奇安信
新一代网络安全领军者

红队视角下的防御体系构建

奇安信安服团队
奇安信行业安全研究中心
2020.12

前　言

网络实战攻防演习，是新形势下关键信息系统网络安全保护工作的重要组成部分。演习通常是以实际运行的信息系统为保护目标，通过有监督的攻防对抗，尽可能地模拟真实的网络攻击，以此来检验信息系统的实际安全性和运维保障的实际有效性。

2016 年以来，在国家监管机构的有力推动下，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。国家有关部门组织的全国性网络实战攻防演习从 2016 年仅有几家参演单位，到 2020 年已扩展到上百家参演单位；同时各省、各市、各行业的监管机构，也都在积极地筹备和组织各自管辖范围内的实战演习。一时间，网络实战攻防演习遍地开花。

在演习规模不断扩大的同时，攻防双方的技术水平和对抗能力也在博弈中不断升级。

2016 年，网络实战攻防演习尚处于起步阶段，攻防重点大多集中于互联网入口或内网边界。

2017 年，实战攻防演习开始与重大活动的网络安全保障工作紧密结合。就演习成果来看，从互联网侧发起的直接攻击仍然普遍十分有效；而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，网络实战攻防演习开始向行业和地方深入。伴随着演习经验的不断丰富和大数据安全技术的广泛应用，防守方对攻击行为的监测、发现和溯源能力大幅增强，与之相应的，攻击队开始更多地转向精准攻击和供应链攻击等新型作战策略。

2019 年以来．网络实战攻防演习工作受到了监管部门、政企

机构和安全企业的空前重视。流量分析、EDR、蜜罐、白名单等专业监测与防护技术被防守队广泛采用。攻击难度的加大也迫使攻击队全面升级，诸如 0Day 漏洞攻击、1Day 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，在实战攻防演练中均已不再罕见，攻防演习与网络实战的水平更加接近。

如何更好地参与网络实战攻防演习？如何更好地借助实战攻防演习提升自身的安防能力？这已经成为大型政企机构运营者所关心的重要问题。

作为国内前沿的网络安全企业，奇安信集团已成为全国各类网络实战攻防演习的主力军。奇安信集团安服团队结合 220 余次实战攻防演习经验，总结编撰了这套实战攻防演习系列丛书，分别从红队视角、蓝队视角和紫队视角，来解读网络实战攻防演习的要领，以及如何结合演习提升政企机构的安防能力。

需要说明的是，实战攻防演习中的红方与蓝方对抗实际上是沿用了军事演习的概念和方法，一般来说，红蓝双方分别代表攻击方与防守方。不过，红方和蓝方的名词定义尚无严格的规定，在实际的攻防演习中，有将红队作为攻击队的、也有将蓝队作为攻击队的。在本系列丛书中，我们依据国内最新的相关工作实践要求，统一将攻击队命名为蓝队，将防守队命名为红队，而紫队则代表组织演习的机构。

《蓝队视角下的防御体系突破》是本系列丛书的第一册。本册希望通过归纳总结蓝队常用的攻击策略和攻击战术，帮助政企机构理解攻方思维，以便提升演习水平，构筑更有效的安全防御体系。正所谓“知己知彼，百战不殆”。

《红队视角下的防御体系构建》是本系列丛书的第二册。本

册希望通过归纳总结红队防御的四个阶段、应对攻击的常用策略，以及建立实战化的安全体系的基本方法，帮助政企机构查找薄弱环节，更好地提升演习水平，构筑更有效的安全防御体系。

《紫队视角下的实战攻防演习组织》是本系列丛书的第三册。本册重点介绍实战环境下的紫队工作，提出如何组织一场有效的实战攻防演习、如何组织演习过程中的应急演练、如何组织对无法开展实战演习的关基设施的沙盘推演。

目　　录

第一章 什么是红队

红队，在本书中是指网络实战攻防演习中的防守一方。

红队一般是以参演单位现有的网络安全防护体系为基础，在实战攻防演习期间组建的防守队伍。红队的主要工作包括演习前安全检查、整改与加固，演习期间进行网络安全监测、预警、分析、验证、处置，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等。

实战攻防演习时，红队通常会在日常安全运维工作的基础上，以实战思维进一步加强安全防护措施，包括提升管理组织规格、扩大威胁监控范围、完善监测与防护手段、增加安全分析频率、提高应急响应速度、增强溯源反制能力、建立情报收集利用机制等，提升整体防守能力。

需要特别说明的是：红队并不仅仅由实战演习中目标系统运营单位一家独立承担，而是由目标系统运营单位、攻防专家、安全厂商、软件开发商、网络运维队伍、云提供商等多方组成的防守队伍。组成红队的各个团队在演习中的角色与分工情况如下。

目标系统运营单位：负责红队整体的指挥、组织和协调。

安全运营团队：负责整体防护和攻击监控工作。

攻防专家：负责对安全监控中发现的可疑攻击进行分析研判，指导安全运营团队、软件开发商等相关部门进行漏洞整改等一系列工作。

安全厂商：负责对自身产品的可用性、可靠性和防护监控策略是否合理进行调整。

软件开发商：负责对自身系统安全加固、监控和配合攻防专家对发现的安全问题进行整改。

网络运维队伍：负责配合安全专家对网络架构安全、出口整体优化、网络监控、溯源等工作。

云提供商（如有）：负责对自身云系统安全加固，以及对云上系统的安全性进行监控，同时协助攻防专家对发现的问题进行整改。

其他：某些情况下还会有其他组成人员，需要根据实际情况具体分配工作。

特别强调，作为红队，了解对手（蓝队）的情况非常重要，正所谓知彼才能知己，从攻击者角度出发，了解攻击者的思路与打法，了解攻击者思维，并结合本单位实际网络环境、运营管理情况，制定相应的技术防御和响应机制，才能在防守过程中争取到更多的主动权。

第二章 红队演变趋势

2016 年和 2017 年，由于监管单位的推动，部分单位开始逐步参与监管单位组织的实战攻防演习，这个阶段各单位主要是作为防守方参加演习。到了 2018 年和 2019 年，实战攻防演习不论是从单场演习的参演单位数量、攻击队伍数量，还是攻守双方的技术能力等方面都迅速增强。实战攻防演习已经成为公认的检验各单位网络安全建设水平和安全防护能力的重要手段，各单位也从以往单纯的参与监管单位组织的演习，逐渐演变成自行组织内部演习或联合组织行业演习。

进入 2020 年，随着实战攻防演习中真刀实枪的不断对抗和磨砺，攻守双方在相互较量中都取得了快速发展和进步，迫于攻击队技战法迅速发展带来的压力，防守方也发生了很大的变化。

1） 防守重心扩大

2020 年之前的实战攻防演习，主要是以攻陷靶标系统为目标，达到发现防守队安全建设和防守短板，提升各单位安全意识的目的。攻击队的主要得分是拿下靶标系统和路径中的关键集权系统、服务器等权限，非靶标系统得分很少。因此，防守队的防守重心往往会聚焦到靶标系统及相关路径资产上。

对于大部分参加过实战攻防演习的单位来说，对于自身的安全问题和短板已经有了充分认识，也都开展了安全建设整改工作。对于这些单位，急需的是通过实战攻防演习检验更多重要系统的安全性，发现更全面的安全风险。因此，2020 年开始，不论是监管单位还是单位自身，在组织攻防演习时，都会逐渐降低演习中靶标系统的权重，鼓励攻击更多的单位、系统，发现更多的问题

和风险。同样，防守队的防守重心也就从靶标系统为主，扩大到所有重要业务系统、所有重要设备和资产、所有的相关上下级单位。

2） 持续加强监测防护手段

随着近几年攻防技术的快速发展，实战攻防演习中各种攻击手段层出不穷、花样百出，各单位在演习中切实感受到了攻击队带来的严重威胁以及防守的巨大压力，防守队的监测和防护体系面临巨大挑战。防守队对于在攻防对抗中确实能够发挥重大作用的安全产品趋之若鹜，投入大量资金来采购和部署。

2018-2019 年，除了传统产品外，全流量威胁监测类产品在攻防对抗中证明了自己，获得了各单位的青睐，到了 2020 年，主机威胁检测、蜜罐以及威胁情报等产品服务迅速成熟并在演习中证明了对主流攻击的监测和防护能力，防守队开始大规模的部署使用。除此之外，钓鱼攻击、供应链攻击等还没有有效的防护产品，不过随着在实战中快速打磨，相应产品也会迅速成熟和广泛使用。

3） 被动防守到正面对抗

要说变化，2020 年防守队最大的变化应该是从被动挨打迅速转变为正面对抗、择机反制。之前，演习中的大部分防守队发现攻击后基本就是封锁 IP、下线系统、修复漏洞，之后接着等待下一轮攻击。敌在暗、我在明，只能被动挨打。2020 年开始，大量的防守队加强了溯源和反制能力，跟攻击队展开了正面对抗，也取得了很多战果。

要具备正面对抗能力，需要重点加强以下几个方面。

快速响应。实战中讲究兵贵神速，在发现攻击时，只有最快速地确认攻击方式、定位受害主机、采取处置措施，才能够有效阻止攻击，并为下一步的溯源和反制争取时间。

准确溯源。俗话说知己知彼百战百胜，要想和攻击队正面对抗，首先要找到攻击队的位置，并想办法获取攻击队的足够信息，才能有针对性的制定反制策略开展反击。

精准反制。反制其实就是防守队发起的攻击。防守队在准确溯源的基础上，需要攻击经验丰富的人员才能够有效精确的实施反制。当然，也有些单位会利用蜜罐等产品埋好陷阱，等着攻击队跳进来之后，利用陷阱中的木马等快速攻陷攻击队系统。

第三章 红队四步走——防守的四个阶段

在实战环境下的防护工作，无论是面对常态化的一般网络攻击，还是面对有组织、有规模的高级攻击，对于防护单位而言，都是对其网络安全防御体系的直接挑战。在实战环境中，红队需要按照备战、临战、实战和战后三个阶段来开展安全防护工作。

一、 备战阶段——不打无准备之仗

在实战攻防工作开始之前，首先应当充分地了解自身安全防护状况与存在的不足，从管理组织架构、技术防护措施、安全运维处置等各方面能进行安全评估，确定自身的安全防护能力和工作协作默契程度，为后续工作提供能力支撑。这就是备战阶段的主要工作。

在实战攻防环境中，我们往往会面临技术、管理和运营等多方面限制。技术方面：基础能力薄弱、安全策略不当和安全措施不完善、产品部署位置不当、防护产品自身安全有问题、监控手段不熟悉、监控手段单一等问题普遍存在；管理方面：制度缺失，职责不明，应急响应机制不完善等问题也很常见；运营方面：资产梳理不清晰、业务架构不了解、漏洞整改不彻底、安全监测分析与处置能力不足等问题随处可见。这些不足往往会导致整体防护能力存在短板，对安全事件的监测、预警、分析和处置效率低下。

针对上述情况，红队在演习之前，需要从以下几个方面进行准备与改进。

1） 技术方面

为了及时发现安全隐患和薄弱环节，需要有针对性地开展自查工作，并进行安全整改加固，内容包括系统资产梳理、应用组件梳理、交互协议梳理、安全基线检查、网络安全策略检查、Web安全检测、关键网络安全风险检查、安全措施梳理和完善、公开情报收集、应急预案完善与演练等。

为了检验监控措施的有效性，还需对安全产品自身的安全性、部署位置、覆盖面进行评估；为了更快的发现问题，尽量部署全流量威胁监测、网络分析系统、蜜罐、主机监测等安全防护设备，提高监控工作的有效性、时效性、准确性；监测人员还需对安全产品熟练掌握、优化安全产品规则。

2） 管理方面

一是建立合理的安全组织架构，明确工作职责，建立具体的工作小组，同时结合工作小组的责任和内容，有针对性地制定工作计划、技术方案、相关方协同机制及工作内容，责任到人、明确到位，按照工作实施计划进行进度和质量把控，确保管理工作落实到位，技术工作有效执行。

二是建立有效的工作沟通机制，通过安全可信的即时通讯工具建立实战工作指挥群，及时发布工作通知，共享信息数据，了解工作情况，实现快速、有效的工作沟通和信息传递。

3） 运营方面

成立防护工作组并明确工作职责，责任到人，开展并落实技术检查、整改和安全监测、预警、分析、验证和处置等运营工作，加强安全技术防护能力。完善安全监测、预警和分析措施，增强监测手段多元化，建立完善的安全事件应急处置机构和可落地的流程机制，提高事件的处置效率。

同时，所有的防护工作包括预警、分析、验证、处置和后续的整改加固都必须以监测发现安全威胁、漏洞隐患为前提才能开展。其中，全流量安全威胁监测分析系统是防护工作的重要关键节点，并以此为核心，有效地开展相关防护工作。

二、 临战阶段——战前动员鼓舞士气

经历了备战阶段的查缺补漏、城防加固等工作，安全防护能力在技术方面、管理方面和运营方面上都有了较大的提升。为了能更多的协同配合，高效的应对实战阶段的攻击，减少分析处置事件的时间，提高防守的效果，还需要做好临战阶段的动员工作。

做好临战阶段的工作建议从三个方面开展。

1） 召开战前动员会

战前动员会主要进行三部分的工作：一是实战演习开始前，通过召开现场战前动员会的形式，进行战前动员，统一思想，统一战术、提高斗志，达成共识。二是强调防护工作中注意的事项，攻击手段多种多样，为防止防守人员被攻击利用，要严格遵守记录红线、做到令行禁止。三是提高大家的攻防意识，对攻击过程进行剖析，对常见的攻击手段部署针对性的防守要点，做到有的放矢。

2） 贯彻工作流程

贯彻工作流程的目的一是对参与防守工作的人员进行任务分工，说明工作职责、各司其职。二是固化每日工作流程、各岗位协同配合，做好攻击事件前期的监测、中期的研判和后期的处置工作。三是贯彻制定的工作排班计划、交接班要求等。通过工作流程做到防守工作有序有效，提升防守的效果。

3） 组织战术培训

战术培训会主要工作内容有两项：一是由安全专家分享其他单位的网络安全实战攻防演练相关经验，协助防守队制定不同攻击场景的防守战术。二是安全专家对演练评分规则的详细解读，提高参演人员对演练的认知。

三、 实战阶段——全面监测及时处置

攻守双方在实战阶段正式展开全面对抗。防护方须依据备战明确的组织和职责，集中精力和兵力，做到监测及时、分析准确、处置高效，力求系统不破，数据不失。

在实战阶段，从技术角度总结应重点做好以下四点。

1） 全面开展安全监测预警

实战阶段监测人员需具备基本的安全数据分析能力，根据监测数据，情报信息能基本判断攻击有效性，如存疑应立即协同专业分析人员协助分析，确保监控可以实时发现，不漏报，为处置工作提供准确信息，同时监测工作应覆盖整个攻击队攻击时间。

2） 全局性分析研判工作

在实战防护中，分析研判应作为核心环节，分析研判人员要具备攻防技术能力，熟悉网络和业务。分析研判人员作为整个防护工作的大脑，应充分发挥专家和指挥棒的作用。向前，对监测人员发现的攻击预警、威胁情报进行分析确认，向后，指导协助事件处置人员对确认的攻击进行处置。

3） 提高事件处置效率效果

确定攻击时间成功后，最重要的是在最短时间内采取技术手

段遏制攻击、防止蔓延。事件处置环节，应联合网络、主机、应用和安全等多个岗位人员协同处置。

4） 追踪溯源，全面反制

在发现攻击事件后，防守队伍可根据安全防护设备、安全监测设备产生的告警信息、样本信息等，结合各种情报系统追踪溯源。条件允许时，可通过部署诱捕系统反制攻击队攻击终端，做到追踪溯源、防守反制。

四、 战后整顿——实战之后的改进

演习的结束也是防护工作改进的开始。在实战工作完成后应进行充分、全面复盘分析，总结经验、教训。有两方面工作需要开展。

一是通过复盘会找出攻防演习备战阶段、临战阶段、实战阶段中的工作方案、组织管理、工作启动会、系统资产梳理、安全自查及优化、基础安全监测与防护设备的部署、安全意识、应急预案及演练、注意事项、队伍协同、情报共享和使用等过程还存在哪些纰漏和不足，输出技术和管理两方面问题整改措施计划。同时，各单位还需立即总结攻防演习防守策略，如情报技术、反制战术、防守作战指挥策略等，为演习队伍在下一次保障提供防守技术指导。

二是网络攻防演练活动不是一次性保障活动，其最终目的是单位通过演习发现网络安全建设存在的不足，改进和提升整体安全防御能力，通过相对独立的安全运营思路，以数据为中心建立整体网络安全防护体系，进而发挥出最有效的安全能力。因此单位通过网络攻防演练积累的经验，沿用演习期间形成的安全运营

机制、安全监测技术和应急响应策略等，在日常安全工作中提供持续安全运营能力，使网络安全防护措施持续发挥成效，进而真实有效地提升安全防护的能力。同时，单位还需加快整改演习发现的网络安全体系建设的不足，以替代演习后保障队伍力量缩减，而导致的整体安全防御降低的能力。

最后，单位参与和自我组织网络攻防演练活动，充分积累演练活动经验，锻炼安全保障队伍，不断完善整体网络安全体系和持续提高安全运营能力。

第四章 红队应对攻击的常用策略

知己知彼，百战不殆。政企安全部门只有在多次经历实战攻防的洗礼，通过实战对攻击队的攻击手法不断深入了解，才能不断发现自身安全防护能力的缺失，防护手段应随着攻击手段的变化升级而进行相应的改变和提升，将是未来的主流防护思想。

攻击者一般会在前期搜集情报，寻找突破口、建立突破据点；中期横向移动打内网，尽可能多地控制服务器或直接打击目标系统；后期会删日志、清工具、写后门、建立持久控制权限。针对攻击队的常用套路，红队应对攻击的常用策略可总结为收缩战线、纵深防御、守护核心、协同作战、主动防御、应急处突和溯源反制等。

一、 收缩战线：缩小攻击暴露面

攻击队首先会通过各种渠道收集目标单位的各种信息，收集的情报越详细，攻击则会越隐蔽，越快速。此外，攻击队往往不会正面攻击防护较好的系统，而是找一些可能连防守者自己都不知道的薄弱环节下手。这就要求防守者一定要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。哪方面考虑不到位、哪方面往往就是被攻陷的点。互联网暴露面越多，越容易被攻击队“声东击西”，最终导致防守者顾此失彼，眼看着被攻击却无能为力。结合多年的防守经验，可从如下几方面收敛暴露面。

1） 敏感信息收集

攻击队会采用社工、工具等多种技术手段，对目标单位可能暴露在互联网上的敏感信息进行搜集，为后期攻击做充分准备。防守队除了定期对全员进行安全意识培训，不准将带有敏感信息的文件上传至公共信息平台外，针对漏网之鱼还可以通过定期开展敏感信息泄露搜集服务，能够及时发现在互联网上已暴露的本单位敏感信息，提前采取应对措施，降低本单位敏感信息暴露的风险，增加攻击队搜集敏感信息的时间成本，为后续攻击抬高难度。

2） 攻击路径梳理

知晓攻击队有可能从哪些地方攻击进来，对防守力量如何部署起关键作用。由于政企机构的网络不断变化、系统不断增加，往往会增加新的系统和产生新的网络边界。防守队一定要定期梳理没每个业务系统的网络访问路径，包括对互联网开放的系统、内部访问系统（含测试系统），尤其是内部系统全国联网的单位更要注重此项梳理工作。

3） 互联网攻击面收敛

一些系统维护者为了方便，往往会把维护的后台、测试系统和高危端口私自开放在互联网上，方便维护的同时也方便了攻击队。攻击队最喜欢攻击的 Web 服务就是网站后台，以及安全状况比较差的测试系统。红队可通过开展互联网资产发现服务，对本单位开放在互联网上的管理后台、测试系统、无人维护的僵尸系统（含域名）、拟下线未下线的系统、高危服务端口、疏漏的未纳入防护范围的互联网开放系统以及其他重要资产信息（中间件、数据库等）进行发现和梳理，提前进行整改处理，不断降低互联网侧攻击入手的暴露。

4） 外部接入网络梳理

如果正面攻击不成，攻击队往往会选择攻击供应商、下级单位、业务合作单位等与目标单位有业务连接的其他单位，通过这些单位直接绕到目标系统内网。防守队应对这些外部的接入网络进行梳理，尤其是未经过安全防护设备就直接连进来的单位，应先连接防护设备，再接入内网。防守队还应建立起本单位内部网络与其他单位进行对接的联络沟通机制，发现从其他单位过来的网络行为异常时，能及时反馈到其他单位，协同排查，尽快查明原因，以便后续协同处置。

5） 隐蔽入口梳理

由于 API 接口、VPN、WiFi 这些入口往往会被安全人员忽略，这往往是攻击队最喜欢突破口，一旦搞定则畅通无阻。安全人员一定要梳理 Web 服务的 API 隐藏接口、不用的 VPN、WiFi 账号等，便于重点防守。

二、 纵深防御：立体防渗透

收缩战线工作完成后，针对实战攻击，防守队应对自身安全状态开展 全面体检，此时可结合战争中的纵深防御理论来审视当前网络安全防护能力。从互联网端防护、内外部访问控制（安全域间甚至每台机器之间）、主机层防护、供应链安全甚至物理层近源攻击的防护，都要考虑进去。通过层层防护，尽量拖慢攻击队扩大战果的时间，将损失降至最小。

1） 资产动态梳理

清晰地信息资产是防守工作的基石，对整个防守工作是否顺利开展起决定作用。防守队应该通过开展资产梳理工作，形成信

息资产列表，至少包括单位环境中所有的业务系统、框架结构、IP 地址（公网、内网）、数据库、应用组件、网路设备、安全设备、归属信息、业务系统接口调用信息等，结合收缩战线工作的成果，最终形成准确清晰地资产列表，并定期动态梳理，不断更新，确保资产信息的准确性，为正式防守工作奠定基础。

2） 互联网端防护

互联网作为防护单位最外部的接口，是重点防护区域。互联网端的防护工作可通过接入第三方云防护平台、部署网络安全防护设备和进行攻击检测两方面开展。需部署的网络安全防护设备包括：下一代防火墙、防病毒网关、全流量分析设备、防垃圾邮件网关、WAF、IPS 等。攻击检测方面，如果有条件，可以事先对互联网系统进行一次完整的渗透测试，检测互联网系统安全状况，查找存在的漏洞。

3） 访问策略梳理

访问控制策略的严格与否，与防守工作至关重要。从实战经验来看，严格的访问控制策略，对攻击队都能产生极大地阻碍。防守队应通过访问控制策略梳理工作，重新厘清不同安全域的访问策略，包括互联网边界、业务系统（含主机）之间、办公环境、运维环境、集权系统的访问以及内部与外部单位对接访问、无线网络策略等访问控制措施。

防守队应按照“最小原则”，只给必须使用的用户开放访问权限。按此原则梳理访问控制策略，禁止私自开放服务或者内部全通情况出现。这样，无论是阻止攻击队撕破边界打点，还是增加进入内部后开展横向渗透的难度，都是非常简单有效的手段。通过严格的访问控制措施尽可能地为攻击队制造障碍。

4） 主机加固防护

当攻击队从突破点进入内网后，首先做的就是攻击同网段主机。主机防护强度直接决定了攻击队内网攻击成果的大小。防守队应从以下几个方面对主机进行防护：对主机进行漏洞扫描，基线加固；最小化软件安装，关闭不必要的服务；杜绝主机弱口令，结合堡垒机开启双因子认证登录；高危漏洞必须打补丁（包括装在系统上的软件高危漏洞）；开启日志审计功能。部署主机防护软件对服务进程、重要文件等进行监控，条件允许的情况下，还可开启防护软件的“软蜜罐”功能，进行攻击行为诱捕。

5） 供应链安全

攻击队擅长对各行业中广泛使用的软件、框架或设备进行研究储备，发现其中的安全漏洞，在攻防对抗中进行有的放矢，突破防守队网络边界，甚至拿下目标系统权限。

政企机构在安全运营工作中，应重视与供应链厂商建立安全应对机制，要求供应链厂商建立起自身网络环境（如搭建带有客户业务的测试环境，还对互联网提供开放）、产品的安全保障机制（包括源码、管理工具、技术文档、漏洞补丁等方面的管理），一旦暴露出安全问题，应及时给政企机构提供修复方案或处置措施。

同时，供应链厂商也应建立内部情报渠道，提高产品的安全性，为政企机构提供更可靠，更安全的产品和服务。

三、 守护核心：找到关键点

正式防守工作中，根据系统的重要性划分出防守工作重点，找到关键点，集中力量进行防守。根据实战攻防经验，核心关键

点一般包括：靶标系统、集权类系统、具有重要数据的业务系统等，在防守前应针对这些重点系统再次进行梳理和整改，梳理的越细越好。必要情况下对这些系统进行单独的评估，充分检验重点核心系统的安全性。同时在正式防守工作，对重点系统的流量、日志进行实时监控和分析。

1） 靶标系统

靶标系统是实战中攻防双方关注的焦点，靶标系统失陷，则意味着防守队的出局。防守队在靶标系统的选择与防护中应更具有针对性。首先靶标系统应经过多次安全测试，自身安全有保障；其次应梳理清与靶标系统有互联的网络，重新进行网络策略梳理，按照最小原则进行访问；最后靶标系统应部署在内部网络中，尽可能避免直接对互联网开放。条件允许的情况下，还可以对靶标系统主机部署安全防护系统，对靶标系统主机进行白名单限制，在防守中，可实时监测靶标系统的安全状态。

2） 集权系统

集权系统一般包括单位自建的云管理平台、核心网络设备、堡垒机、SOC 平台、VPN 等，它们是攻击队最喜欢打的内部系统，一旦被拿下，则集权系统所控制的主机可同样视为已被拿下，杀伤力巨大。

集权系统是内部防护的重中之重。防守队一般可从以下几个方面做好防护：集权系统的主机安全、集权系统已知漏洞加固或打补丁、集权系统的弱口令、集权系统访问控制、集权系统配置安全以及集权系统安全测试等。

3） 重要业务系统

重要业务系统如果被攻击队攻破，也会作为攻击重要成果的一部分，因此，在防守过程中，也应该被重点防护。针对此类系统除了常规的安全测试、软件、系统打补丁升级及安全基线加固外，还应针对此类系统加强监测，并对其业务数据进行重点防护，可通过部署数据库审计系统、DLP 系统加强对数据的安全保护。

四、 协同作战：体系化支撑

面对大规模有组织地攻击时，攻击手段会不断加速变化升级，防守队在现场人员能力无法应对攻击的情况下，还应该借助后端技术资源，相互配合协同作战，建立体系化支撑，才能有效应对防守工作中面临的各种挑战。

1） 产品应急支撑

产品的安全正常运行是防守工作顺利开展的前提。但在实际中不可避免的会出现产品故障、产品漏洞等问题，影响到防守工作。因此防守队需要会同各类产品的原厂商或供应商，建立起产品应急支撑机制，在产品出现故障、安全问题时，能够快速的得到响应和解决。

2） 安全事件应急支撑

安全事件的应急处置，一般会涉及蒸汽机构的多个不同部门人员，防守队在组件安全事件应急团队时，应充分考虑哪些人员纳入到应急支撑团队中。在实战中需要对发生的安全事件应急处置时，如果应急团队因技术能力等原因无法完成对安全事件的处置时，可考虑寻求其他技术支撑单位的帮助，来弥补本单位应急处置能力的不足。

3） 情报支撑

随着攻防演练向现代化，地区化发现，攻击手段的日益丰富，0Day、NDay 漏洞、钓鱼、社工、近源攻击的频繁使用以及攻击队信息搜集能力的大大提高，攻击队已发展成为集团军作战模式。

所以，在实战阶段，仅凭一个单位的防守力量可能无法真正的防护住攻击队伍的狂轰滥炸。在各自的防护能力之外，各个单位防守队伍需建立有效的安全情报网，通过民间、同行业、厂商、国家、国际漏洞库收集情报，形成情报甄别，情报利用机制，高效快速抵御攻击队攻击。攻防演练对抗本质就是信息战，谁掌握的情报越多越准确谁就能立于不败之地。

4） 样本数据分析支撑

现场防守人员在监测中发现可疑、异常文件时，可将可疑、异常文件提交至后端样本数据分析团队，根据样本分析结果，判断攻击入侵程度，及时开展应对处置工作。

5） 追踪溯源支撑

当现场防守人员发现攻击队的入侵痕迹后，需对攻击队的行为、目的、身份等开展溯源工作时，可寻求追踪溯源团队的帮助，凭借追踪溯源团队的技术力量，分析出攻击队的攻击行为、攻击目的乃至攻击队的身份。必要情况下，还可以一起对攻击队开展反制工作，最大化扩展防守成果。

五、 主动防御：全方位监控

近两年的红蓝对抗，攻击队的手段越来越隐蔽，越来越单刀直入，通过 0Day、NDay 直取系统漏洞，直接获得系统控制权限。

红队需拥有完整的系统隔离手段，蓝队成功攻击到内网之后，

会对内网进行横向渗透。所以系统与系统之间的隔离，就显得尤为重要！红队必须清楚哪些系统之间有关联、访问控制措施是什么！在发生攻击事件后，应当立即评估受害系统范围和关联的其他系统，并及时做出应对的访问控制策略，防止内部持续的横向渗透。

任何攻击都会留下痕迹。攻击队尽量隐蔽痕迹、防止被发现。而防守者恰好相反，需要尽早发现攻击痕迹，并通过分析攻击痕迹，调整防守策略、溯源攻击路径甚至对可疑攻击源进行反制。建立全方位的安全监控体系是防守者最有力的武器，总结多年实战经验，有效的安全监控体系需在如下几方面开展。

1） 自动化的 IP 封禁

在整个红蓝对抗过程中，如果红队成员 7X24 小时不间断从安全设备的高警中识别风险，将极大地消耗监测人员、处置人员的精力。通过部署态势感知与安全设备联动，收取全网安全设备的告警信息，当态势感知系统收到安全告警信息后，根据预设规则自动下发边界封禁策略，使封禁设备能够做出及时有效的阻断和拦截，大大降低了人工的参与程度，提高整个红队的防守效率。

2） 全流量网络监控

任何攻击都要通过网络，并产生网络流量。攻击数据和正常数据肯定是不同的，通过全网络流量去捕获攻击行为是目前最有效的安全监控方式。红队或防守者通过全流量安全监控设备，结合安全人员的分析，可快速发现攻击行为，并提前做出针对性防守动作。

3） 主机监控

任何攻击最终目标是获取主机（服务器或终端）权限。通过部署合理的主机安全软件，审计命令执行过程、监控文件创建进程，及时发现恶意代码或 WebShell，并结合网络全流量监控措施，可以更清晰、准确、快速地找到攻击者的真实目标主机。

4） 日志监控

对系统和软件的日志监控同样必不可少。日志信息是帮助防守队分析攻击路径的一种有效手段。攻击队攻击成功后，打扫战场的首要任务就是删除日志，或者切断主机日志的外发，以防止防守队追踪。防守队应建立一套独立的日志分析和存储机制，重要目标系统可派专人对目标系统日志和中间件日志进行恶意行为监控分析。

5） 蜜罐诱捕

随着红蓝对抗的持续化发展，蜜罐技术是改变红队被动挨打局面的一把利器！其特点是诱导攻击队攻击伪装目标，持续消耗攻击队资源，保护真实资产，监控期间针对所有的攻击行为进行分析，可意外捕获 0Day 信息。

目前的蜜罐技术可分为 3 种：自制蜜罐、高交互蜜罐和低交互蜜罐，也可诱导攻击队下载远控程序，定位攻击队自然人身份，提升主动防御能力，让对抗工作由被动变主动。

6） 情报工作支撑

现场防守队员在防守中，一是要善于利用情报搜集工作提供的各种情报成果，根据情报内容及时对现有环境进行筛查和处置。二是对已获取的情报，请求后端资源对情报进行分析和辨别，以方便采取应对措施。

六、 应急处突：完善的方案

通过近几年的红蓝对抗发展来看，红蓝对抗初期，蓝队成员通过普通攻击的方式，不使用 0Day 或其他攻击方式，就能轻松突破红队的防守阵地。

但是，红队防护体系的发展早已从只有防火墙做访问控制，到现在逐步完善了 WAF、IPS、IDS、EDR 等多种防护设备，使红队无法突破，从而逼迫红队成员通过使用 0Day、NDay、现场社工、钓鱼等多种方式入侵红队目标，呈无法预估的特点。

所以应急处突是近两年红蓝对抗中发展的趋势，同时也是整个红队防守水平的体现之处，不仅考验应急处置人员的技术能力，更检验多部门(单位)协同能力，所以制定应急预案应当从以下几个方面进行。

一是完善各级组织结构，如：监测组、研判组、应急处置组（网络小组、系统运维小组、应用开发小组、数据库小组)、协调组等。

二是明确各方人员，在各个组内担任的角色，如：监测组的监测人员。

三是明确各方人员，在各个组内担任的职责，如：监测组的监测人员，负责某台设备的监测，并且 7X24 小时不得离岗等。

四是明确各方设备的能力与作用，如防护类设备、流量类设备、主机检测类设备等。

五是制定可能出现的攻击成功场景，如:Web 攻击成功场景、反序列化攻击成功场景、WebShell 上传成功场景等。

六是明确突发事件的处置流程，将攻击场景规划至不同的处置流程：上机查证类处置流程、 非上机查证类处置流程等。

七、 溯源反制：人才是关键

溯源工作一直是安全的重要组成部分，无论在平常的运维工作，还是红蓝对抗的特殊时期，在发生安全事件后，能有效防止被再次入侵的有效手段，就是溯源工作！

在红蓝对抗的特殊时期，防守队中一定要有经验丰富、思路清晰的溯源人员，能够第一时间进行应急响应，按照应急预案分工，快速查清入侵过程，并及时调整防护策略，防止再次入侵，同时也为反制人员提供溯源到的真实 IP，进行反制工作。

反制工作是防守队反渗透能力的体现，普通的防守队员一般也只具备监测、分析、研判的能力，缺少反渗透的实力。这将使防守队一直属于被动的一方，因为防守队没有可反制的固定目标，也很难从成千上百的攻击 IP 里，确定哪些可能是攻击队的地址，这就要求防守队中要有经验丰富的反渗透的人员。

经验丰富的反渗透人员会通过告警日志，分析攻击 IP、攻击手法等内容，对攻击 IP 进行端口扫描、IP 反查域名、威胁情报等信息收集类工作，通过收集到的信息进行反渗透。

防守队还可通过效防攻击队社工手段，诱导攻击队进入诱捕陷阱，从而达到反制的目的，定位攻击队自然人的身份信息。

第五章 建立实战化的安全体系

安全的本质是对抗。对抗是攻防双方能力的较量，是一个动态的过程。业务在发展，网络在变化，技术在变化，人员在变化，攻击手段也在不断变化。网络安全没有“一招鲜”的方式，需要在日常工作中，不断积累不断创新，不断适应变化，持续地构建自身的安全能力，才能面对随时可能威胁系统的各种攻击，不能临阵磨枪、仓促应对，必须立足根本、打好基础，加强安全建设、构建专业化的安全团队，优化安全运营过程，并针对各种攻击事件采取重点防护才是根本。

防守队不应以“修修补补，哪里出问题堵哪里”的思维来解决问题，而应未雨绸缪，从管理、技术、运行等方面建立实战化的安全体系，有效应对实战环境下的安全挑战。

一、 完善面对实战的纵深防御体系

实战攻防演习的真实对抗表明，攻防是不对称的。通常情况下，攻击队只需要撕开一个点，就会有所“收获”，甚至可以通过攻击一个点，拿下一座“城池”。

但对于防守工作来说，考虑的却是安全工作的方方面面，仅关注某个或某些防护点，已经满足不了防护需求。实战攻防演习过程中，攻击队或多或少还有些攻击约束要求，但真实的网络攻击则完全无拘无束，与实战攻防演习相比较，真实的网络攻击更加隐蔽而强大。

为应对真实网络攻击行为，仅仅建立合规型的的安全体系是远远不够的。随着云计算、大数据、人工

智能等新型技术的广泛应用，信息基础架构层面变得更加复杂，传统的安全思路已越来越难以适应安全保障能力的要求。必须通过新思路、新技术、新方法，从体系化的规划和建设角度，建立纵深防御体系架构，整体提升面向实战的防护能力。

从应对实战角度出发，对现有安全架构进行梳理，以安全能力建设为核心思路，面向主要风险重新设计政企机构整体安全架构，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，并努力将安全工作前移，确保安全与信息化“三同步”(同步规划、同步建设、同步运行)，建立起能够具备实战防护能力、有效应对高级威胁，持续迭代演进提升的安全防御体系。

二、 形成面向过程的动态防御能力

在实战攻防对抗中，攻击队总是延续信息收集、攻击探测、提权、持久化的一个个循环过程。攻击队总是通过不断的探测发现环境漏洞，并尝试绕过现有的防御体系，成功的入侵到网络环境中。如果防御体系的安全策略长期保持不变，一定会被“意志坚定”的攻击队得手。所以，为了应对攻击队的持续变化的攻击行为，需要防御体系自身具有一定适应性的动态变得检测能力和响应能力。

在攻防对抗实践中，防守对应利用现有安全设备的集成能力和威胁情报能力，通过云端威胁情报的数据，让防御体系中的检测设备和防护设备发现更多的攻击行为，并依据设备的安全策略做出动态的响应处置，把攻击队阻挡在边界之外。同时，在设备响应处置方面，也需要通过攻击队的攻击行为和动机支持多样化的防护能力，例如封堵 IP、拦截具有漏洞的 URL 的组页面访问等策略。

通过动态防御体系，不仅可以有效拦截攻击队的攻击行为，同时还可以迷惑攻击队，让攻击队的探测行为失去方向，让更多的攻击队知难而退，从而在对抗过程中占得先机。

三、 建设以人为本的主动防御能力

安全的本质是对抗，对抗两端是人与人之间的较量。攻防双方都在对抗过程中不断提升各自的攻防能力。在这个过程中，就需要建立一个高技术的安全运营团队，利用现有的防御体系和安全设备，持续地检测内部的安全事件告警与异常行为，通过安全事件告警和异常行为分析，发现已进入到内部的攻击队，并对其采取安全措施，压缩攻击队停留在内部的时间。

构建主动防御的基础是可以采集到内部的大量的、有效的数据，包括安全设备的告警、流量信息、账号信息等。为了对内部网络影响最小，采用流量威胁分析的方式，实现“全网”流量威胁感知，特别是关键的边界流量、内部重要区域的流量。安全运营团队应利用专业的攻防技能，从这些流量威胁告警数据中发现攻击线索，并对已发现的攻击线索进行威胁巡猎、拓展，一步步找到真实的攻击点和受害目标。

主动防御能力主要表现为构建安全运营的闭环，包括以下几个方面。

在漏洞的运营方面，形成持续的评估发现、风险分析、加固处置的闭环，减少内部的受攻击面，提升网络环境的内生安全。

在安全事事件运营方面，对实战中的攻击事件的行为做到“可发现、可分析、可处置”的闭环管理过程，实现安全事件的全生命周期的管理，压缩攻击队停留在在内部的时间，降低安全

事件的负面影响。

在资产运营方面，逐步建立起配置管理库（CMDB），定期开展暴露资产发现，并定期更新配置管理库，这样才能使安全运营团队快速定义攻击源和具有漏洞的资产， 通过对未知资产处置和漏洞加固，减少内外部的受攻击面。

四、 基于情报数据的精准防御能力

在实战攻防对抗中，封堵 IP 是很多防守队的主要响应手段。这种手段相对来讲简单、粗暴。同时，采用这种手段，容易造成对业务可用性的影响，主要体现在以下两个方面。

1）如果是检测设备误报，就会导致被封堵的 IP 并非是真实的攻击 IP,这会影响到互联网用户的业务。

2）如果攻击 IP 自身是一个 IDC 出口 IP，那么封堵该 IP，就可能造成 IDC 后端大量用户的业务不可用。

所以，从常态化安全运行的角度来看，防守队应当逐步建立基于情报数据的精准防御能力。具体来说，主要包括以下几个方面。

首先，防守队需要建设一种精准防御的响应能力，在实战攻防对抗中针对不同的攻击 IP、攻击行为可采用更加细粒度、精准的防御手段。

结合实战攻防对抗场景，防守队可以利用威胁情报数据共享机制，实现攻击源的精准检测与告警，促进进精准防御，减少检测设备误报导致业务部分中断的影响。此外，让威胁情报数据共享在多点安全设备上共同作用，可以形成多样化、细粒度化的精

准防御。例如，在网络流量检测设备、终端检测与响应系统、主机防护系统等。

其次，为了最小化攻防活动对业务可用性的影响，需要设计多样化的精准防御手段与措施，既要延缓攻击，同时也要实现业务连续性需要。

例如，从受害目标系统维度去考虑设计精准防御能力，围绕不同的目标系统，采取不同的响应策略。如果是针对非实时业务系统的攻击，可以考虑通过防火墙封禁 IP 的模式;但如果是针对实时业务系统的攻击，就应考虑在 WAF 设备上拦藏具有漏洞的页面访问请求，从而达到实时业务系统的影响最小化。

最后，为了保证实战攻防对抗过程不会大面失陷，在重要主机侧应加强主机安全防护，阻止主机层面的恶意代码运行与异常进程操作。例如域控服务器、网管服务器、OA 服务器、邮件服务器等。

五、 打造高效一体的联防联控机制

在实战攻防对抗中，攻击是一个点，攻击队可以从一个点就攻破整座“城池”。所以在防守的各个阶段，不应只是安全部门在孤独的战斗，而是需要更多的资源、更多的部门协同工作，才有可能做好全面的防守工作。

例如，一个攻击队正在对某个具有漏洞的应用系统渗透攻击，在检测发现层面，需要安全运营团队的监控分析发现问题，然后通知网络部门进行临时封堵攻击 IP，同时要让开发部门对应用系统的漏洞尽快进行修复。这样才能在最短时间内让攻击事件的处置形成闭环。

在实战攻防对抗中，要求防守队一定要建立起联防联控的机制，分工明确、信息通畅。 唯有如此，才能打好实战攻防演习的战斗工作。联防联控的关键点。

1） 安全系统协调

通过安全系统的接口实现系统之间的集成，提升安全系统的联动，实现特定安全攻击事件自动化处置，提高安全事件的响应处置效率。

2） 内部人员协同

内部的安全部门、网络部门、开发部门、业务部门全力配合实战攻防对抗工作组完成每个阶段的工作，同时在安全值守阶段全力配合工作组做好安全监控与处置的工作。

3） 外部人员协同

实战攻防对抗是一个高频的对抗活动，在这期间，需要外部的专业安全厂商配合工作组一起来防守，各个厂商之间应依据产品特点和职能分工落实各自工作，并在期间做到信息通讯顺畅、听从指挥。

4） 平台支撑、高效沟通

为了加强内部团队的沟通与协同，在内部通过指挥平台实现各部门、各角色之间的流程化、电子化沟通，提升沟通协同效率，助力联防联控有效运转。

第六章 强化行之有效的整体防御能力

2020年的实战攻防演习的最新要求是:与报备目标系统同等重要的系统被攻陷也要参照报备目标系统规则扣分。

这就对大型机构的防守队带来了前所未有的防守压力。原来通行的防守策略是重兵屯在总部（目标系统一般在总部），提升总部的整体防御能力。但是随着实战攻防演习规则的演变，总部和分支机构就变的同等重要。

从攻击路径来看，分支机构的安全能力一般弱于总部，同时分支机构和总部网络层面是相通的，并且早期安全建设的时候往往会默认对方的网络是可信的；在安全防护层面，总部一般也仅仅是对来自分支机构的访问请求设置一些比较粗犷的访问控制措施。这些安全隐患都会给攻击队留出机会，使攻击队可以从薄弱点进入，然后横向移动到总部的目标系统。

因此，防守队只有将总部和分支机构进行统一的安全规划和管理，形成一个整体防御能力，才能有效的开展实战攻防对抗。在整体防御能力上，建议防守队开展如下工作。

1） 互联网出口统一管理

条件允许的情况下，应尽量上收分支机构的互联网出入口。统一管理的好处是集中防御、节约成本、降低风险。同时，在整体上开展互联网侧的各类风险排查，包括互联网来知资产、敏感信息泄露、杜工信息的清理等工作。

2） 加强分支机构防御能力

如果无法实现分支机构的互联网出入口统一管理，则分支机

构需要参考总部的安全体系建设完善其自身的防御能力，避免成为安全中的短板。

3） 全面统筹、协同防御

在准备阶段，应配合总部开展风险排查；在实战值守阶段，与防守队一起安全值守，并配置适当的安全监控人员、安全分析处置人员，配合防守队做好整体的防御，配合防守队做好攻击的应急处置等工作。

附录 奇安信红队能力及攻防实践

自 2016 年奇安信集团协助相关部委首次承办网络实战攻防演习以来，这种新的网络安全检验模式已经有了长足的发展。

2016 年至 2020 年，奇安信集团参与了全国范围内 380 场实战攻防演习的红队活动，其中参与监管部门组织的防守 110 场，参与行业主管部门组织的防守 60 场，参与各政企单位组织的防守 210 场。

在 2016 年至 2020 年的网络实战攻防演习中，奇安信集团共协助 520 家政企机构开展现场防守工作，涉及 34 个行业，共投入现场防守团队 3712 人次，二线专家与远程支持团队 1410 人次，后勤保障团队 242 人次，累计投入约 37381 人日。