极牛网络安全通讯 • 社群期刊 2021 年 8 月 第 2 期

网安观察



P15
网安行业投融资大爆发：2021年上半年已超去年全年

P20 网络安全实战攻防演习的五大演变
P22 攻防演习暴露十大薄弱环节
P27 九大措施应对网络攻击"七十二变"

第 2 期
2021年8月

极牛网

极牛网 网络安全行业媒体

致力于促进中国网络安全行业创新思维的交流与碰撞，搭建中国网络安全技术社区和交流平台



技术格局

网安工程师的成长，需要锻炼开阔的技术视野和统筹全局的战略高度，能够着眼现在思考未来，做懂业务懂策略的工程师。

管理之道

网安工程师随着职业发展，必然面临着向技术总监、CTO等管理角色转型，改变管理思维，建立属于自己的管理哲学。

人才梯队

作为技术管理者，如何建立一个稳固、高效的人才队伍是核心任务，更应该从人才梯队的角度，关注人才的培养的更迭。

企业战略

技术管理者应该建立技术以外的格局，经济形势、商业模式、投融资等等，才能助力企业发展，做与创始人同频的CTO。

产品运营

敢于拥抱和应对变化，敢于创新，在创新的基础框架下，寻找创新的实践方法论，激发技术人员创新能力，推动业务发展。

布道能力

作为技术工程师，需要重点培养自己的布道能力，能将自己的技术成果和理念传播出去，才能拓宽和升级自己的认知边界。

网络安全的本质是攻防对抗

——写在建军94周年之际

2021年上半年，全球范围内网络安全重大事件频发，供应链攻击、勒索攻击、工控设备攻击、APT攻击、数据窃取等各种攻击手段层出不穷，网络攻击也成为大国间对抗的热点话题。未来，国家背景的网军、APT组织、有组织网络犯罪将成为网络安全最大的威胁，网络攻击的目标、手法，产生的破坏都突破常规，威胁不断升级走向高端化。

对于 中国的网络安全产业未来的发展有以下观点：

一、攻防对抗是本质

网络安全的本质应该是攻防对抗，必须从攻防视角来理解网络安全，而安全的对手并非同行，而是病毒木马黑客、网络安全黑产或是某些来自国家的网络攻击部队。

一切的网络安全标准和规范的推进最终都是为了实现在真实的网络攻击中的攻防对抗能力，在完善IT架构的安全建设规范后，需要以护网行动为标准推动以实网攻防对抗的目标的攻防演练常态化，这样才能真正检验网络安全的能力。

二、对抗的核心是人才

网络安全的攻防对抗归根结底是双方人才的较量和对抗，想要真正夯实我国网络安全的能力就必须重视网安人才的培养。我国在高校端的网安人才培养才刚刚开始改革，网络空间安全一级学科才刚开始在部分高校建设。

在下一阶段希望能加快网络安全学科专业和院系建设，并建立适合网络安全人才培养的创新机制，加强网络安全教材的建设，让一线的网络安全工程师将真正的攻防对抗经验形成教材，避免重理论轻实战的老路。强化网络安全师资队伍建设，目前高校教师鲜少有网络安全资深专家，建议引进有教学能力的一线工程师进入高校授课，并且推动高校和企业的合作育人协同创新机制。

三、未来的趋势是协同

网络安全的发展趋势必然是协同创新，由于网络安全产业的特殊性，必须由国家在法律法规层面进行规范，通过政策和产业资源进行统筹，形成国家与企业、企业与企业之间的协同效应。

国家需要重视在网络安全数据和能力方面与民营企业的合作，在网络安全中政府起到一个领导者和指挥者的作用，融合政府、国企、民营企业的能力和数据，提升国家网络安全能力。

国家需要在国防装备发展中大力推进军民融合。雷神公司是美国的网络安全国防承包商，它就是一家民营公司，这个公司先后收购了WEBsense、黑鸟等多家公司，它的安全能力强了，美国国防网络安全水平自然就会提高。在这点上美国模式很值得我们学习，在网络安全领域推进军民融合。

总顾问

叶绍琛

2021年8月1日

CONTEN

目录



安全态势

P5 | 美国数十家医院诊所遭勒索攻击系统瘫痪，患者紧急转移

P5 | 国际电信巨头 T-Mobile 遭遇重大安全事件，近 5 千万美国用户数据泄露

P6 | 国内摄像头黑产治理：发现 4 万多个联网摄像头漏洞

P6 | 知名计算机制造商技嘉遭勒索软件攻击，上百 GB 数据失窃

P7 | Linux kernel 拒绝服务漏洞（CVE-2021-38207）预警

P7 | Realtek SDK 多个高危漏洞预警

P8 | Microsoft Exchange 多个远程代码执行漏洞预警

P8 | Linux eBPF 本地提权漏洞安全风险通告

P9 | 国内攻防演习 7 月态势：哪些薄弱点最易被利用?

P12 | 《个人信息保护法》表决通过，2021 年 11 月 1 日起施行

P12 | 网信办等五部门发布《汽车数据安全管理若干规定（试行）》

P13 | 《党委（党组）网络安全工作责任制实施办法》公开

P13 | 美参议院通过基础设施法案，为网络安全拨款 20 亿美元

产业发展

P15 网安行业投融资大爆发：2021 年上半年已超去年全年

P16 | 20 年未见安全公司估值如此快速上升

P16 | 2021 年网络安全投资将达去年 2 倍

P16 | 大手笔并购和 IPO 层出不穷

P17 | 云安全与身份安全是投资热点

P17 | 中国投融资交易数量超以色列，但金额远逊

P18 | 豪赌下一个 CrowdStrike



ONTENTS

网安专题

P20
网络安全实战攻防演习的五大演变

P22
攻防对抗演习暴露十大薄弱环节



P27
九大措施应对网络安全攻击的“七十二变”

P31
2021网络安全实战攻防演习“兵器谱”



第 2 期
《网安观察》编辑部
主办 极牛网

总 编 辑：陈鑫杰
总 顾 问：叶绍琛
副 总 编：王文彦
安全态势主编：乔跃春
网络攻击主编：王新睿
漏洞情报主编：黎治声
移动安全主编：蔡国兆
安全人才主编：林俊濠
安全产业主编：张 程

公众号　小程序　网站

电子版请访问 www.jikenb.com 阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

E m a i l：hi@jikenb.com
地 址：深圳市龙岗区江灏科技园1栋西座
邮 编：518000
电 话：0755-33228862

印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

版权所有 ©2021 极牛网，保留一切权利。
非经极牛网书面同意，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，极牛网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，极牛网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。



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

事件篇

关基网络威胁形势严峻，美国电信巨头近 5 千万用户数据外泄，南非重要港口系统瘫痪数天官方称属于“不可抗力”；勒索软件持续猖獗，美国数十家医院诊所系统瘫痪致使患者紧急转移，咨询巨头埃森哲数据外泄被索要 3.2 亿元赎金，知名计算机制造商技嘉上百 GB 数据外泄……



美国数十家医院诊所遭勒索攻击系统瘫痪，患者紧急转移

据 Arstechnica 8 月 17 日消息，8 月 15 日凌晨，美国医疗连锁机构 Memorial Health System 遭遇勒索软件攻击，致使 IT 系统瘫痪，旗下 3 家医院无法正常运营。Memorial Health System 旗下拥有 3 家医院和 64 家诊所，遭到攻击后，3 家医院着手将急诊病患转移至卡姆登克拉克医疗中心，大部分诊所取消了安排在次日的所有非紧急手术和放射性检查，建议患者提前来电沟通商议应对办法。今年以来，已出现数十起针对医疗机构的网络攻击活动。

国际电信巨头 T-Mobile 遭遇重大安全事件，近 5 千万美国用户数据泄露

据 Vice 8 月 15 日消息，国际电信巨头 T-Mobile 旗下美国公司遭遇了一起重大安全事件。有网络犯罪论坛上兜售其超过 1 亿用户的敏感数据，包括姓名、社保号码、电话号码、居住地址、IMEI、驾照等信息。卖家声称，在两周前入侵了 T-Mobile 的生产、部署和开发服务器，窃取了多个数据库共计 106GB 数据，包括可以追溯到 2004 年的 IMEI 历史数据库。卖家还声称，此举是为了对美国情报机构进行报复，打击美国的基础设施。T-Mobile 后续回应称，确认近 5000 万用户的个人信息遭泄露。

咨询巨头埃森哲遭勒索软件攻击数据外泄：对方索要 3.2 亿元赎金

据 The Record 8 月 11 日消息，勒索软件团伙 LockBit 发布公告，声称已攻破国际咨询巨头埃森哲的内网，窃取了 6TB 内部数据，要求支付 5000 万美元（约 3.2 亿人民币）的赎金。根据泄露数据样本显示，主要有埃森哲的产品手册、员工培训课程及各类营销材料等，似乎不包含任何敏感信息。埃森哲随后承认，确实遭到勒索软件攻击，但公司运营未受到影响，相关系统已通过备份副本恢复。

越南知名安全厂商 Bkav 源代码泄露，售价 25 万美元

据 VNExpress 8 月 11 日消息，越南知名网络安全公司 Bkav 旗下产品的源代码遭到窃取，在一个数据泄露论坛上被出售，总价 25 万美元。卖家声称，已成功入侵了 Bkav 的服务器并窃取了产品源代码，被出售的源代码包括反病毒等产品，以每个 1 万至 3 万美元的价格出售，其中一个人工智能程序的源代码标价 10 万美元。Bkav 公司确认泄露的源代码是真的，但都是旧代码，泄漏不会

影响到客户。该公司还表示，该事件是一名前雇员造成的，泄露时间在一年前。

国内摄像头黑产治理：发现 4 万多个联网摄像头漏洞

据网信中国 8 月 9 日消息，今年 5 月以来，中央网信办会同多部门深入推进摄像头偷窥等黑产集中治理工作。其中，网信办对存在隐私视频信息泄露隐患的 14 家视频监控 APP 厂商进行了约谈，并督促其完成整改。工信部组织对 18 家具有行业代表性的视频监控云平台开展检查，发现处置 SQL 注入、越权操作等一批高危漏洞；全面排查联网摄像头存在的安全隐患，发现 4 万多个弱口令、未授权访问、远程命令执行等摄像头漏洞，取证并处置 500 余个。公安部查获非法控制的网络摄像头使用权限 2.5 万余个。

知名计算机制造商技嘉遭勒索软件攻击，上百 GB 数据失窃

据 The Record 8 月 6 日消息，中国台湾知名计算机制造商技嘉遭 RansomExx 勒索软件攻击，位于总部台湾的系统被迫关闭，多个网站无法访问，超 112GB 签署过保密协议的商业数据遭泄露，涉及英特尔、AMD 等合作伙伴。攻击者威胁称，除非支付赎金，否则将公开被窃取的数据。过去几年来，台湾电子制造业一直笼罩在勒索软件攻击的阴影之下，富士康、宏碁、研华、仁宝、广达以及佳明等知名厂商均遭受过重大打击。

内部人员反水！勒索软件团伙 Conti 攻击手册泄露

据 BleepingComputer 8 月 5 日消息，一名反水的 Conti 加盟机构成员在地下论坛发帖，公开泄露了有关 Conti 勒索软件操作的信息，包括 Cobalt Strike C2 服务器的 IP 地址和一个 113MB 的档案，其中包含大量用于进行勒索软件攻击的工具和培训材料。该成员表示，他发布这些材料的原因是在一次攻击后的分赃中只获得了 1500 美元，而团队的其他成员却将赚取数百万美元。有威胁情报专家指出，此次泄露的攻击手册与 Conti 的活跃案例相符，基本可以确认是真实泄露。

意大利地方疫苗接种预约系统因网络攻击被迫关闭

据路透社 8 月 1 日消息，意大利拉齐奥地区政府表示，黑客攻击了管理罗马周边的拉齐奥地区 COVID-19 疫苗预约的公司的 IT 系统，导致疫苗预约系统被迫关闭。该地区官员在 Facebook 上说：“一场针对该地区数据库的强大黑客攻击正在进行中。”所有的系统都被停用，包括该地区的卫生门户网站和疫苗接种网络的系统，接种计划可能会因此受到延误。意大利警方正在调查此事，找出攻击的幕后黑手。近日，意大利跟随法国宣布，接种疫苗或提供 COVID-19 免疫证明，将成为参加各种聚集活动的强制要求。

南非重要港口因网络攻击系统瘫痪近一周，官方称属于“不可抗力”

据 Moneyweb 7 月 27 日消息，南非国家运输公司（Transnet）港口部门在 7 月 26 日宣布，近期遭遇的网络攻击事件属于不可抗力性质，这在全球尚属首次。该事件导致其港口运输系统瘫痪近一周，该公司随即将港口系统转为手动操作，但随着卡车运输的进一步延误，导致多个港口出现故障，特别是负责南非全国超六成运输量的德班港遇到严重阻塞问题，港口部门只能发布“不可抗力”通报。港口部门是南非国家运输最大和最重要的部门，它的发声可以证明这家公司甚至南非全国港口物流确实遭受了重大打击。

漏洞篇

8月，微软爆出多个漏洞预警，包括Exchange服务多个远程代码执行漏洞、Windows 打印服务最新 0day 漏洞、Windows NTLM 中继攻击漏洞等；根据华云信安威胁情报中心显示，近期需重点关注 27 个高风险漏洞……



Linux kernel 拒绝服务漏洞（CVE-2021-38207）预警

2021 年 8 月 16 日，网络安全威胁和漏洞信息共享平台发布预警，Linux 发布了 Linux kernel 存在拒绝服务漏洞（CVE-2021-38207）的风险通告。攻击者可利用该漏洞导致拒绝服务，Linux kernel 低于 5.12.13 的版本均受影响。目前官方已修复该漏洞，建议受影响用户及时更新至安全版本，并做好资产自查及预防工作，以免遭受黑客攻击。

Realtek SDK 多个高危漏洞预警

2021 年 8 月 18 日，网络安全威胁和漏洞信息共享平台发布预警，国外研究人员公开披露了多个 Realtek SDK 高危漏洞（CVE-2021-35392、CVE-2021-35393、CVE-2021-35394、CVE-2021-35395）的细节和 POC。攻击者可利用这些漏洞使设备崩溃、注入任意命令并以最高权限执行任意代码。该漏洞影响范围较广，且危害较大，目前厂商已修复漏洞，建议受影响用户及时更新至安全版本，并做好资产自查及预防工作，以免遭受黑客攻击。Realtek SDK 是瑞昱（Realtek）公司的一套 SDK 开发包。

Windows Print Spooler 远程代码执行 0day 漏洞安全风险通告

2021 年 8 月 12 日，奇安信 CERT 监测到微软紧急发布 Windows Print Spooler 远程代码执行漏洞（CVE-2021-36958）通告。该漏洞细节已公开披露，当 Windows Print Spooler 服务不正确地执行特权文件操作时，存在远程执行代码漏洞。成功利用此漏洞的攻击者可以使用 SYSTEM 权限运行任意代码。截至本文发布时，微软尚未发布针对此漏洞的补丁程序。鉴于此漏洞影响较大，建议客户尽快自查，并采取处置建议中的措施以缓解此漏洞。

微软 8 月安全更新多个漏洞预警

2021 年 8 月 11 日，国家漏洞库 CNNVD 发布预警，微软官方发布了多个安全漏洞的公告，包

括 Microsoft Windows TCP/IP component 缓冲区错误漏洞（CNNVD-202108-856、CVE-2021-26424）、Microsoft Windows 代码注入漏洞（CNNVD-202108-863、CVE-2021-26432）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据、提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

Microsoft Exchange 多个远程代码执行漏洞预警

2021年8月9日，网络安全威胁和漏洞信息共享平台发布预警，有关 Microsoft Exchange 多个远程代码执行漏洞（CVE-2021-34473、CVE-2021-34523、CVE-2021-31207）的技术细节以及 POC 已在互联网上公开，攻击者可根据这些漏洞细节开发出漏洞利用代码，从而在无需身份验证的情况下组合这些漏洞在目标服务器上执行远程代码，从而接管目标服务器。微软已在7月补丁日发布这些漏洞的修复补丁，建议受影响用户及时更新漏洞补丁，做好资产自查及预防工作，以免遭受黑客攻击。

Linux eBPF 本地提权漏洞安全风险通告

2021 年 8 月 6 日，监测到有安全研究员发布了 Linux kernel eBPF 本地提权漏洞 (CVE- 2021-3490) 的漏洞细节和 POC，并在 Ubuntu 21.04上进行了演示。该漏洞是由于按位操作（AND、OR 和XOR）的 eBPF ALU32 边界跟踪没有正确更新 32 位边界而导致，利用该漏洞可触发越界读写，从而从普通权限提升到 root 权限。鉴于漏洞危害较大，建议用户及时升级版本。

Windows NTLM 中继攻击漏洞安全风险通告

2021 年 8 月 5 日，监测到微软发布了针对 Active Directory 证书服务 (AD CS) 的 NTLM 中继攻击漏洞缓解通告（ADV210003）。此漏洞允许攻击者强制域控制器向指定机器进行 NTLM 身份认证，未经身份认证的攻击者可利用此漏洞发起 NTLM 中继攻击并接管 Windows 域。目前该漏洞的细节及 POC 已公开，漏洞危害上升，强烈建议客户实施微软推送的缓解措施，以缓解该漏洞危害。

Node.js 远程代码执行漏洞 (CVE-2021-22930) 预警

2021 年 8 月 4 日，网络安全威胁和漏洞信息共享平台发布预警，Node.js 发布安全更新，修复了 Node.js 中的一个释放后使用 (Use-After-Free) 漏洞（CVE-2021-22930）。攻击者可利用该漏洞执行远程代码攻击，最终获取服务器控制权。建议受影响用户尽快更新至安全版本，并做好资产自查及预防工作，以免遭受黑客攻击。

华云信安威胁情报中心：近期需重点关注的 27 个高风险漏洞

2021 年 7 月，监测到新增漏洞 2072个。经人工研判，本月值得重点关注的漏洞共 103 个，其中高风险漏洞共 27 个，包括多个 WebLogic 远程触发漏洞、多个遭在野利用的 Windows 内核漏洞等，约一半漏洞细节和 POC 已公开或遭到在野利用。

对抗篇

国内攻防演习 7 月态势：哪些薄弱点最易被利用?



一、本月演习整体情况

本月攻防演习成果如下表。

二、本月任务目标特点

本月攻防演习和评估任务覆盖多个行业，客户存在的安全问题主要涉及互联网侧应用更新不及时、内网安全设备策略配置不当，以及人员网络安全意识不足。具体情况如下。

1、钓鱼攻击方式多样

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

2、供应链攻击途径丰富

本月任务中供应链攻击手段运用比较丰富，除了常见的第三方软件代码审计、漏洞挖掘，还根据目标业务自身特点，针对目标网络内自研产品的开发包进行恶意代码植入来完成供应链攻击。

3、业务网络缺乏纵深防护机制

目标网络及关键业务安全防护缺乏纵深防护机制。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缺乏。

4、人员网络安全意识不足

本月任务中发现各目标客户在网络安全意识方面存

本月攻防演习成果：

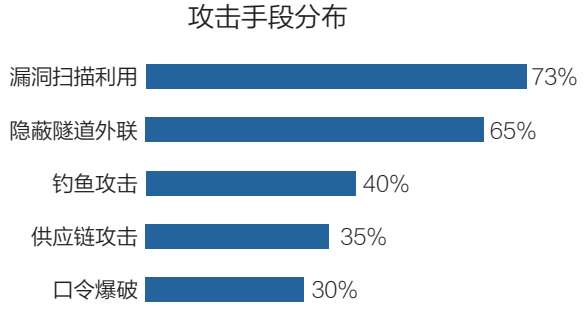
目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	15	6	15	48	5	36	72	2110

在严重不足，在弱口令、防范钓鱼攻击方面意识淡薄，为攻击队突破网络提供了可乘之机。

三、 主要攻击手段分析

基于本月实战成果分析，对目标业务突破，采用互联网侧系统漏洞利用和钓鱼攻击进行突破，内网横向拓展则以隐蔽隧道外联、内网漏洞利用、水坑攻击、仿冒认证、弱口令（口令复用）等手段为主。

使用的主要攻击手段分布如下：



1、漏洞扫描利用

本月任务中发现的漏洞主要集中在行业应用系统上，主要以 Weblogic 反序列化、Shiro 反序列化、Fastjson 反序列化、WebSphere 反序列化漏洞为主。这些漏洞大量存在主要是由于相关行业应用开发平台比较集中，应用组件多存在缺陷导致。而目标系统运维人员安全意识不足、没有形成常态化的安全运营机制则导致应用系统版本更新不及时、安全策略设置不严格。

2、隐蔽隧道外联

本月任务中因大部分目标内网无法通过外网直接访问，需要借助端口转发、隐蔽隧道技术等手段实现转发通信。尤其是对于网络功能区划分严格、核心业务内网隔离措施完善的目标，甚至需要两到三层以上通道转发才能实现对目标核心内网的稳定控制。

3、钓鱼攻击

本月任务中外网突破钓鱼手段丰富，有针对性地对客服人员、第三方服务支持或人事招聘人员开展钓鱼诱骗，通过业务咨询、业务合作及岗位应聘等途径进行诱骗。

4、供应链攻击

本月任务中采用多种途径对目标网络进行了供应链攻击，主要包括：针对某目标官网的第三方开发应用，通过特征定位搜索开源代码，对源码审计、挖掘漏洞并成功利用；针对某目标内网自研安全浏览器，分析发现该浏览器基于 Chrome 内核调用实现功能，利用 Chrome 安全机制提取相关缓存认证信息；针对某目标应用系统的开发环境，对其可调用的 PIP 工具包进行污染，植入恶意代码来完成供应链攻击。

5、口令爆破

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

四、典型攻击手段的实现案例

1、外部漏洞利用突破

（1）某目标互联网回溯管理平台系统存在 Shiro 反序列化漏洞，可通过漏洞利用获取服务器控制权限。

（2）某目标外网 e-learning 学习系统存在 Fastjson 反序列化漏洞，可通过漏洞利用获取服务器控制权限。

（3）某目标电子文档管理系统存在 Apache Solr 远程命令执行漏洞，可通过漏洞利用其突破外网。

（4）某目标外网 OA 系统存在 0day 漏洞，可通过漏洞利用远程命令执行控制 OA 服务器。

2、钓鱼突破

（1）针对某电子商务平台客户服务、第三方合作客



服业务较多的特点，以假冒客户投诉、第三方业务合作咨询等身份对相关客服人员进行钓鱼攻击，成功获取内网个人终端控制权。

（2）利用某目标单位正在招聘的时机，以应聘的名义对目标 HR 人员进行钓鱼诱骗，获取人事部门计算机控制权。

（3）针对某政务系统对外服务的特点，以相关业务报告形式对目标职能人员进行钓鱼诱骗，获取该政务系统运维人员主机控制权限。

3、供应链攻击

（1）本月任务中通过对某目标官网进行分析，利用系统特征定位服务商为 bocadmin，进一步通过 GitHub 寻找到相关代码，对代码进行审计，挖掘出未授权任意密码重置漏洞，利用此漏洞获取该目标官网后台控制权限。

（2）本月任务中发现某目标业务内网使用内部自研浏览器，经分析发现该浏览器基于 Chrome 内核调用实现功能，遂利用 Chrome 安全认证机制成功提取到目标业务人员的浏览器缓存认证信息，获取了对内网进一步拓展的关键条件。

（3）经前期信息搜集发现，某目标业务部署较多是自研应用或平台，分析发现其主要开发语言为 Python，随即对开发所需的 PIP 工具包进行污染，植入恶意代码，来完成供应链攻击。

4、内网弱口令横向拓展

（1）某目标内网 mysql 数据库服务器普遍存在弱口令，通过弱口令可控制内网 594 台数据库服务器。

（2）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 13 个域控、16 万 + 域内主机和 8 万 + 域内用户。

（3）某目标内网 vCenter 服务器存在弱口令，通过弱口令拓展控制该 vCenter 服务器，可控制内网百余台测试服务器，其中包括 OA 系统、数据库测试集群、Zabbix、动态感知、POC 链路监控系统等核心系统服务器。

政策篇

国内，《个人信息保护法》通过，我国个人信息保护有了法律“安全锁”；《关键信息基础设施安全保护条例》历经四年打磨终于发布，标志着我国网络安全保护进入了以关键信息基础设施安全保护为重点的新阶段。

国际上，美参议院通过基础设施法案，为网络安全拨款 20 亿美元；拜登总统签发改善关键基础设施控制系统网络安全备忘录，为关基设施制定网络安全绩效目标；NIST 发布《零信任架构规划指南》草案，概述了如何用风险管理框架帮助开发和实施零信任架构。

国内

《个人信息保护法》表决通过，2021 年 11 月 1 日起施行

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，自 2021 年 11 月 1 日起施行。其中明确：通过自动化决策方式向个人进行信息推送、商业营销，应提供不针对其个人特征的选项或提供便捷的拒绝方式；处理生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息，应取得个人的单独同意；对违法处理个人信息的应用程序，责令暂停或者终止提供服务。

网信办等五部门发布《汽车数据安全管理若干规定（试行）》

2021 年 8 月 20 日，网信办、发改委、工信部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》），自 2021 年 10 月 1 日起施行。《规定》倡导，汽车数据处理者在开展汽车数据处理活动中坚持“车内处理”“默认不收集”“精度范围适用”“脱敏处理”等数据处理原则，减少对汽车数据的无序收集和违规滥用。

李克强签署国务院令，公布《关键信息基础设施安全保护条例》

2021 年 8 月 17 日，国务院总理李克强签署国务院令，公布《关键信息基础设施安全保护条例》，自 2021 年 9 月 1 日起施行。《条例》明确了关键信息基础设施范围和保护工作原则目标；明确了监督管理体制；完善了关键信息基础设施认定机制；明确运营者责任义务；明确了保障和促进措施；明确了法律责任。《条例》的公布，标志着我国网络安全保护进入了以关键信息基础设施安全保护为重点的新阶段。

工信部印发《关于加强智能网联汽车生产企业及产品准入管理的意见》

2021 年 8 月 12 日，工信部印发《关于加强智能网联汽车生产企业及产品准入管理的意见》，要求加强汽车数据安全、网络安全、软件升级、功能安全和预期功能安全管理，保证产品质量和生产一致性，推动智能网联汽车产业高质量发展。《意见》从加强数据和网络安全管理、规范软件在线升级、加强产品管理、保障措施等方面提出了 11 项具体意见。

《党委（党组）网络安全工作责任制实施办法》公开

2021年8月4日，《人民日报》头版发布《中国共产党党内法规体系》一文。同时，《中国共产党党内法规体系》公开出版发行，收录了《党委（党组）网络安全工作责任制实施办法》，这是该文件首度解密公开。《实施办法》提出，各级党委（党组）领导班子主要负责人是本地区本部门网络安全工作的第一责任人。《实施办法》作为《中国共产党党内法规体系》唯一收录的网络安全领域的党内法规，它的公开发布对厘清网络安全责任、落实保障措施、推动网信事业发展将产生巨大影响。此前在2017年8月15日，中共中央印发《党委（党组）网络安全工作责任制实施办法》。

国际

美参议院通过基础设施法案，为网络安全拨款20亿美元

据ITPro 8月12日消息，美国参议院8月10日通过拨款总额过万亿美元的《基础设施投资和就业法案》。参议院多数党领袖查克·舒默表示，该法案是“数十年来最强劲的基础设施注入资金”，将振兴美国的基础设施。该法案为网络安全拨款约20亿美元，其中约10亿美元将用于设立州和地方政府网络安全拨款；3.5亿美元用于加强电网安全；2.5亿美元用于加强能源网络安全；1.57亿美元用于国土安全部科技署开展网络安全研究；1亿美元用于网络响应和恢复基金等。

NIST发布《零信任架构规划指南》草案

2021年8月4日，美国国家标准与技术研究院（NIST）发布了《零信任架构规划：管理员入门指南（草案）》白皮书，本白皮书提供了NIST风险管理框架的顶层概述及其如何帮助开发和实施零信任架构。NIST认为，零信任是在规划和实施企业体系架构时使用的一系列网络安全原则。零信任架构要成功地改善企业安全态势，需要来自企业各利益相关方的输入和合作，但由于其中一些利益相关方可能不熟悉风险分析和管理，风险管理框架为安全规划人员和系统操作人员提供了一套通用的概念和任务。



美国海岸警卫队发布2021版《网络战略展望》

据Defense Daily 8月3日消息，美国海岸警卫队发布《网络战略展望》，这是其2015年发布初版以来的首次更新。该文件重申将网络空间确立为海岸警卫队的新作战领域，将采取行动保护海上运输系统免受在网络空间和通过网络空间传递的威胁，以及追究那些通过攻击美国的网络、操作或海上运输系统对美国造成伤害人员的责任。该文件共八个部分，简介、海岸警卫队和网络空间行动、网络空间中的海上运输系统、行动1- 保卫和运行企业任务平台、行动2- 保护海上运输系统、行动3- 通过网络空间开展行动、关键赋能者和结论。

拜登总统签发改善关键基础设施控制系统网络安全备忘录

据美国白宫7月28日消息，美国总统拜登签署了改善关键基础设施控制系统网络安全国家安全备忘录。该备忘录通过指导国土安全部和商务部与其他机构一起合作，制定网络安全绩效目标，设定一个清晰、易于理解的安全基线，向改善关键基础设施网络安全迈出了关键的一步。近半年来，美国白宫和相关部委发布了多项网络安全政策文件。

极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

极牛网旗下面向网络安全工程师的社群平台，汇聚行业中网安工程师的知识和社交平台，围绕『技术』『管理』和『圈子』三个核心能力，将前沿的技术内容、技术管理成长感悟、技术圈子社群平台等向优质的网安工程师开放，每月定期组织社群会员线下活动，强调内容分享的体系化和活动内容的多样性，为中国网络安全工程师打造专属的全方位综合赋能的社群平台。

技术

聚焦前沿技术、热点技术、难点技术，提升网安在企业架构中的决策能力和迭代能力。

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

建立精准的技术方向圈子，针对不同的职业发展阶段，组成技术成长小组一起结伴同行。

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

网安行业投融资大爆发：2021 年上半年已超去年全年

一系列震惊世界的网络攻击事件正在加速对网络安全初创公司的投资。

2021 年刚刚过去七个月，投资者已经向网络安全公司投入了 122 亿美元，这比 2020 年全年还要多 20 亿美元以上。

业内人士认为，今年全球网络安全领域的投资总额，将达到前所未有的 150 亿至 200 亿美元之间。

由于勒索软件攻击和国家支持的黑客都十分活跃，导致油气管道停运，医院和零售中断，供应链安全危及国家情报机构。这些威胁都利好网络安全初创公司。投资者认为，安全公司将比以往拥有更广阔的市场前景和国家使命。

行业资深专家 Dave DeWalt 表示：“网络安全发展的超级周期已经到来，网络威胁空前严峻，疫情和监管倒逼企业安全支出大幅增长，行业投融资规模也远超往年，这是头一次威胁周期、客户周期、投资周期几乎同时出现。”

Dave DeWalt 曾先后担任 McAfee 和 FireEye 首席执行官十余年，目前在多家明星安全公司担任董事，并正在运营一家刚刚募得 7.5 亿美元的网络安全专业基金。



20 年未见安全公司估值如此快速上升

自 2019 年开始，网络安全领域的投资增速就超过风投行业的整体增速。近期出现的激增则是由于一系列备受瞩目的网络攻击的发生，包括针对美国油气运输管道 Colonial Pipeline、软件制造商 Kaseya、肉制品加工商 JBS 等公司的攻击。

美国总统拜登和俄罗斯总统普京也在会谈中深入探讨了有关网络攻击的问题。

日益增长的网络攻击引发了公司和政府的担忧，这会促进网络安全产品的销售。Gartner 预测，今年全球信息安全和相关服务支出将达到 1500 亿美元，相比去年增长 12%。

Dave DeWalt 说，据他担任董事的多家安全公司了解，目前接触的财富 500 强企业，全部都在为正在发生的事件而大幅增加网络安全支出。

线上借贷平台 LendingTree 公司的信息安全经理 John Turner 表示，原来安全团队在艰苦的条件下艰难地保护每一分钱。现在，形势逆转了。公司高管开始主动询问：“我们是否受到了合适的防护，安全团队还需要什么？”

所有这些都推动了网络安全公司的业务发展。根据 PitchBook 的数据，今年融资的网络安全公司的平均估值，从 2020 年的 2.218 亿美元增长到 2021 年的 5.241 亿美元。

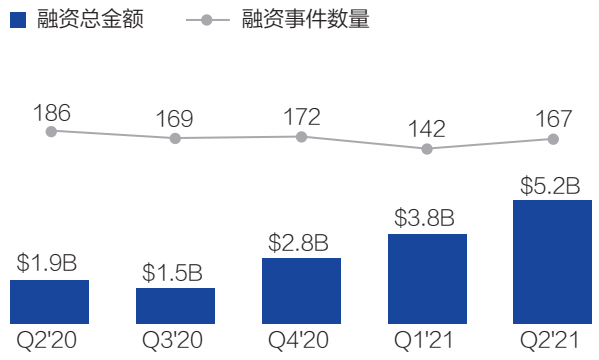
Greylock Partners 的投资人 Asheem Chandna 曾成功投资过 Palo Alto Networks 等安全公司。他表示，“作为风险投资人，二十年来都没有见过公司估值上升的如此之快”。

2021 年网络安全投资将达去年 2 倍

2020 年是网络安全投资创纪录的一年，全球网络安全行业投资超过了 78 亿美元。但 2021 年的网络安全投资总额有可能将达到 2020 年的 2 倍以上。

业内人士表示，几乎可以肯定的是，2021 年全球网络安全领域投资总额将至少达到 150 亿美元；如果热度毫不衰退，200 亿美元也将不在话下。

全球网络安全融资数量及金额统计



数据：CrunchBase

据投融资数据平台 CrunchBase 统计，今年上半年，网络安全行业共完成 309 笔交易，总融资高达 90 亿美元，是去年同期 44 亿美元融资金额的 2 倍以上。

单是今年第二季度，网安行业的融资数字就达到 52 亿美元，去年同期则不到 20 亿美元。

截至 2021 年 7 月底，投资者已经向网络安全公司投入了 122 亿美元，这比 2020 年全年还要多 20 亿美元以上。实际上根据统计，自 2011 年以来，对网络安全公司的投资已增长了 9 倍以上。

大手笔并购和 IPO 层出不穷

除了融资，安全初创公司也被大手笔收购或者筹备 IPO。

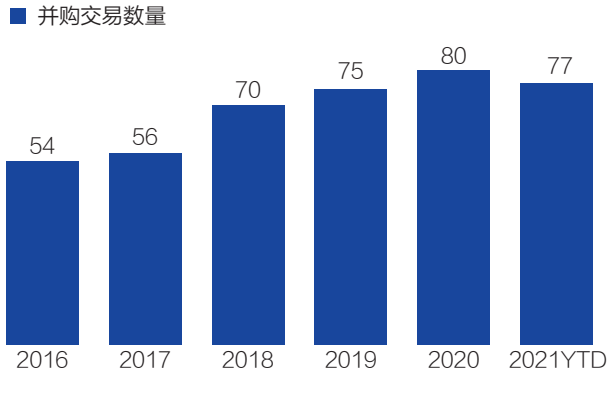
2021 年 6 月，端点安全公司 SentinelOne 成功上市，以 90 亿美元估值募资 12 亿美元，这被认为是网络安全史上规模最大的 IPO。

身份识别公司 Clear Secure、反欺诈公司 Riskified、AI 安全公司 Darktrace、安全意识培训公司 KnowBe4 等也纷纷上市，均募集了数亿美元规模的资金。

此外，还有数家募资数亿美元、专门针对网络安全行业的 SPAC 壳公司成功上市，充分展示了本行业的资本吸引力。

2021 年 4 月，私募股权巨头 Thoma Bravo 宣布以 123 亿美元的价格收购综合安全公司 Proofpoint。5 月，身份认证公司 Auth0 被 Okta 以 65 亿美元的价格收购。

全球风险投资支持的网络安全并购交易数量统计



数据：CrunchBase

根据 CrunchBase 的数据，2021 年前七个月，风险投资支持的网络安全企业并购交易数量几乎达到去年全年总数。今年已经有 77 笔交易——而去年则是创纪录的 80 笔。

云安全与身份安全是投资热点

2021 年 7 月，云安全初创公司 Netskope 以 75 亿美元估值融资 3 亿美元，这是今年网络安全领域内较大规模的融资。

过去几年，机构向云端转移。新冠疫情大大加速了数字化转型和云化。连接互联网的资产数量日益增长，攻击面也随之扩大。传统依赖边界防护的思路正在失效，这为更多的安全公司提供了机会：云安全和身份认证是新的行业热点。

云计算普及加速 Lacework、Aqua Security、OwnBackup、Axonius 等云安全公司的发展势头。

自疫情爆发以来，云安全公司已筹集了超过数十亿美元的资金。今年仅前七个月，投资者已向云安全、身份认证和隐私保护等细分领域的公司投资超过 122 亿美元。

根据 PitchBook 的数据，这一数字已经超过 2020 年的总投资额 104 亿美元，更是远远超过 2016 年的 48 亿美元的投资额。

网络安全投资咨询公司 Momentum Cyber 创始董事 Dino Boukouris 表示，除了云安全，身份与访问管理、风险与合规等细分领域在 2021 年上半年同样表现良好，在可预见的未来应该会保持强劲势头。

Thomvest Ventures 的合伙人 Umesh Padval 表示，今年下半年将重点关注云安全（典型代表如 Lacework、Wiz）、API 安全与持续上下文身份验证等技术方向。

API 安全在 2021 年二季度迎来了一波融资热潮：总部位于伦敦的 42Crunch、来自帕洛阿尔托的 Salt Security、位于科罗拉多的 ThreatX 以及来自加利福尼亚州桑尼维尔的 API 安全厂商 Cequence Security 等均宣布了新的融资。

随着许多机构宣布无限期延续远程工作优先政策，预计安全公司高速发展的势头将会一直保持下去。

中国投融资交易数量超以色列，但金额远逊

以色列国家网络局（INCD）表示，2021 年上半年，以色列网络安全公司总共融资 50 笔，筹得 34 亿美元，融资金额已占据全球总额的近四成。

从数据来看，今年有 7 家以色列企业成功跻身网安独角兽行列，全球超过三分之一的网安独角兽企业来自以色列。独角兽是指估值超过 10 亿美元的私营公司。

据《安全内参》基于公开信息梳理，2021 年 1-7 月，国内共计发生 61 起网络安全投融资事件，公开披露涉及金额超 59 亿元，约占全球总额的 10%。

2021 年 1-7 月我国网络安全初创企业投融资事件数据

	1 月	2 月	3 月	4 月	5 月	6 月	7 月
融资事件数量 / 起	6	6	12	9	7	10	11
披露融资金额 / 亿元	7.8+	2+	13.6+	7.45+	3.3+	12+	13.3+

其中，风控厂商数美科技、主机安全厂商青藤云安全、威胁检测厂商微步在线，分别以 1.35 亿美元（约 8.78 亿元）、6 亿元、5 亿元位列融资金额前三，数美科技融资后的估值接近独角兽。

国家工业信息安全发展研究中心统计数据显示，2021 年 1-7 月，国内近四成网安企业融资事件的融资额超过 1 亿元，近两成事件融资额超过 2 亿元，超亿元融资事件数量较去年同期增长约 1.2 倍。

统计数据还显示，投资机构对网络安全领域早期、中后期项目的关注度较为均衡，中后期项目占总融资事件近一半，所占比例略高于早期项目（部分项目未披露具体融资轮次）。

从上述数据可以看出，中国网安初创企业投融资的繁荣度已和全球接轨，规模上也有大幅增长，但总金额和网络强国相比还有较大差距，特别是在领军企业上，今年没有一家新晋独角兽。

以色列国家网络局经济与增长主任Roi Yarom表示，网络安全行业已成为以色列国家经济的增长引擎，同时也将提高以色列对于未知网络攻击的抵御能力。

豪赌下一个 CrowdStrike

随着网络安全企业的不断发展，投资者的心态发生变化：从平均投资多家创业公司，转向为少数公司提供巨额资金——他们的目标非常明确，豪赌其中某家能成为下一个 CrowdStrike。

但 SineWave Ventures 创始人、SentinelOne 早期投资者 Yanev Suissa 表示，目前很多融到大量资金的解决方案，仍然属于“治标不治本”的低价值产品，只能解决某些非常具体的安全问题或特定场景。

“现在市场上仍然缺乏充足的革命性技术平台，我们只看到了一大堆「还可以」的解决方案。”

但或许正如微软公司首席信息安全官 Bret Arsenault 在 RSAC 2021 演讲时指出的那样，完美不是安全的目标，改进才是。当前影响安全提升的一大原因，是对完美主义的过分追求。

其实，安全专家早就放弃寻求银弹的希望。最近热门的零信任、SASE 等创新技术不会是安全挑战的终结者，也不能取代现有边界防护手段。

在没有银弹的世界，任何的技术进步都应是我们积极把握的机会。这或许才是推动我们实现安全能力逐步提升的最现实道路。

附：2021 年网络安全重大融资事件

2021 年 1 月，云安全厂商 Lacework 获 5.25 亿美元融资，投后估值超 10 亿美元。

2021 年 3 月，云安全初创公司 Orca Security 宣布融资 2.1 亿美元，投后估值 12 亿美元。

2021 年 3 月，开发安全厂商 Snyk 宣布融资 3 亿美元，投后估值 47 亿美元。

2021 年 6 月，威胁检测厂商 Exabeam 获 2 亿美元融资，投后估值 24 亿美元。

2021 年 6 月，身份验证公司 Trulioo 获得了 3.94 亿美元投资。

2021 年 6 月，数字资产安全厂商 Ledger 宣布融资 3.8 亿美元。

2021 年 6 月，无密码验证厂商 Transmit Security 宣布 A 轮融资 5.43 亿美元，投前估值 23 亿美元。

2021 年 7 月，云安全初创公司 Netskope 融资 3 亿美元。

2021 年 8 月，云数据备份公司 OwnBackup 宣布融资 2.4 亿美元，投后估值 33.5 亿美元。

极牛·产业生态

网络安全产业生态平台

极牛网络安全产业生态平台，通过产服、产孵、产投、产研四大引擎，打通技术、产品、平台能力以及B端G端场景和服务体系，构建产业核心生态圈，与合作伙伴共生共赢，助力网安产业智慧升级。



四大引擎

产服

以产业基地为载体
提供产业生态服务
助力产业发展

产孵

以产业加速器为载体
孵化优质企业
与ToB业务的合作

产投

以产业生态投资
为重要抓手
构建产业生态体系

产研

构建产学研体系
聚焦底层技术创新
全面赋能网安产业

产业生态架构

与生态伙伴一起持续加大资本 、资源 、 技术 、 能力和商机投入，助力科技创新驱动网络安全产业升级，为社会创造更大价值



网络安全实战攻防演习的五大演变

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。

攻防演习暴露十大薄弱环节

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2020年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


CTFWAR 2021
国际网络安全攻防对抗联赛
时间：2021.10.23 - 2021.10.24

九大措施应对网络攻击“七十二变”

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，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，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。

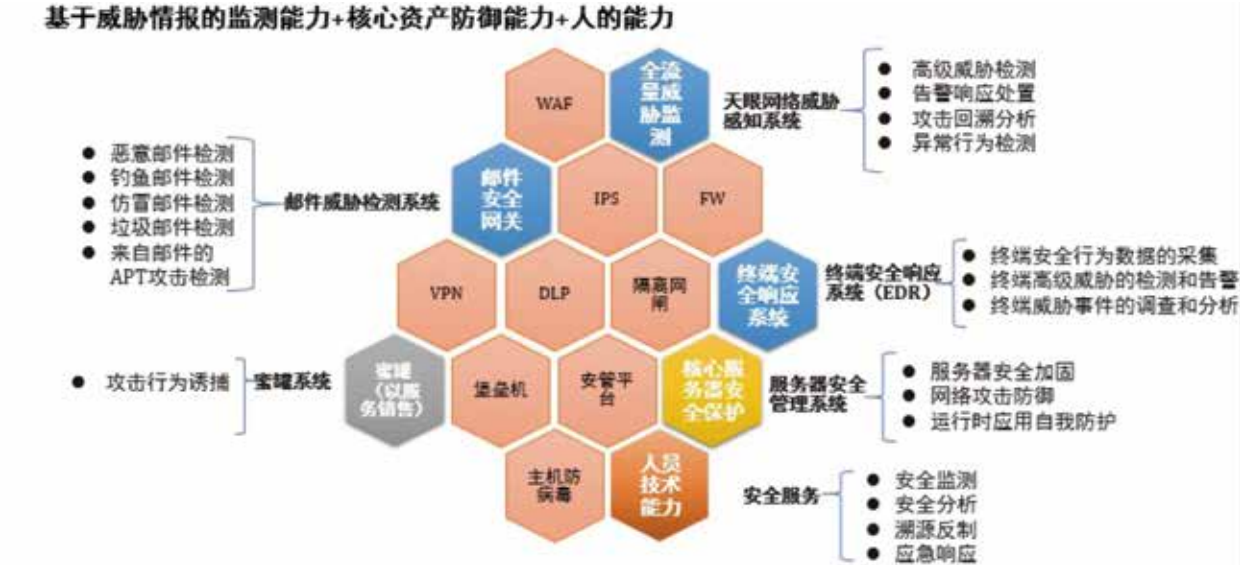
举措四

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，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，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，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。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。

“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《网安观察》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：

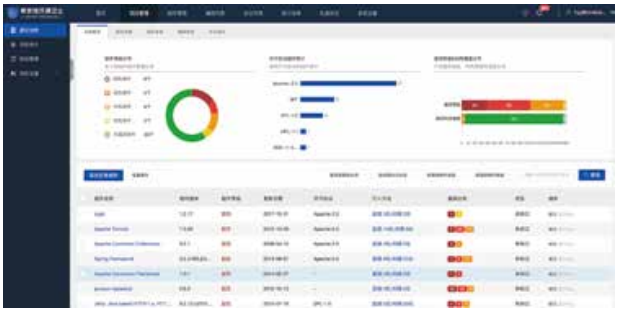
软件设计阶段：可通过奇安信开源卫士开源软件查验功能检索预使用的开源软件的版本是否存在已知漏洞和协议风险，在技术选型时，及早规避引入有漏洞的开源软件，从源头把控开源软件的风险。

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

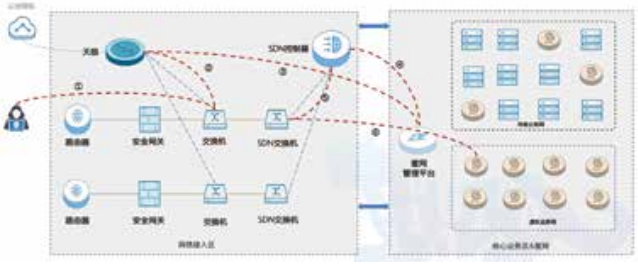
大量的误报会阻碍安全工作，过多的噪音可能导致 IT 团队忽略了潜在的真正威胁。攻击诱捕技术理论上不会产生任何误报，可以做到触碰即告警，告警即发现，减轻用户安全运维的负担。

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。

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称“华云信安”，HuaYunSec）成立于2016年，是一家深耕于网络信息安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安总部位于深圳，在上海、广州、苏州、武汉设有分支机构，公司核心团队来自腾讯、网易、阿里巴巴、思科等国际知名科技企业，具有丰富的技术积淀和管理经验。

华云信安目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安基于业内领先的网络安全解决方案、雄厚的技术实力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、零售等行业的广大用户，提供优质多元的网络信息安全解决方案、网络信息安全技术服务和基础架构实施服务。

服务实施组

华云信安安全服务团队主要由具有多年安全经验的业界专家、咨询顾问及攻防安全研究员组成，多名成员获得CISSP/CISP/COBIT/ITIL 等安全相关认证。服务团队现有数十人并在持续壮大中，凭借专业的素养、高超的技术和丰富的经验，为众多客户提供安全咨询、安全评估、安全培训、安全审计、安全检查、安全保障等服务，赢得高度赞誉和广泛认可。

攻防实验室

华云信安攻防实验室由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

安全咨询服务　安全评估服务　安全检查服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028