或安全 Sensor 监测措施。如果属实，根据已经被突破的层进行针对性的改进。安全运营持续改进要求每天、每周、每月都坚持进行安全事件 review，有可能重要事件被一时大意的一线人员放过，也可能是其他原因。

安全运营持续改进流程的质量可能决定了整个企业的安全工作质量。

4、资源

很多时候安全工作不能顺利开展，都是因为资源问题。

改变理念：安全团队是因为工作干得好，才能获取资源；而不是拿到了资源才能干得好。

上层文化：抓住公司的文化、组织、变革的变化，及时嵌入安全，让安全从中获益。当公司有巨大变化、活动时，一定要想到加入安全的元素、成分。

获取资源策略：作为安全团队的负责人一定要主动去想办法争取更多的资源，常见的有将安全工作显性化，通过红蓝对抗中打胜仗、重大安全事件复盘、对标同等或更好的企业投入，以获取更多的资源。

主动创造资源：从管理学的角度来讲就是胡萝卜管理哲学，公司给到员工的报酬肯定是有限的，除了金钱外，可以主动创造一些荣誉，在内部进行奖励和激励，特别是很支持安全工作的部门和个人。

本文节选自奇安信集团网络安全部总经理聂君的一次专题分享，本次分享还包括多个实战场景复盘案例、实战下的安全建设新思路等内容，关注公众号“奇安信集团”，发送“实战复盘”即可查看全文。安

图 3 技术维度复盘示例

全球国防网络安全演习新模式新形态解析

作者 网络空间安全军民融合创新中心 赵慧杰

在和平时期，网络演习竞赛既是检验网络部队作战水平的“试金石”，也是锤炼网络部队作战能力的“磨刀石”和发展网络攻防战术的“铺路石”。2020年以来，虽然受新冠疫情影响，美欧等国仍通过各种方式开展网络演习训练和竞赛活动，在实战中评估网络部队战备水平，检验和提升部队的网络作战能力。

一、举行新型战术演习，磨练部队网络攻防技战术

面对作战概念、作战场景、作战需要的变化，美军正在对网络演习进行动态创新发展，改进演习形式，改善演练内容，从而使网络战士更好地为战术作好准备。

美国空军第567网络空间作战大队开展名为“狩猎活动”（Hunt Event）的演习活动，并迅速将该活动发展成为国防部最大的网络空间演练活动之一。该大队旨在更好地训练防御“猎手”，改善防御战术、技术和程序（TTPs），并发展防御性间谍技术。

演习每两个月举行一次，主要训练战士如何在网络上开展“狩猎”。除了美国空军的网络保护团队（CPTs）外，来自空军特殊调查局、专门防御空军任务和设施的任务防御小组的成员也参加了演习。

相比以往给定脚本的夺旗演习培训，该演习实现了APT级别上训练，使得网络战士模拟与使用TTPs的高级敌手开展对抗，以帮助网络战士不断成长并成长为真正的“猎人”。

美国陆军正在更改“网络闪电战”（Cyber Blitz）演习，以帮助努力塑造和装备一个新的多域编队。该活动2021年将转变为“多领域实时作战”（MDO Live）。

作为更大规模的“保卫太平洋”演习的一部分，它将主要支持多域特遣部队的情报、信息、网络、电子战和太空（I2CEWS）支队。改变“网络闪电战”的一个主要原因是需要使多域作战和力量成熟，目的是使陆军和部队可以专门评估和提供有关技术的反馈，以此来确定作战需求。

二、举行信息作战演习，整合网络和信息作战效果

美军将信息能功列为基本作战能力，将其划分为三组活动：一是了解作战环境中的信息；二是利用信息影响相关行为者的行为；三是支持友好的人为和自动决策。美军正在寻求将网络与信息环境中的其他能力进整合，从而扩大网络的影响范围。2020 年以来，美军已经举行多次聚焦信息作战的演习活动，通过实战演练提高部队信息环境作战能力。

美国陆军第 915 网络战营于 10 月 1 日至 12 日在印第安纳州慕斯卡塔克城市培训中心开展首次专门演习。该部队由陆军网络司令部于 2019 年正式创建，规划由 12 支远征网络和电磁队（ECT）组成，致力于运用网络战、电子战和信息战能力支持旅级战斗队伍或其他战术编队。

目前，该部队目前仅有的第 1 远征网络和电磁队（ECT-01）参加了此次演习，以测试和训练部队的概念和战术。第 915 网络战营指挥官表示，此次演习的首要任务是确保远征网络和电磁队的培训水平并构建围绕该部队场景，次要任务是制定训练计划，以指导未来如何培训新成立的远征网络和电磁队。

美国国民警卫队于 9 月 12 日至 26 日举行“网络盾牌 2020”演习，此次演习更加注重信息作战。约 800 多名美国陆军和空军国民警卫队成员参加演习，重点放在信息行动和减轻网络司令部战备评估中发现的漏洞上。

“网络盾牌”演习负责人乔治 · 巴蒂斯泰利表示，部分志愿者将开展影响力行动，而提供更多地防御性网络行动要素，可使网络保护团队获得更多能力来鉴别上述行动，上述团队在现实世界中也就越能辨别它们。

此外，美国空军计划于 2021 年春季在新墨西哥州普拉亚斯市新建立的信息战训练基地举行一次信息战“旗帜”演习活动。该基地致力于完善信息战战术，例如磨练网络电子战和电磁频谱能力。

三、举行军民融合演习，完善网络威胁响应防御体

网络安全领域具有天然的军民融合特性，发展网络安全军民融合已经成为欧美各主要国家维护国家安全的普遍做法。美欧以关键基础设施防护、公私和军地部门协作共享为重点，举行军民联动网络演习活动，组织军事、政府、私营机构参加，不断完善网络空间军地协同防御机制。

美国新英格兰国民警卫队 7 月 21 日至 31 日举行“网络扬基 2020”演习活动，旨在测试警卫人员和关键基础设施运营商的网络能力。参与人员包括来自新英格兰各州的文职人员、现役官兵和联邦政府成员等。因疫情影响，出席本次演习的人数较往年减少，部分人员通过网络远程参与。

本次演习主要对象为新英格兰 6 个州的电力和水利系统，内容包括：以社交媒体话题帖模拟真实互联网环境，测试人员需从海量信息中辨别可用来支持决策和识别风险

的内容；识别被攻击的网站，找出攻击源并实施维护；保护计算机文件不被窃取或利用等。

新英格兰国民警卫队官员表示，该演习活动能够帮助国民警卫队、关键基础设施运营商和政府之间建立合作伙伴关系，以在真正危险到来时了解情况并及时应对。

美国陆军网络学院 9 月组织美国军方及私营部门的网络安全专家与美国两座城市合作开展“Jack Voltaic 3.0”演习，测试市政部门在模拟网络攻击中的响应能力，特别是期间对于多种模拟物理破坏的应对举措。除了查尔斯顿与萨凡纳市政府、南卡罗来纳州与乔治亚州国民警卫队、陆军网络司令部、海岸警卫队之外，参与本次演习的还有 Verizon、AT&T 等私营企业。

演习中，南卡罗来纳州的查尔斯顿与乔治亚州的萨凡纳成为恶意软件与勒索软件的攻击目标，旨在测试其抵御数字威胁的能力。除此之外，演练攻击方还设计同一系列物理层面的紧急状况，进一步提高了演练难度。在对抗恶意软件攻击的同时，市政部门还需要处理模拟形式的货船事故、灌水与报警系统故障。

美国防部和能源部于 10 月在普拉姆岛举行演习，旨在为全美各大型电力供应商提供重要的防御指导，同时应对黑客组织对电力行业工控系统的持续入侵。

此次演习以远程方式开展，仅有 30 人以内电力公司雇员及政府承包商获准登岛。演习通过反常规场景设计，以有效模拟人员如何针对广泛网络攻击做出远程响应。演习规划者们还充分借鉴了相关真实案例，例如俄罗斯 2015 年涉嫌对乌克兰电力基础设施发动网络攻击。

演习要求电力企业指派真正的一线员工组成防守团队，尝试在一系列强有力的网络攻击之后快速恢复电力供应。参与者必须使用发电机逐步重启电力系统，而后沿供电线路恢复各处变电站，且全程测试由 DARPA 提供的取证工具能否准确捕捉到攻击方留下的痕迹。DARPA 的快速攻击检测、隔离和特征识别系统（RADICS）提供的仪表板在演习中发挥了巨大作用，该仪表板使用户得以准确监控网络活动，甚至可以发现系统是否有异常。

四、举行网络攻防竞赛，发现安全漏洞并培养人才

除军事演习外，美军还举行网络攻防竞赛活动，组织人员在仿真场景中开展攻防演练，以达到发现安全漏洞、培养网络人才、提高实战经验等目的。

美国太空部队以虚拟形式举行“黑掉卫星”网络安全竞赛将。竞赛将分两阶段举行，包括 5 月 22 日至 24 日的在线初赛资格认证活动，以及 8 月 7 日至 9 日的决赛在线资格认证活动。在第一阶段竞赛中，将允许黑客和研究人员入侵地面“扁平卫星”的电子组件。进入决赛的参赛黑客，将尝试通过拔下植入的“旗帜”或软件代码来攻击轨道上的一颗小型卫星。获胜最多的前三支球队将赢得高达 5 万美元的奖金。

美国空军表示，国防部已经成为“黑掉卫星”网络安全竞赛的主要支持者，因为该竞赛能够帮助美国军方发现其系统中的缺陷，并且可以借此机会发现网络安全人才。

应美国网络司令部要求，美国“梦想港”于 11 月 16 日至 19 日举行“黑掉楼宇”网络攻防演习活动。该演习将展示信息技术、物联网和运营技术网络攻击对关键建筑物自动化和任务运营的影响。根据活动安排，11 月 16 日举行攻击演习；11 月 17 日举行攻击演习，以及楼宇自动化和控制系统网络安全虚拟会议和小场地比赛；11 月 18 日、19 日举行攻防对抗活动。

五、举行国际联盟演习，增强网络空间作战协同性

美欧盟国将联盟关系从现实世界推动到网络空间，通过加强在网络空间的合作，在新兴作战领域建立集体作战优势，力图掌握未来作战主导权。2020 年，相关国家继续举行联合网络演习活动，促进盟国之间在网络空间的练兵协作。

美国网络司令部于 6 月 15 日至 26 日举行“网络旗帜 20-2”演习。此次完全是防御性演习，来自 5 个国家的 500 多名参与者和 17 个团队参加，其中包括美国国民警卫队、美国能源部和“五眼”联盟国家。

演习旨在继续建立防御性网络作战伙伴关系，提高“五眼”联盟抵御网络侵略者的整体能力。此次演习涉及到相关团队保护 IT 和作战安全网络，对抗敌方试图破坏、拒止和降级空军基地作战能力的行动。遭受到攻击的网络是模拟的工业控制系统，可为航空加油站、电网、空中交通管制雷达和电子门禁系统生成网络流量。攻击以针对燃油和电力设备的恶意软件形式出现。

欧盟网络与信息安全局 6 月举行“网络欧洲 2020”演习，旨在建设网络安全能力，加强欧盟合作并提高医疗健康领域的网络安全意识。

“网络欧洲”演习是欧盟网络与信息安全局目前主办的最大规模活动，每两年举办一次，今年是第六次，活动场地分布在整个欧洲的几个中心地带，并由演练控制中心统一协调。参加演习的人员来自欧盟各成员国的网络应急机构、电信、能源企业、网络安全部门、金融机构、互联网服务提供商，以及其他私营公司和公共组织。

军心如铁 战必胜

——走近奇安信网络实战攻防演习总指挥张翀斌

作者 公关部 孙丽芳

军人出身的张翀斌，非常喜欢战斗前夕的那种气氛。他当兵多年，在信息化和网络安全领域打过无数硬仗，每逢备战，便厉兵秣马，枕戈待旦。

3月1日，北京正经历倒春寒，北风萧瑟，一夜返冬。而在位于西直门外南路26号的奇安信安全中心会议室里，大家摩拳擦掌，气氛非常热烈。

副总裁张翀斌正在主持奇安信今年的网络实战攻防演习启动会。

不久后，全国规模的网络实战攻防演习将正式打响。

用实战检验“网络安全领军者”成色的时刻，也就又要到了！

听完总体部署，会场里有的人跃跃欲试，有的人暗自较劲，凝重而又兴奋的气息四处弥漫。

多年担任奇安信网络实战攻防演习总指挥的身份，让张翀斌得以长时间、近距离，对网络实战攻防演习进行深度参与、仔细观察、深入思考。

迈出关键的第一步

“网络实战攻防演习最早是美国从2006年开始，主导的全方位大规模网络安全演习‘网络风暴’，咱们国家的网络实战攻防演习是从2016年开始的。”

张翀斌1999年毕业于解放军理工大学通信专业。2000年，部队开始搞信息化，当时对口的人才很缺，学通信的张翀斌被选中先“顶上”，开始转行搞信息化和网络安全。这一搞就是21年，淬炼为行业“老兵”。

“当时奇安信就在协助国家有关部门和单位做网络实战攻防演习的技术支撑，我们也派出了攻击队，也就是蓝队”。

2016年的实战攻防演习参演单位数量较少，攻防重点大多集中于互联网入口。

“不过，对于中国关键信息基础设施网络安全保护的工作，迈出了关键的一步。

静态的标准和要求解决不了动态的攻击

对于网络实战攻防演习的重要意义，张翀斌觉得，再怎么强调，都不为过。

“传统的网络安全这么多年走下来，大家是怎么衡量网络安全部门的成绩呢？第一是合规要求，如通过测评看分数的高和低。第二就是上级部门的工作检查。过去就只有这两种办法。网络实战攻防演习改变了整个网络安全行业的规则，改变了网络安全主责部门，让大家理解到，在合规的基础上一定要去考虑实战化，它们是叠加的关系，不是互相谁取代谁的关系。”

张翀斌曾任中国信息安全测评中心副总工、处长，曾获国家和部级科技进步奖多项，主持和参加多项安全标准的制定工作。但是对于合规、标准这件事，张翀斌一直有自己的看法。

“网络安全领域有个特殊性，它是实时对抗的，也就是不论在何时何地，都有人惦记着你。所以我以前一直提，反对用传统‘质检’的思路来管理网络安全。比如水的标准，标准一旦制定可以多年不用修订。为什么？因为没

有人会故意操纵水的组成，让水去改变，去对抗这个标准。但是网络安全领域面临的情况是，某项标准公布的当天，就是树立了一个标靶，攻击者就会寻找其中的漏洞和缺陷，找到攻击方式，这也就意味着该标准就会失效。合规是必须的，但是只合规是远远不够的。”

静态的标准和要求解决不了动态的攻击，能解决这一问题的，张翀斌认为，正是网络实战攻防演习。

“合规驱动的是正向网络安全防护思维，而攻防演习突出逆向思维，体现的是实战化。这就是说即使测评得了 100 分，检查没有任何问题，也不代表你的工作就做好了，因为你没有经受过实战的检验。

打造实战攻防利器

改变甲方的同时，网络实战攻防演习对乙方的改变，张翀斌觉得，也不亚于一场地震。

“对于安全厂商而言，以前客户的最大需求就是合规，那大家就围绕合规做产品。但一旦实战来临，这些产品到底能不能发挥作用？其实大家心里都没底。

所以实战网络攻防演习开始后，就逼着产业要去做出能够实际发挥效益的产品。这就有了比如我们奇安信高级威胁检测产品天眼，服务器加固产品椒图云锁、态势感知与安全运营平台 NGSOC 等等，这些都是实战化的新产品，是对传统安全产品的有力补充。老三样（防火墙、入侵检测系统和反病毒）有用，但面对实战，只有老三样是远远不够的。我们的这些产品就是在实战化的过程中被催生、被打磨，被检验出来的，而且每年都被检验。”

在网络实战攻防演习的战场摸爬滚打多年，张翀斌对各种“武器”的性能了如指掌。

“圈子里流传着一个段子，无天眼不演习。”张翀斌笑着说，“实战攻防演习发展到现在这个阶段，这句话也不仅仅是一个段子了，它真实反映了天眼的实战地位。”

提起天眼这款在实战攻防演习中屡建奇功的利器，张翀斌赞许有加，天眼能够主动采集全流量进行检测分

析，并把所有网络会话以日志的形式记录下来，帮助防守队的分析师进行攻击溯源，针对加密流量的检测也有很好的效果。

“可能有人也知道，国内追溯到的第一个海外 APT 组织海莲花，就是天眼检测到的。机会留给有准备的人，这话我认为特别对。奇安信作为一个后起之秀，能有今天的市场地位，我觉得就是抓住了机会，这里很重要的就是网络攻防实战演习。从 2016 年最开始，我们抓住了机会，我们产品就跟上来了。今年，我们还整合了另外一个针对服务器安全防护的重量级武器——椒图。我相信很快，业内这句话会改为叫：无天眼和椒图，不演习。”

攻防俱佳 组织得力

2016 年以来，在国家有关部门的有力推动下，网络实战攻防演习日益得到重视，演习范围越来越广，演习周期越来越长，演习规模越来越大。从国家到行业到地方，都在积极地筹备和组织各自管辖范围内的实战演习。

而从最初就参与了网络实战攻防演习规则制定、平台开发的奇安信，多年来已经全面、深入参与到了这项工作中，并凭借自己的绝对实力，“打”出了攻防俱佳、组织得力的好战绩。

“2016年我们蓝队的攻击方法还很传统，基本就是从外部互联网往里打，到后来，如0Day漏洞攻击、团队社工、身份仿冒、钓鱼WiFi、鱼叉邮件、水坑攻击等高级攻击手法，在实战攻防演习中已屡见不鲜。攻防相持，这里面就会发生很多有意思的事，比如说供应链的攻击，我们蓝队就有过这样的战例。”

“当时我们的靶标是某单位的官网。对方屯重兵防的特别好。那我们怎么办呢？你的官网肯定不是你自己开发的，总有供应商给你开发，对吧？那我们就在想，供应商有没有你家的源代码呢，以及供应商为了维护方便，有没有可能存有你家的账号密码呢？顺着这个思路，我们直奔供应商。供应商根本就没想过自己要防。很快，供应商就被打下来了。这个供应商为了方便维护，随时测试，搭了一套跟客户一模一样的系统挂在互联网上。这套测试系统的账号密码跟实际在跑的系统完全一样。我们把这边打下来后，到了官网都不用攻击，正常登录就把系统控制权拿下来了，防守方全程毫无察觉。”

因为成绩突出，奇安信的蓝队非常受欢迎，邀约不断，全年无休。

“我们蓝队的规模大，承接的任务也多。我们可以同时打几十场，其他厂商可能只能同时打几场。”

仅2020年全年，奇安信就参与了全国范围内数百场实战攻防演习的蓝队活动，攻破了数千个目标系统。项目涵盖党政机关、公安、政企单位、民生、医疗、教育、金融、交通、电力、银行、保险、能源等各个行业。奇安信在所有行业化的实战攻防演习排名中名列前茅。

“对于我们的红队（防守团队），客户的原话是：‘确实专业’。我想，专业体现在三个方面。一是我们有一套完整的体系化的框架。告诉客户，这件事分几个阶段，

每个阶段应该做什么工作，然后分几个组，哪些厂商必须协同。我们给客户担当的是技术指挥的角色；二是我们队员的技术能力确实强；三是我们的队员非常敬业，干活积极主动。客户的赞扬是由衷的”。

能攻善守之外，奇安信还长于组织。我们推出的实战攻防演习服务，采用演习组织服务＋演习平台的形式，为客户提供全流程保障、全环境支撑、全风险可控的全程管家式服务，保障演习的顺利进行。”

截止目前，奇安信已参与组织实战攻防演习数百次。组织演习的对象包括部委、省市级政府、省公安和网信等主管机构，以及银行、交通、能源、民生等行业单位。

不是一个人在战斗

一直管理着奇安信实战攻防演习团队的张翀斌，虽然已离开部队多年，身上仍留有明显的军人特质。人品正直、性格也直，雷厉风行、说话不绕弯、脾气有点爆。而手下的技术高手们，普遍反映是:“很喜欢跟着老张干”。多少有些粗豪的张翀斌，是怎么来带这群兵的呢?

“第一是要成就大家，也就是给大家成长的条件，有人带你，有人教你，同时待遇有保证、激励措施到位；第二是体系化作战，我们构建了一套体系化的作战系统。队员在场上不是孤军奋战，一看作战目标是这样的，哪些工具我直接就能用，哪些工具仓库里没有，马上告诉后台我缺什么，后台立刻组织研发这个工具。这是战时，而在平时，我们除了对队员们进行知识点、技能的培训，很重要的是进行战法的总结，大家在一起复盘自己的得与失。我用这个方法打进去了，但用那个方法就没奏效。这样大家会觉得每打一场我就提高一次，而且不是一个人在战斗，会越来越体会到整体作战的感觉。大家身体可能累但心不累。”

有了制度的保证和充分的战前准备，演习真正开始的时候，总指挥张翀斌并不喜欢呆在指挥室，而是去前线，到防守方驻场。

“作战方案我之前都过完了，由副总指挥顾鑫在家坐镇，我会去客户现场。因为首先，客户现场是真正能发现问题的地方。我去了一般一呆就是一天，从早上8点到晚上11点，客户所有的会我都参加，跟客户一块研判，当天的工作全部完事我再撤。第二，去发现我们自己人有什么问题，发现我们这个防守工作组织的有没有问题。第三其实也是去看望大家。演习的时候，驻场的队员天天熬夜，非常辛苦。”

2021年大年三十，张翀斌到客户现场看望值守的同事们。

2021年的网络实战攻防演习即将正式开始，今年还是重保大年，有建党100周年、冬奥会相关的系列重保工组。除了网络实战攻防演习，张翀斌还带领着公司的服务团队，今年的工作压力可想而知。张翀斌有两个女儿，大女儿今年中考，理想的学校是101中学，这也是全家今年的核心目标。而繁忙的工作让张翀斌在这件事中，只能当个甩手掌柜。张翀斌感慨地说：“祝愿女儿能考上理想的学校。家人是我的大后方，有她们的支持和包容，我才能在网安前线安心工作。等我退休了，我给她们娘仨当后方”。安


CRYPTOCURRENCY HACK
HACK
CRYPTOCURRENCY
HACK

在奇安信内部的一次实战攻防演习中，攻击队利用某销售员的安全意识淡薄，成功渗透进内网并下发彩蛋。

网络空间的攻防博弈是残酷的。一次小小的失误，就能被攻击队抓住并无限放大，最终以你意想不到的方式，击穿防守方的防线。因此对于防守方而言，你需要的不仅仅是优秀的产品、优秀的攻防专家，更需要健全的网络安全管理制度和全体员工的安全意识。

大事记

奇安信与阿里云达成战略合作

3月4日，阿里云与奇安信(688561.SH)宣布达成战略合作，双方将围绕重点行业的云安全领域进行自主研发，同时将在工业物联网、应急与攻防演练等场景，展开技术、产品、市场、资本等领域全面深入合作。

根据协议，阿里云与奇安信将共同打造适配主流云计算平台的云+安全解决方案。同时，奇安信与阿里云整合双方在产业资源、技术生态、人才培养、安全运营等方面的优势，共同拓展新的业务合作。

面对国内云安全等新兴安全需求的爆发，奇安信积极布局网络安全新赛道。其中，奇安信基于内生安全框架，打造出了一站式安全能力交付平台——云安全管理平台，涵盖数据安全、主机安全、网络安全和应用安全的全栈安全能力，成为奇安信“云+网+端”一体化安全体系构建的重要组成部分。IDC报告显示，奇安信云安全管理平台凭借18.1%的市场份额，位列国内安全资源池第一名。

北京网络安全大会（BCS2021）全球议题征集活动开启

3月18日，BCS主席、奇安信集团董事长齐向东宣布，第三届北京网络安全大会（BCS2021）议题征集正式启动。

本次议题征集围绕关键信息基础设施安全、安全规划与建设、数据安全、5G安全、云安全、供应链安全、区块链安全、工业互联网安全、物联网安全、车联网安全、人工智能安全、移动安全、远程办公安全、威胁情报、攻防对抗、零信任、商用密码、身份安全、应用加密、隐私计算、代码安全、安全运营、DevSecOps、SD-WAN、SOAR（安全编排与自动化响应）、SASE安全访问服务边缘、等保2.0、隐私保护、网安政策法规、网络犯罪打击治理、安全意识及安全人才培养等网络安全前沿技术和研究方向。

奇安信顺利完成2021全国“两会”网络安全保障工作

3月11日，2021年全国“两会”在北京顺利闭幕。“两会”期间，在网络安保主管单位的统一指挥下，奇安信组织2700人次技术人员投入安保任务，积极配合开展检查检测、实时监测和应急值守处突，圆满完成了网络安全保障工作，得到了相关部门的认可和表扬。

经过多年的重保任务实践，奇安信在重保指挥体系化方面积累了丰富的经验，形成了成熟的一线专家值守、二线应急支撑、三线产品保障以及后勤保障的专业重保运营机制。

截至目前，奇安信已先后完成了国庆70周年、亚洲文明对话大会、一带一路高峰论坛、海军建军70周年、全国两会、春晚、中非合作论坛、上合组织成员国峰会、十九大、博鳌论坛等国家级网络安全保卫任务。

国投董事长、党组书记白涛一行调研奇安信

3月12日上午，国家开发投资集团有限公司（以下

简称国投）董事长、党组书记白涛一行到访奇安信，与奇安信集团董事长齐向东等公司高管进行了座谈交流。

调研期间，白涛对奇安信近些年的快速、高质量发展以及展示出来的网络安全技术能力表示赞誉。他说，网络安全市场空间巨大，十四五期间，国投将进一步加大布局战略性新兴产业，网络安全将是一个重要领域。国投将与奇安信从资本、业务等方面开启更大合作，努力在落实国家创新驱动战略、科技自立自强、发挥国有经济战略支撑作用、以及守护国家网络安全等方面做出表率。

奇安信与通辽市政府达成战略合作 助力通辽市数字经济发展

3 月 18 日下午，通辽市委副书记、市长郭玉峰一行赴奇安信集团考察，并与奇安信签订战略合作协议。双方将在通辽市开展全方位网络安全产业战略合作，共同打造通辽市数字经济网络安全产业园，助力通辽市数字经济发展。

协议约定，奇安信将为通辽市提供不限于物联网、大数据、云计算、数据中心、新基建等全方位网络安全服务。双方将围绕网络安全中心及平台基地建设、网安人才培养、攻防演练、网络安全技术共享等方面深入推进，促进通辽市网络安全产业生态发展，支撑新基建的网络安全建设，为通辽市构建现代产业体系保驾护航。

GSMA 发布《人工智能赋能安全应用案例集》奇安信多项成果入选

世界移动通信界的三大国际组织之一，GSMA（全球移动通信系统协会）在 MWCS 21（世界移动通信大会）上发布了《人工智能赋能安全应用案例集》（以下简称《案例集》）。

奇安信集团天眼产品线提供的“基于机器学习的未知恶意代码检测”、“针对 DGA 隐蔽域名的人工智能发现机制”，以及数据智能产品线提供的“基于人工智能与机器视觉的视频行为分析系统”等成果入选该案例集。

央视对话吴云坤：钱在哪，黑客就盯上哪

在 CCTV 2《对话》栏目中，奇安信集团总裁吴云坤表示，对于网络安全来说，数字化比较特别。

从防范黑客的角度看，“钱在哪里，黑客就会盯上哪里。”吴云坤指出，随着数字经济发展规模的增长，黑客产业链规模已经超过了千亿，病毒产生速度也从万级到千万级；在大数据、人工智能技术的加持下，病毒检测的速度也从此前的分钟级进化为毫秒级。数字经济对网络安全行业的推动作用可见一斑。

吴云坤认为，网络安全产业将在数字化的未来发展占据重要位置。

上市刚过半年 奇安信入选科创 50 指数样本股

据上交所公告，根据指数规则，上海证券交易所与中证指数有限公司决定于 2021 年 3 月 15 日起，对科创

50 等指数的样本进行调整，调入奇安信等 5 只股票。

“科创 50”指数作为首条表征科创板市场的指数，是投资者观察科创板市场的重要参考，指数成交金额（量）显示为全部科创板证券的成交金额（量），可方便投资者观察科创板整体情况。

按照指数调整规则，现阶段新股上市满 6 个月后可纳入样本空间。此次调入科创 50 指数样本股的奇安信，是网络安全龙头企业，于去年科创板开板一周年之际正式上市。刚过 6 个月即被调入科创 50 指数样本股，足见资本市场对奇安信的认可。

羲和实验室发布春节期间 DDoS 攻击报告：春节七天假 黑客在加班

奇安信旗下羲和实验室发布的春节期间 DDoS 攻击报告显示，春节假期期间（即 2021 年 2 月 11 日至 2021 年 2 月 17 日），奇安信星迹 DDoS 观测系统累计观测到反射放大 DDoS 攻击事件 65912 个，涉及被攻击 IP 57096 个。绝大部分被攻击 IP 分布于中国香港和美国；大陆被攻击 IP 主要分布于我国东部及南部省份。与春节前一周相比，DDoS 攻击事件数增加约 25.0%，被攻击 IP 数增加 37%。可见，春节期间 DDoS 攻击呈显著增加态势。

《2020 年人工智能优秀产品和应用解决方案》正式发布 奇安信监管类态势感知成功入选

国家工业信息安全发展研究中心（简称“中心”）发布的“2020 年人工智能优秀产品和应用解决方案”名单中，“奇安信网神网络空间安全态势感知与协调指挥系统”（简称：奇安信监管类态势感知平台）成功入选。

奇安信作为国内最早推出网络安全态势感知技术及平台的安全厂商，通过 7+1 能力体系，集业务能力、数据能力、技术能力、服务能力、安全能力、呈现能力、交付能力为一体，以平台化技术进行整合，建立知行合一、平战结合、攻防兼备、智能开放的网络安全治理平台，使其成为监管机构、行业主管部门治理、保护网络安全的核心抓手。

作为多个国家级重大活动网络安保的独家支撑平台，2020 年，奇安信监管类态势感知参与了全国两会、世界互联网大会、国家网络安全宣传周、贵阳数博会等多个重大活动，并为数十次实战攻防演习活动，提供了网络安全监测与指挥保障。

奇安信与科蓝软件达成战略合作 助力金融科技安全融合创新发展

奇安信科技集团股份有限公司与北京科蓝软件系统股份有限公司在科蓝公司总部签署战略合作协议，达成全面战略合作，奇安信集团总裁吴云坤、副总裁陈华平，科蓝软件董事长王安京、副总裁田忠广出席签约仪式。

此次达成战略合作，奇安信与科蓝软件将发挥各自专业优势，在银行系统、CRM 系统、电子支付平台等产品与服务展开深度合作，联合发布行业应用解决方案，推动网络安全与电子银行业务技术融合；合作共建金融科技安全创新实验室，围绕电子银行应用场景，共同探索安全 + 应用的新业务场景；合建安全响应中心，在研究、技术、市场、服务等方面协同并进，促进行业可持续发展。

本次合作是奇安信“共享、共生、共赢”融合生态体系的重要体现。双方战略合作的达成，有利于安全技术融入到更多的金融场景与行业应用当中，实现安全技术对金融科技领域的价值加成，推动网络安全与电子银行业务技术融合。

雄安科企联第一届理事会二次会议召开 齐向东连任会长

在雄安新区科技创新企业联合会（以下简称雄安科企联）第一届理事会二次会议上，表决通过了会长连任、秘书长及副秘书长提名等决议。科企联会长、奇安信集团董事长齐向东成功连任。

在会长发言时他表示，发起雄安科企联，就是为了凝聚多方力量，更好地为雄安新区建设服务，同时也助力企业自身实现高质量发展。

本次科企联理事会以“聚焦雄安建设·融动科技新城”为主题，齐向东在会上作《2020 年雄安科企联理事会工作总结及 2021 年工作规划》工作报告。他表示，新冠疫情带来了前所未有的考验，并且仍将持续。如何应对新冠疫情带来的严峻挑战，是必须面对的难题。

对此，齐向东提出了三点建议：第一，坚定信念，逢山开路、遇水架桥。第二，耐住寂寞，勇于创新、敢于蜕变。第三，开放合作，取长补短、互利共赢。

奇安信与水运院共建联合实验室

近日，奇安信（688561.SH）与交通运输部水运科学研究院签署智能航运网络与信息安全联合实验室共建协议，双方达成合作关系。实验室将依据《智能航运发展指导意见》，共同加快推进交通强国、网络强国和数字中国建设。

根据协议，奇安信与水运院联合开展智能港口、智能船舶、智能监管、智能航保、智能航运服务领域的网络和信息安全需求调研、技术开发、实验测试和人才培养，共同探索智能航运网络和信息安全行业应用解决方案，联合推进智能航运网络和信息安全标准化工作。

此次合作对我国智能航运意义重大，联合实验室将围绕智能航运发展过程中所涉及到的网络和信息安全问题，专注于前瞻性技术研究和示范项目建设，开展产、学、研、用一体化的关键技术研究、装备系统开发和工程示范应用，逐步提升我国智能航运网络和信息安全水平以及相关软硬件产品的市场竞争力。

荣誉墙

奇安信获赛可达实验室两项大奖 终端安全能力再获认可

近日，国际知名第三方网络安全服务机构——赛可达实验室发布了 2020 年度赛可达优秀产品奖（SKD AWARDS）获奖名单，奇安信天擎终端安全管理系统内置的 QOWL 反病毒引擎、终端检测与响应（EDR）凭借强大的终端安全检测和反病毒能力，斩获赛可达实验室两项大奖。

赛可达方面表示，所有获奖产品都经过了赛可达实验室专业测试团队的严格测试，所有测试都参照了国内外最新产品标准和发展趋势，在接近真实应用场景中完成，各获奖产品彰显出了它们在网络安全行业各自细分领域的国际先进水准。

奇安信终端安全专家表示，QOWL 引擎是一款完整

的反病毒特征引擎，具有丰富的格式识别和解析能力、支持 PE 和非 PE 病毒查杀，可完美修复被感染文件、能检测近十年的高危漏洞。

SKD AWARDS 自 2013 年至今已成功举办七届，得到了国内外网络安全界的认可，被誉为“网络安全产品的奥斯卡”，已成为衡量网络安全产品水平的重要指标之一。奇安信天擎一举获得两项大奖，侧面映证了其安全能力在该领域的领先地位。

科创板 225 家上市企业有效发明专利排行榜 奇安信位列第五

在知识产权产业媒体 IPRdaily 与 incoPat 创新指数研究中心联合发布“科创板 225 家上市企业有效发明专利排行榜”中，奇安信 (688561.SH) 以中国有效发明专利数 473 件、全球发明专利数量 1299 件位列榜单第五。

据统计，自科创板开板以来，截至 2021 年 2 月 1 日，科创板上市公司达 225 家，IPO 募资合计 3180.48 亿元。该排行榜对 225 家企业截至 2021 年 2 月 2 日公开的中国有效发明专利数量（不含港澳台）进行了统计分析，其中，中国有效发明专利数量在 100 件以上的有 29 家企业，中国有效发明专利数量在 400 件以上的企业仅有 6 家。

排名	企业全称	证券代码	证券简称	证监会行业(门类/大类)	中国有效发明专利数量/件	全球发明专利数量/件
1	中芯国际集成电路制造有限公司	688981	中芯国际-U	制造业/计算机、通信和其他电子设备制造业	2298	5272
2	中国铁路通信信号股份有限公司	688009	中国通号	制造业/铁路、船舶、航空航天和其他运输设备制造业	695	2358
3	昆山龙腾光电股份有限公司	688055	龙腾光电	制造业/计算机、通信和其他电子设备制造业	662	1305
4	华润微电子有限公司	688396	华润微	制造业/计算机、通信和其他电子设备制造业	548	1180
5	奇安信科技集团股份有限公司	688561	奇安信-U	信息传输、软件和信息技术服务业/软件和信息技术服务业	473	1299
6	中微半导体设备（上海）股份有限公司	688012	中微公司	制造业/专用设备制造业	467	1142
7	天能电池集团股份有限公司	688819	天能股份	制造业/电气机械和器材制造业	392	1201
8	交控科技股份有限公司	688015	交控科技	制造业/铁路、船舶、航空航天和其他运输设备制造业	374	811
9	深圳光峰科技股份有限公司	688007	光峰科技	制造业/计算机、通信和其他电子设备制造业	357	1774
10	天合光能股份有限公司	688599	天合光能	制造业/电气机械和器材制造业	289	816
11	北京金山办公软件股份有限公司	688111	金山办公	信息传输、软件和信息技术服务业/软件和信息技术服务业	244	931
12	中科寒武纪科技股份有限公司	688256	寒武纪-U	信息传输、软件和信息技术服务业/软件和信息技术服务业	242	1385
13	福建福光股份有限公司	688010	福光股份	制造业/仪器仪表制造业	233	535
14	浙江中控技术股份有限公司	688777	中控技术	信息传输、软件和信息技术服务业/软件和信息技术服务业	200	520
15	杭州安恒信息技术股份有限公司	688023	安恒信息	信息传输、软件和信息技术服务业/软件和信息技术服务业	197	1255
16	天臣国际医疗科技股份					

作为该专利排行榜前十名中，唯一一家信息传输、软件和信息技术服务业企业，也是唯一一家网络安全企业，奇安信一直坚持“强研发”战略，其重视研发程度在行业内有目共睹。

奇安信零信任远程访问解决方案获“金智奖 · 优秀解决方案奖”

近日，2020 年度（第五届）“中国网络安全与信息产业金智奖”评选结果公布。奇安信科技集团股份有限公司（以下简称“奇安信”）零信任远程访问解决方案从多个解决方案中脱颖而出，斩获“优秀解决方案奖”。

奇安信零信任远程访问解决方案是奇安信零信任身份安全整体解决方案关键场景的子方案。该解决方案立足于零信任架构的“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四大关键能力，可适用于业务访问、远程运维、开放众测等多种业务场景，对应用、功能、接口各个层面形成纵深的动态访问控制机制，既适用于传统办公访问场景，在云计算、大数据中心、物联网等新 IT 场景也具备普适性。

由信息安全与通信保密杂志社发起的“金智奖年度评选”至今已成功举办了五届，被中国网络安全产业视

为发展的风向标，得到了业界的高度关注和认可，有效地提升了企业的影响力、竞争力和品牌价值，并推动了网安产业的发展。

金融信创生态建设成效显著 奇安信获专业实验室认可

近日，金融信息技术创新生态实验室（以下简称“实验室”）给奇安信集团发来感谢信，对奇安信在金融信创生态工作中发挥的积极作用给予感谢，并期望未来和奇安信展开更深层次的合作。这标志着奇安信在金融信创领域的综合能力获得行业高度认可，在金融信创领域的市场拓展驶入快车道。

实验室由中国人民银行领导，中国金融电子化公司牵头组建，是专注金融信息技术创新的重要基础设施和专业化实验平台，多家重要金融机构和产业机构、金融信创生态产学研用相关单位参与其中。

实验室在感谢信中对奇安信 2020 年在基于金融业务场景的适配验证、技术攻关和标准制定方面及金融行业信息技术创新解决方案和实施路径拓展方面给予实验室的支持和发挥的积极作用表示衷心感谢。

奇安信网神获 CNNVD 年度优秀技术支撑单位等两项荣誉

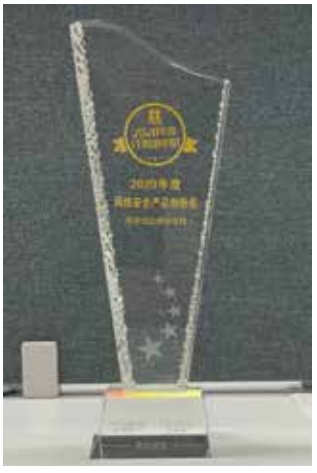
根据《国家信息安全漏洞库（CNNVD）技术支撑单位计划指南》相关规定，国家信息安全漏洞库对现有 115 家技术支撑单位 2020 年度支撑贡献情况进行了总结评价。

2020年度CNNVD获奖单位清单

序号	项目类别	评选单位
1	一、年度优秀技术支撑单位	北京启明星辰信息安全技术有限公司
2		北京奇虎科技有限公司
3		北京知道创宇信息技术股份有限公司
4		北京天融信网络安全技术有限公司
5		北京华云安信息技术有限公司
6		北京长亭科技有限公司
7		北京神州绿盟科技有限公司
8		深信服科技股份有限公司
9		网神信息技术（北京）股份有限公司
10		杭州迪普科技股份有限公司
11		北京数字观星科技有限公司
1	二、漏洞报送专项奖	北京奇虎科技有限公司
2		北京启明星辰信息安全技术有限公司
3		北京天融信网络安全技术有限公司
4		北京神州绿盟科技有限公司
5		北京长亭科技有限公司
1	三、漏洞预警报送专项奖	北京知道创宇信息技术股份有限公司
2		杭州迪普科技股份有限公司
3		北京启明星辰信息安全技术有限公司
4		网神信息技术（北京）股份有限公司
5		北京奇虎科技有限公司
1	四、年度新秀奖	重庆梦之想科技有限责任公司
2		南京中新赛克科技有限责任公司
3		内蒙古洞明科技有限公司

奇安信旗下网神信息技术（北京）股份有限公司作为一级技术支撑单位，获得 CNNVD“年度优秀技术支撑单位”和“漏洞预警报送专项奖”两个奖项。

奇安信边界安全栈荣膺 2020 年度 IT 影响中国网络安全产品创新奖



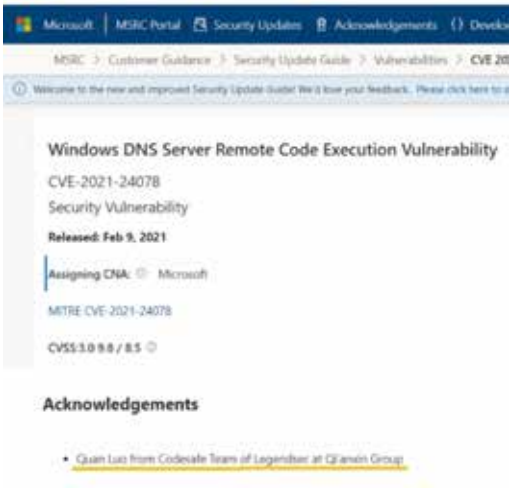
日前，2020 年度 IT 影响中国特别奖项“网络安全产品创新奖”揭晓，奇安信边界安全栈凭借创新的产品理念、领先的产品能力获此殊荣。

作为科技行业的年度影响力评选，2020 年度 IT 影响中国深入挖掘行业创新价值、倾听消费者心声、聚合业内最

强资源，评选表彰优秀、创新的科技产品、品牌和行业数字化转型最佳实践。

奇安信边界安全栈通过智能服务链编排，实现安全资源集约化建设、灵活按需部署；结合 SSL 解密功能，可对加密流量进行解密及针对性调度；在业务上线、变更、下线的全生命周期中，提供定制化安全防护，进而提升整体安全防护能力。

中国安全研究员首次发现微软蠕虫级严重漏洞获微软致谢



奇安信代码安全实验室研究员为微软发现一个严重的 DNS 服务器远程代码执行漏洞 (CVE-2021-24078)，第一时间报告并协助其修复漏洞。微软针对该漏洞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。

该漏洞是首个由国内安全研究员发现并提交的蠕虫级漏洞，危害巨大，CVSS 评分为 9.8 分，堪比去年微软修复的类似漏洞 (CVE-2020-1350)。

隐私合规能力获认可 工信部致信感谢奇安信

近日，因高效配合和助力工业和信息化部（简称：工信部）发起的 APP 侵害用户权益专项整治行动，奇安信集团收到了来自工信部的致信感谢。

工信部在感谢信中指出，APP 侵害用户利益专项整治是践行以人民为中心发展思想的具体行动。工信部自 2020 年 7 月开展专项行动以来，积极凝聚产业力量，推动建设全国 APP 技术检测平台，持续加大监管力度，APP 个人信息保护工作取得积极成效。

感谢信中称，在专项行动期间，奇安信积极响应工信部号召，发挥自身技术优势，高效配合和助力工信部技术手段建设和专项治理等工作，为专项行动顺利开展提供了强大保障。

奇安信隐私卫士负责人表示，工信部感谢信是对公司 APP 隐私合规检测技术与能力的认可。未来隐私合规产品线将依托盘古团队对安卓和 iOS 系统的深刻解读，结合奇安信全面的安全服务能力，共同服务监管，在进一步加强对多方监管的支持同时，也积极为广大的企业进行 APP 隐私合规检测能力与服务的输出，切实落实各级政府和部委对 APP 隐私合规要求，维护好用户个人信息安全、数据安全，推动产业健康、持续发展。

工业和信息化部司局简函

感 谢 信

奇安信科技集团股份有限公司：

APP 侵害用户权益专项整治是践行以人民为中心发展思想的具体行动。工业和信息化部自 2020 年 7 月开展专项行动以来，积极凝聚产业力量，推动建设全国 APP 技术检测平台，持续加大监管力度，APP 个人信息保护工作取得积极成效。

专项行动期间，你公司积极响应我部号召，发挥自身技术优势，高效配合和助力我部技术手段建设和专项整治等工作。在此，特向你公司的大力支持，及盘古、安全服务团队，和晏晨、陈洪斌、王菁、徐龙华、赵帅、刘涛、吕百奎、陈圆成等同志的辛勤工作表示衷心的感谢！

未来，我部还将继续深化 APP 侵害用户权益专项整治工作，希望你公司再接再厉，继续做好相关工作，共同与我部维护好用户个人信息安全、数据安全。

工业和信息化部信息通信管理局

2021 年 1 月 29 日

奇安信

防范钓鱼邮件

• 网络安全部温馨提示

- ☆ 钓鱼邮件一般利用人们使用习惯、焦急心理等因素进行钓鱼攻击
- ☆ 收到可疑邮件需要仔细观察邮件有没有异常提醒或提示，核对发件人信息与邮件所显示的是否一致
- ☆ 谨慎面对邮件中的链接，不相信任何弹出的要求输入账号密码的页面
- ☆ 遇到公司部门发送需要收集信息的通知邮件，要通过蓝信聊天 / 必读号核实
- ☆ 附件先用天擎杀毒再打开
- ☆ 除了邮件外警惕二维码、社交软件聊天、加微信等社会工程学钓鱼。你以为的交友，可能是为了套取你的信息
- ☆ 警惕上下文关联的钓鱼邮件
- ☆ 保护好公司和个人的信息、权限、不确认不提供，遇到问题及时联系网络安全部（g-sec@qianxin.com）

奇安信

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

网络安全科普系列

网络安全实战系列

国际经验分享系列

网络安全认证系列

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。

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁情报中心

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证