奇安信
新一代网络安全领军者

实战攻防演习之

蓝队视角下的防御体系构建

奇安信安服团队

2019. 8

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 2019 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、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全能力？这已经成为大型政企机构运营者关心的重要问题。

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 200 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全能力。

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，红方与蓝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，也有一些实际的攻防演习，将蓝队设为攻击队、将红队设为防守队。在本系列丛书中，我们依据绝大多数网络安全工作者的习惯，统一将攻击队命名为红队，将防守队命名为蓝队，而紫队则代表组织演练的机构。

《蓝队视角下的防御体系构建》是本系列丛书的第二本。本书希望通过归纳总结蓝队防御的三个阶段、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，帮助政企机构弥补薄弱环节，更好地提升演习水平，构筑更有效的安全防御体系。

目　　录

第一章 什么是蓝队

蓝队，一般是指网络实战攻防演习中的防守一方。

蓝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。蓝队的主要工作包括前期安全检查、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。

实战攻防演习时，蓝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、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，提升防守能力。

特别需要说明的是：蓝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。

下面是组成蓝队的各个团队在演习中的角色与分工情况：

目标系统运营单位：负责蓝队整体的指挥、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。

某些情况下，还会有其他组成人员，这需要根据实际情况具体分配工作。

特别的，作为蓝队，了解对手（红队）非常重要。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主动权。

第二章 蓝队三步走——防守的三个阶段

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，蓝队需要按照备战、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、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，蓝队在演习之前，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、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、应急预案完善与演练等。

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，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，全流量安全威胁检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、 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三点：

1） 做好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进行分析确认并溯源，向后，指导协助事件处置人员对确认的攻击进行处置。

2） 全面布局安全监测预警

安全监测须尽量做到全面覆盖，在网络边界、内网区域、应用系统、主机系统等方面全面布局安全监测手段，同时，除了 IDS、WAF 等传统安全监测手段外，尽量多使用天眼全流量威胁检测、网络分析系统、蜜罐、主机加固等手段，只要不影响业务，监测手段越多元化越好。

3） 提高事件处置效率效果

安全事件发生后，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。

三、 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。应对准备、预演习、实战等阶段工作中各环节的工作进行全面复盘，复查层面包括工

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、应急预案及演练和注意事项等所有方面。

针对复盘中暴露出的不足之处，如管理层面的不完善、技术层面需优化的安全措施和策略、协调处置工作层面上的不足、人员队伍需要提高的技术能力等各个方面，应进行立即整改，整改加固安全漏洞隐患，完善安全防护措施，优化安全策略，强化人员队伍技术能力，有效提升整体网络安全防护水平。

第三章 蓝队应对攻击的常用策略

未知攻焉知防。如果企业安全部门不了解攻击者的攻击思路、常用手段，有效的防守将无从谈起。从攻击者实战视角去加强自身防护能力，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。针对攻击者或红队的常用套路，蓝队应对攻击的常用策略可总结为：防微杜渐、收缩战线、纵深防御、核心防护、洞若观火等。

一、 防微杜渐：防范被踩点

攻击者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。前期防踩点，首先要尽量防止本单位敏感信息泄露在公共信息平台，加强人员安全意识，不准将带有敏感信息的文件上传至公共信息平台。

社工也是攻击者进行信息收集和前期踩点的重要手段，要定期对信息部门重要人员进行安全意识培训，如：来路不明的邮件附件不要随便点开，聊天软件未经身份确认不要随便添加。此外，安全管理和安全意识培训难免也会有漏网之鱼，安全运营部门应定期在一些信息披露平台搜索本单位敏感词，查看是否存在敏感文件泄露情况。

二、 收缩战线：收敛攻击面

门用于防盗，窗户没关严也会被小偷得逞。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，越容易被攻击者“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互联网暴露面。

1） 攻击路径梳理

由于网络不断变化、系统不断增加，往往会产生新的网络边界和新的系统。蓝队（防守单位）一定要定期梳理自己的网络边界、可能被攻击的路径，尤其是内部系统全国联网的单位更要注重此项梳理工作。

2） 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、测试系统和端口私自开放在互联网上，方便维护的同时也方便了攻击者。攻击者最喜欢攻击的 WEB 服务就是网站后台，以及安全状况比较差的测试系统。蓝队须定期检测如下内容：开放在互联网的管理后台、开放在互联网上的测试系统、无人维护的僵尸系统、拟下线未下线的系统、疏漏的未纳入防护范围的互联网开放系统。

3） 外部接入网络梳理

如果正面攻击不成，红队或攻击者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。防守单位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。

4） 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，这往往是攻击者最喜欢打的入口，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。

三、 纵深防御：立体防渗透

前期工作做完后，真正的防守考验来了。防守单位在互联网上的冠名网站、接口、VPN 等对外服务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，同时试图建立多条隐蔽隧道，巩固成果，使防守者顾此失彼。

此时，战争中的纵深防御理论就很适用于网络防守。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、重点集权系统防护、无线网络防护、外部网络接入防护甚至物理层面的防护，都需要考虑进去。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。

1） 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部署网络防护设备和开展攻击检测两方面开展。需部署的网络防护设备包括：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（云 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。

2） 访问控制措施

互联网及内部系统、网段和主机的访问控制措施，是阻止攻击者打点、内部横向渗透的最简单有效的防护手段。防守者应依照“必须原则”，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的情况出现，通过合理的访问控制措施尽可能地为攻击者制造障碍。

3） 主机防护

当攻击者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者内网攻击成果的大小。防守者应从以下几个方面对主机进行防护：关闭没用的服务；修改主机弱口令；高危漏洞必须打补丁（包括装在系统上的软件高危漏洞）；安装主机和服务器安全软件；开启日志审计。

4） 集权系统

集权系统是攻击者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。

蓝队或防守者一般可从以下方面做好防护：集权系统的主机安全；集权系统访问控制；集权系统配置安全；集权系统安全测试；集权系统已知漏洞加固或打补丁；集权系统的弱口令等。

5） 无线网络

不安全的开放无线网络也有可能成为攻击者利用的攻击点。无线开放网络与业务网络应分开。一般建议无线网接入采用强认证和强加密。

6） 外部接入网络

如果存在外部业务系统接入，建议接入的系统按照互联网防护思路，部署安全设备，并对接入的外部业务系统进行安全检测，确保接入系统的安全性，防止攻击者通过这些外部业务系统进行旁路攻击。

四、 守护核心：找到关键点

核心目标系统是攻击者的重点攻击目标，也应重点防护。上述所有工作都做完后，还需要重点梳理：目标系统和哪些业务系统有联系？目标系统的哪些服务或接口是开放的？传输方式如何？梳理得越细越好。同时还须针对重点目标系统做一次交叉渗透测试，充分检验目标系统的安全性。协调目标系统技术人员及专职安全人员，专门对目标系统的进出流量、中间件日志进行安全监控和分析。

五、 洞若观火：全方位监控

任何攻击都会留下痕迹。攻击者会尽量隐藏痕迹、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） 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。蓝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。

2） 主机监控

任何攻击最终都会落到主机（服务器或终端）上。通过部署合理的主机安全软件，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。

3） 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者分析攻击路径的一种有效手段。攻击者攻击成功后，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，以防止防守者追踪。防守者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。

4） 情报监控

高端攻击者会用 0day 或 Nday 漏洞来打击目标系统、穿透所有防守和监控设备，防守者对此往往无能为力。防守单位可通过与更专业的安全厂商合作，建立漏洞通报机制，安全厂商应将检测到的与防守单位信息资产相关的 0day 或 Nday 漏洞快速通报给防守单位。防守单位根据获得的情报，参考安全厂商提供的解决方案，迅速自查处置，将损失减到最少。

第四章 建立实战化的安全体系

安全的对抗是动态的过程。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。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、优化安全运维，并针对各种攻击事件采取重点防护。蓝队或防守单位不应以“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、 认证机制逐步向零信任架构演进

从实战攻防对抗的结果来看，传统网络安全边界正在被瓦解，无穷无尽的攻击手段导致单位网络安全防护措施难以起到效果，网络是不可信任的。在这种情况下，应该将关注点从“攻击面”向“保护面”上转移，而零信任安全则是从“保护面”上考虑，提出了解决安全问题，提高防御能力的一种新思路。

零信任安全针对传统边界安全架构思想进行了重新评估和审视，并对安全架构思路给出了新的建议，其核心思想是：默认情况下不应该信任网络内部和外部的任何人、设备和系统，需要基于认证和授权重构访问控制的信任基础。零信任对访问控制进行了范式上的颠覆，引导安全体系架构从网络中心化走向身份中心化，其本质诉求是以身份为中心进行访问控制。

零信任体系会将访问控制权从边界转移到个人设备与用户上，打破传统边界防护思维，建立以身份为信任基础的机制，遵循先验证设备和用户、后访问业务的原则，不再自动信任内部或外部任何人、设备和应用，在授权前对任何试图接入网络和访问业务应用的人、设备或应用都进行验证，并提供动态的细粒度访问控制策略以满足最小权限原则。

零信任体系把防护措施建立在应用层面，构建从访问主体到客体之间端到端的、最小授权的业务应用动态访问控制机制，极大地收缩了攻击面。零信任安全在实践机制上拥抱灰度，兼顾难以穷尽的边界情况，最终以安全与易用平衡的持续认证，改进原有固化的一次性强认证，以基于风险和信任持续度量的动态授权替代简单的二值判定静态授权，以开放智能的身份治理优化封闭僵化的身份管理，提升了对内外部攻击和身份欺诈的发现和响应能力。建议单位网络安全基础架构逐步向零信任体系演进。

二、 建立面向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，攻击者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，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、同步使用），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。

三、 强化行之有效的威胁监测手段

在实战攻防对抗中，监测分析是发现攻击行为的主要方式，在第一时间发现攻击行为，可为应对和响应处置提供及时支撑，威胁监测手段在防护工作中至关重要。通过对多个单位安全防护工作进行总结分析，威胁监测手段方面存在的问题主要是：

1） 没有针对全流量威胁进行监测，导致分析溯源工作无法开展；

2） 有全流量威胁监测手段，但流量覆盖不完全，存在监测盲区；

3） 只关注网络监测，忽视主机层面的监测，当主机发生异常时不易察觉；

4） 缺乏对邮件安全的监测，使得钓鱼邮件，恶意附件在网络中畅通无阻；

5） 没有变被动为主动，缺乏蜜罐等技术手段，无法捕获攻

击、进一步分析攻击行为。

针对上述存在的问题，强化行之有效的威胁监测手段，建立以全流量威胁监测分析为“大脑”，以主机监测、邮件安全监测为“触角”，以蜜罐监测为“陷阱”，以失陷检测为辅助手段的全方位安全监测机制，更加有效地满足实战环境下的安全防守要求。

四、 建立闭环的安全运营模式

分析发现，凡是日常安全工作做得较好的单位，基本都能够在实战攻防演习时较快地发现攻击行为，各部门之间能够按照约定的流程，配合得当、快速完成事件处置，在自身防护能力、人员协同等方面较好地应对攻击。

反之，日常安全工作较差的单位，大多都会暴露出如下问题：很多基础性工作没有开展，缺少相应的技术保障措施，自身防护能力欠缺；日常安全运维不到位，流程紊乱，各部门人员配合难度大。这些问题导致攻击行为不能被及时监测，攻击者来去自由；即便是好不容易发现了入侵行为，也往往会因资产归属不清、人员配合不顺畅等因素，造成处置工作进度缓慢。这就给了攻击者大量的可乘之机，最后的结果往往是目标系统轻而易举地被攻陷。

所以，政企机构应进一步做好安全运营工作，建立闭环的安全运营体系：

通过内部威胁预测、外部威胁情报共享、定期开展暴露资产发现、安全检查等工作，实现攻击预测，提前预防的目的；

通过开展安全策略优化、安全基线评估加固、系统上线安全检查、安全产品运行维护等工作，建立威胁防护能力；

通过全流量风险分析、应用失陷检测、渗透测试、蜜罐诱导等手段，对安全事件能进行持续检测，减少威胁停留时间；

通过开展实战攻防演习、安全事件研判分析、规范安全事件处置流程，对安全事件及时进行控制，降低危害影响，形成快速处置和响应机制。

闭环安全运营体系非常重视人的作用。配备专门的人员来完成监控、分析、响应、处置等重要环节的工作，在日常工作中让所有参与人员能够熟悉工作流程、协同作战，使得团队能不断得到强化锻炼，这样在实战时中才能从容面对各类挑战。

安全防御能力的形成并非一蹴而就，单位管理者应重视安全体系建设，建立起“以人员为核心、以数据为基础、以运营为手段”的安全运营模式，逐步形成威胁预测、威胁防护、持续检测、响应处置的闭环安全工作流程，打造“四位一体”的闭环安全运营体系，通过日常网络安全建设和安全运营的日积月累，建立起相应的安全技术、管理、运营体系，形成面向实战的安全防御能力。

附录 奇安信蓝队能力及攻防实践

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 2019 年上半年，奇安信集团参与了全国范围内 139 场实战攻防演习的蓝队活动，其中参与监管部门组织的防守 47 场，参与行业主管部门组织的防守 35 场，参与各政企单位组织的防守 57 场。

在 2016 年至 2019 年上半年的网络实战攻防演习中，奇安信集团共协助 302 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 1856 人次，二线专家与远程支持团队 510 人次，后勤保障团队 126 人次，累计投入约 24920 人日。