安天 ANTIY

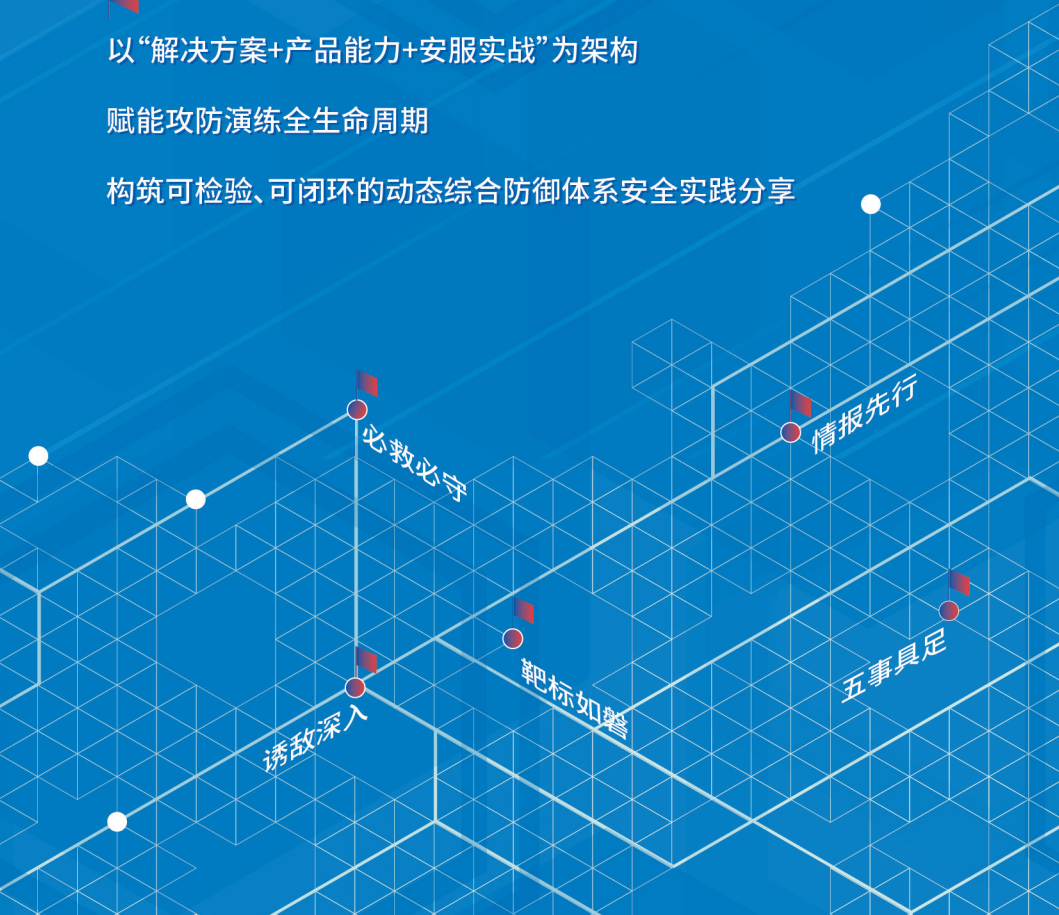
攻防演练庙算记

2023安天网络安全实战攻防演练专题集

以“解决方案+产品能力+安服实战”为架构

赋能攻防演练全生命周期

构筑可检验、可闭环的动态综合防御体系安全实践分享



前言

网络安全实战攻防演练活动，是目前通过发现各行业重要信息系统的安全风险与隐患、考察网络安全责任落实情况、检验防守单位的安全防护能力，进而系统提升安全防护水平和技术对抗能力的重要手段。安天在2022 年，结合攻防演练的防守要点、各阶段 / 场景化专项防护方案、终端 / 云主机防护、全流量威胁检测、文件分析、欺骗式防御 & 威胁捕获、边界阻断与入侵防护等维度组织了《2022 安天网络安全实战攻防演练专题》[1]，综合分享了实践经验、产品创新与场景价值，提供了系统解决方案参考，受到用户的肯定与关注。

同时，在 2022 年各类攻实战防演练活动中，安天不仅有效支撑客户完成了防守任务，还帮助客户取得了超越预期的成绩。包括：

1) 在专项威胁情报场景中，为某客户单位监测并阻断网络攻击高达近 4 万起，溯源加分 500 分；

2) 在邮件安全监测场景中，为某客户单位监测分析钓鱼邮件攻击事件 10 余起，溯源加分 720 分；

3) 在网站安全防护场景中，为某客户单位阻断 Web 攻击事件近 3 万起，监测入侵蜜罐事件 11 起，溯源加分 400 分；

4) 在终端威胁检查场景中，为某客户单位排查发现终端威胁文件 200 余个（其中远控木马 18 个），并成功清除终端威胁隐患；

5) 在威胁诱捕分析场景中，为某客户单位捕获攻击事件 70 余起，溯源加分 900 分；

6) 在网络边界监测场景中，监测发现网络攻事件高达近 80 万起，并有效阻断；

7) 在靶标系统防护场景中，为超过 40 家客户单位靶标系统提供的防护服务，并保障了所有靶标系统均未被攻陷等。

凭借优质的服务品质、产品价值与实战能力，安天获得了多家客户的感谢信。（详见图 I ）

图 I　安天获得客户感谢信部分展示

以攻练防，以防治攻。结合安天全新安全产品生态体系[2]，以《孙子兵法》中重要战术素养和作战精神主题的 2023 安天网络安全实战攻防演练专题——《2023 安天实战攻防演练庙算记》，也于 2023 年 5 月正式发布。

《2023 安天实战攻防演练庙算记》不仅是在《2022 安天网络安全实战攻防演练专题》基础上的优化升级，更是针对在如今严峻的网络安全形势下，如何进行有效威胁对抗的一次系统思考、实践与总结。所以，整体内容将更聚焦于安全实战场景，以达成客户有效安全价值为目的，分享 2023 年安天以“解决方案 + 产品能力 + 安服实战”为架构，布防基础安全产品防御能力联动安全专家现场响应能力，针对易失分点、威胁情报、邮件安全、网站安全、网络边界、终端威胁、威胁诱捕及靶标安全等攻防演练活动“事前、事中、事后”中的关键防护场景，构筑的可检验、可闭环的动态综合防守体系。

参考资料

[1] 2022 安天攻防演练收录版（含视频）
https://mp.weixin.qq.com/s/Ct1DMpcNGrNWDsy-nZrxZw
[2] 聚合 效能 闭环丨安天发布六项创新产品
https://mp.weixin.qq.com/s/pAKRBCBkfXyv2NtEZMjrHA

目录

CONTENTS

01 整体防守方案：五事具足

《孙子兵法》开篇即是“战略观”，并用“五事”说明了在所有对抗中的要素：一曰道，二曰天，三曰地，四曰将，五曰法。

道者，令民与上同意也，故可以与之死，可以与之生，而不畏危。

天者，阴阳、寒暑、时制也。

地者，高下、远近、险易、广狭、死生也。

将者，智、信、仁、勇、严也。

法者，曲制、官道、主用也。

事实上，发生在网络空间的“攻防演练对抗”亦是如此，胜利的意志、对业务系统的了解、安全设备部署的方案、人员团队、方法策略缺一不可。

1. 明确演练目的

“道者”，是明确网络安全实战攻防演练的目的并达成的一致认知：发现系统漏洞、检验防护策略、锻炼应急能力和构筑防御体系。根据当前网空威胁和防御的发展现状，防御没有“银弹”，没有单一技术或者单一种安全框架可以解决所有的问题，因此在整体网空防御安全体系化建设中，需要进行不断地的叠加演进、体系化的建设安全防御保障，从而适应发展的需要。

安天将威胁对抗经验与安全规划需求进行整合，基于防御关键动作的概念，于 2020 年提出安天防御框架 (ISPDR) [1]，包括 5 个部分 (详见图 1-1)：

1) 识别：是网络安全管理的基础；

2) 塑造：是建立防御主动性的前提；

3) 防护：是系统对威胁做出的行为反应；

4) 检测：是发现、定位和定性网络安全威胁的方法；

5) 响应：是处置、管理风险和威胁事件的过程。

图 1-1 安天防御框架（ISPDR）

安天提出，“塑造”是防御动作的关键环节，它突出的是安全参与 IT 规划整个生命周期的过程性，强调 IT 的可塑性能够在一定程度上带来防御的主动性。也就是说，我们需要把整个安全基因的能力沉浸式嵌入到数字化系统中，这样在后期的威胁对抗与安全应用中，才能更好的实现积极防御能力，使我们在和对手的对抗中获得一个更具优势的地位。

2. 制定防护体系

“天者”，是以基础安全产品为能力支撑，覆盖攻防演练活动的启动、备战、迎战、总结等所有环节，提供质量有保障、流程标准化、成果价值高的全生命周期的安全防护服务。

安天安全服务体系依托于安天防御框架（ISPDR），系统映射在演练活动的各个阶段，全面满足在攻防演练活动中场景、事件与人员的相关需求。

3. 优势能力支撑

“地者”，是安天充分发挥下一代威胁检测引擎和安全内核的基础优势，自主研发了可覆盖信息安全领域全场景的安全产品生态体系，为攻防演练活动中防守服务的落地实施提供了更直接顺畅的有效支撑。终端防护、云主机安全、流量监测、威胁分析、威胁捕获、边界防护、防病毒网关等安天多款产品可实现威胁情报协同共享，有效拓宽防御覆盖面与纵深度，共同发现和阻断攻击。

4. 安全专家实战

“将者”，乃是攻防演练的队伍，安天基于近二十三年的应急响应支撑工作经验，以及多年的安全服务、技术、人才和产品的积淀，形成了先进、完善的攻防演练服务框架。（详见图 1-2）

图 1-2 安天攻防演练防守服务概览

安天从 2016 年开始连续多年参与国家级攻防演练行动，协助 70 余个国家部委、能源电力、交通运输、金融、大型国企等客户单位圆满完成了

防守保障任务，并收到了专项感谢信。在攻防演练活动中，安天主要通过四大优势为客户持续赋能有效安全价值：

1) 基于近二十三年对网络空间攻防对抗的深入研究，以及多年大型攻防演练的实战积淀，对网络安全事件的预防、监控、处置与溯源，有着成熟先进的方法体系；

2) 基于建立完善的动态综合防御体系，利用专业的监控平台、边界防护设备、终端防护软件、威胁情报及处置分析工具，形成覆盖“边界侧 + 端点侧 + 网络流量侧”的全方位监测能力；

3) 基于“人机共智”的服务理念，结合专业的安全产品，从检测发现、整改加固、整体布防、安全监测、应急响应及云端检测，可支撑攻防演练活动全生命周期的各个环节防守任务，能整体把控安全态势；

4) 基于实战经验丰富的安全服务团队储备，能最大可能的为不同行业客户保驾护航。

5. 闭环方法指导

最后，所谓“法者”，是主用，也是最具体的一环，【安天攻防演练庙算记】最独特的就是在攻防演练的各个环节对应了安天防御框架（ISPDR），也就是“道”，为客户从启动、准备、迎战、总结的全生命周期防守提供了闭环方法指导。

5.1 启动阶段：对应 “识别” 部分

深入了解客户的业务系统和工作场景，通过安天可扩展威胁检测响应平台 XDR（简称：安天 XDR）进行自动化资产梳理和网络安全防护现状调研，协助客户建立健全的攻防演练组织和管理规划，明确演练期间的各项工作机制，向所有相关责任人宣贯攻防演练的重要性和工作部署方案。

同时，对客户的网络安全架构进行评估，并及时制定优化方案。

5.2 准备阶段：对应 “塑造” 与 “防护” 部分

首先，组织专项团队为客户提供脆弱性检测服务，检测方法包括基线检查、漏洞扫描、渗透测试等，并附带提供威胁检测与处置服务。同时，可以通过安天 XDR 实现漏洞的全生命周期管理，例如漏洞的导入、匹配和监测等；也可以运用安天 XDR 导入漏扫结果或者通过流量被动发现来实现弱口令的管理。

然后，及时对脆弱性关联的资产进行全方位的安全加固，同时依据安全现状进行演练常见的安全防守策略调优。

在演练活动临近时，内部组织多场景的攻防演练预演，以此验证安全加固和优化工作的有效性，以及各项工作机制的可操作性。

此外，将同步为客户提供安全意识、安全攻防技术等安全培训，全面提升相关人员的安全意识和防护水平。

最后，在演练活动正式开始前，协同客户制定演练期间的值守方案，确保值守方案可有效落地执行。

5.3 迎战阶段

安天将基于自身的威胁情报分析平台和威胁捕获系统为客户提供威胁情报服务，协助客户全方位掌握演练期间的相关威胁情报。同时，运用自研安全产品和客户已有的第三方安全产品，为客户提供 7×24 小时的安全监测值守服务，以及支撑威胁情报、邮件安全、网站防护、网络边界、终端威胁、威胁诱捕及靶标系统等七大关键场景防护的专项服务。

在安全监测值守期间，组织专项团队对安全告警和威胁情报等进行分析确认，结合安天 XDR，可对接主流安全平台收集告警与日志，进行关联分析，从而对攻击画像展开描述；可联动安天探海威胁检测系统（以下简称“探海”）进行流量包深度分析等，对证据进行留存。同时，工单系统在迎战过程中全程跟进，对各项操作性任务进行备档追踪。在确认发现安全事件时，如防线被攻击方攻破、信息破坏事件（篡改、泄露、窃取、丢

失等）、大规模病毒事件、网站漏洞事件等，安天将及时提供应急处置服务，并协调相关资源进行追踪溯源，协助客户撰写防守成果报告，报送给相关单位，获得加分。

5.4 总结阶段：对应 “塑造” 部分，形成闭环

演练活动结束后，将对演练期间攻击成功的事件和防守成功的事件等相关情况，进行详细的全过程复盘与总结。同时，根据演练过程中暴露的安全问题和流程问题，为客户提供针对性的解决措施和建议，并协助客户完善安全防御机制，优化安全防护体系。

最后，安天还将为客户提供具有针对性的专项技能培训服务，协助客户培养符合自身网络安全要求的人才体系。

参考资料

[1]《安天安全理念：动态综合网络安全防御》
https://www.antiy.cn/safety_concept/index.html

02 十大防守要点：必救必守

在攻防对抗中，攻守双方必须要有对彼此敌情、行动、意图等的分析，才能知得失之计。《孙子兵法·行军篇》中有讲，兵非贵益多也，唯无武进，足以并力、料敌、取人而已。而《虚实篇》也提到：攻而必取者，攻其所不守也；守而必固者，守其所不攻也。故善攻者，敌不知其所守；善守者，敌不知其所攻。也就是说在作战前，必须对彼此所处的位置和可能的行动做到胸中有数。

在攻防演练“处军相敌”的持续对抗中，攻守双方在静动、进退、起伏等状态中不断布阵较量。对于攻击方来说，攻其所不守；作为防守方，需要知其所攻，方能守其必取。

为了帮助防守方能知晓攻击方可能攻击的关键点，安天基于攻击方视角分析，结合多年攻防实战经验，将攻击方可能用到的关键攻击动作通过“网络杀伤链”的逻辑进行归类总结，即（图 2-1）《攻击方视角分析表》。

通过利用《攻击方视角分析表》中的攻击手段，攻击方将发起攻击到拿下靶标的全过程，共分为三个重要阶段：

首先，是从防守方网络外围逐步向内渗透，通过对暴露在互联网的网站、邮箱、OA 等信息进行攻击，进而获取控制权；

其次，再对目标内部网络进行横向渗透，获取更多业务系统、办公终端、网络设备与安全设备的权限；

最终，实现攻陷，以达成攻击目标。

守而必固者，敌不知其所攻。攻击方为达成攻击目标所利用的各种攻击手段，不仅限于针对防守单位的资产暴露面和防御脆弱面，同时还包含了针对防守单位的供应链风险隐患和工作人员安全意识薄弱等一切可能利

踩点	攻击面发现	目标基本信息的搜集	
		网络空间测绘平台	
		github、gitee、网盘等泄露信息查询	
		DNS、开放端口查询、IP c段、爆破域名等方法	
		APP、小程序、H5等移动端 ……	
	重点资产发现	中间件情况	
		应用系统的供应商、软件版本	
		网络设备版本 ……	
	资产扫描		
钓鱼	构建主题、搜集信息、确定方法	人	财务、人力、客服、信息化、供应商 .....
		部门	基础信息
	免杀、宏病毒文件、对抗反垃圾邮件等		
	网络聊天群、招聘软件、邮件、客服、400、电话等		
	网址混淆、仿站、邮件内URL和ip的混淆、APP、二维码、附件、软件捆绑等		
渗透	弱口令		
	漏洞	逻辑漏洞、web自身漏洞、系统漏洞、不安全基线、APP及组件漏洞 …	
	Nday	中间件流行漏洞、软件流行漏洞、设备流行漏洞、主机流行漏洞 …	
	0day	网络设备、安全设备、VPN设备0day	
		源码审计 …	
	漏洞扫描		
对抗技术	反向代理、socks代理		
	流量混淆	CDN、伪装成web、域前置、云函数	
	流量加密	tor网络、ssl加密	
	无实体文件落地	内存webshell	对抗防守方
		powershell …	
	免杀框架、远控框架	生成免杀	
	商业军火及二开	cs、sliver、二开cs	
	反蜜罐插件		
	后渗透框架		
内网渗透	内网扫描		
	弱口令、口令复用		
	域控漏洞		
	主机漏洞		
	内网系统漏洞		
	办公设备、物联网设备、网络设备		
	权限提升、维持权限		
	移动终端		
	内网穿透 …		

图 2-1 攻击方视角分析表

用突防的攻击面。依托安天安全产品生态体系，安天制定了十大防守要点，针对这些必守、必救之处进行相应的安全设备加固和策略部署，是能够少失分，甚至多加分的前提和关键。（详见表 2-1）

表 2-1 2023 安天攻防演练解决方案十大防护要点综述

序号	易丢分点	防护要点
1	互联网资产范围不清晰，开放过多敏感端口，管理后台未做好访问控制；	资产暴露面管控
2	信息系统存在安全漏洞和弱口令情况，被攻击方利用后获取权限；	系统漏洞管理
3	网络边界缺乏有效安全管控和监测措施，攻击方很容易突破进行横向移动；	网络边界监测与防御
4	缺失对所有主机统一安全管理防护，被攻击方突破后植入木马进行远程控制；	端点安全统管
5	缺乏有效威胁情报来源，对已暴露的攻击手段和最新漏洞无法及时获悉；	专项威胁情报
6	缺少可以迷惑攻击方、延缓攻击、溯源加分的诱饵系统；	欺骗式防御构建
7	靶标系统防护强度不够，被攻击方进入内网后攻陷；	靶标安全防护
8	员工安全意识薄弱，容易被攻击方社工钓鱼邮件攻击；	安全意识宣贯 & 攻防预演
9	供应链存在风险隐患，容易被攻击者利用进行突破；	供应链安全管控
10	防守队伍安全技术能力不足，在对抗过程中无法精准定位、分析溯源与处置威胁。	安全专家支撑

安天充分发挥下一代威胁检测引擎和安全内核的基础优势，自主研发了可覆盖信息安全领域全场景的安全产品生态体系，为攻防演练防守任务的落地与实施提供了更直接、更便捷、更有效的安全实战支撑。同时，安天多款产品可实现威胁情报协同共享，有效拓宽防御覆盖面与纵深，共同发现和阻断攻击。

安天安全产品生态体系对攻防演练全生命周期防守任务支撑分布情况详见（表 2-2）。

表 2-2 安天安全产品生态体系支撑十大防护要点

序号	防护要点	支撑产品
1	资产暴露面管控	安天可扩展威胁检测响应平台 XDR（安天 XDR） 安天智甲终端防御系统 安天智甲云主机安全监测系统 安天漏洞扫描系统 安天下一代 WEB 应用防护系统（WAF）
2	系统漏洞管理	安天漏洞扫描系统 安天智甲终端防御系统 安天智甲云主机安全监测系统 安天应用威胁自免疫（Antiy RASP） 安天代码安全检测系统（Antiy SCS）
3	网络边界监测与防御	安天镇关下一代防火墙 安天镇关防病毒网关系统 安天入侵防御系统 安天下一代 WEB 应用防护系统（WAF） 安天探海威胁检测系统

4	端点安全统管	安天智甲终端防御系统 安天智甲云主机安全监测系统 威胁猎杀服务
5	专项威胁情报	安天威胁情报综合分析平台 安天捕风蜜罐系统
6	欺骗式防御构建	安天捕风蜜罐系统 安天追影威胁分析系统
7	靶标安全防护	安天全线安全产品生态体系
8	安全意识宣贯 & 攻防预演	安天安全培训服务 安天可扩展威胁检测响应平台 XDR（安天 XDR）
9	供应链安全管控	安天代码安全检测系统（Antiy SCS） 安天应用威胁自免疫（Antiy RASP） 安天可扩展威胁检测响应平台 XDR（安天 XDR）
10	安全专家支撑	安天安全服务专家团队

03 专项威胁情报：情报先行

攻守双方必须要有对彼此敌情、行动、意图等的分析，才能在行动中知得失之计。即《孙子兵法·行军篇》中提到的：兵非贵益多也，唯无武进，足以并力、料敌、取人而已。也就是说在作战前，必须对彼此所处的位置和可能的行动做到胸中有数。

所以，《孙子兵法·用间篇》有云：成功出于众者，先知也。意指之所以出手就能战胜敌人，功业超越众人，就在于能预先掌握敌情；同时，又补充到：先知者，不可取于鬼神，不可象于事，不可验于度，必取于人，知敌之情者也。也就是说想要事先了解敌情，不可求神问鬼，不可用相似的现象作类比推测，也不可用日月星辰运行的位置去验证，一定要取之于人，从那些熟悉敌情的人的口中去获取。

在实战攻防演练活动持续对抗场景中，所谓的“先知”即指威胁情报；“必取于人”中的“人”即是经受过实战考验的可靠的威胁情报产品，以及拥有丰富经验的专家。

威胁情报正是网络攻防战场上“知己知彼”与“掌控敌情”的关键，特别是在攻防对抗中，防守方在明处，防护的资产则是一个不能移动和隐藏的靶标；而攻击方躲在暗处，利用攻击行动匿名性、攻击针对性、攻击自由度、人性弱点等，总是可以找到突防机会。依靠威胁情报作为支撑，在提前掌握攻击方的攻击技术、攻击手法、攻击意图等方面“敌情”的基础之上，可有效缩短防御响应周期并提高防护针对性，对攻击方的攻击行为和攻击动作上进行阻断，驱动决策完善安全防御体系，提前部署防御策略，从而提高防御能力。

同时，在这个过程中，时间是非常重要的因素，因为攻防双方都会在

指定时间内，模拟更接近于战时的对抗状态，投入足够多的攻防资源参与对抗。因此，制胜的防守不仅仅取决于技术，还取决于组织的协作和应急响应的能力；落实到威胁情报，即其供给的精准性和快速性至关重要。

所以，安天实战攻防演练专项威胁情报服务（以下简称“安天专项威胁情报服务”，示意图详见图 3-1）立足于攻防对抗实战场景，打磨团队的战时情报作业流程，不断提升战时状态下的情报生产能力与效率，通过提供更具价值的威胁情报和更专业的解决方案，以提高防守客户单位的安全保障能力，帮助客户更好地应对攻防演练的安全挑战。

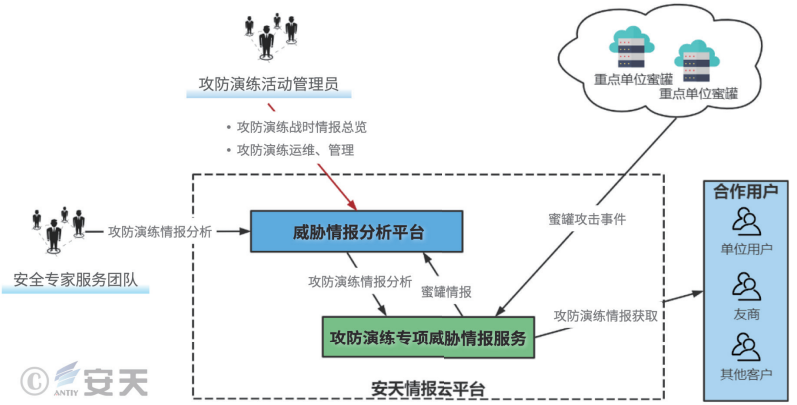


图 3-1 安天专项威胁情报服务示意图

安天专项威胁情报服务，主要通过以下 5 种手段达成客户有效安全价值：

1) 提供实时最新汇聚的情报（包含机读情报和情报交换组件产品），支撑客户提前将情报更新到防御阻断策略，让情报价值真正落实进防护体系中，避免遭受相关威胁源攻击；

2) 提供分析辅助工具，把情报顺畅地提供给安全分析人员使用。针对发现的威胁线索，如可疑 IP、域名、URL、邮箱、文件 HASH 等，可在线查询到详尽的威胁情报信息，帮助安全分析人员溯源并得分；

3) 针对攻防演练过程中暴露出的 0Day、1Day 等，收集样本信息，验证样本和漏洞，发布最新的查杀方法、修补建议；

4) 提供客户本地的情报生产和消费能力，包括对抗状态下的情报生产能力，同时支持多种方式的生成和分发流程，以满足客户各类实战场景需求。

5) 安天针对部分客户网络策略更为严格的场景，进行了专门的设计：考虑了隔离网不能第一时间更新情报库的情况，安天基于近二十三年反病毒引擎技术的耕耘，为客户提供了恶意执行体的特异性向量情报，基于执行体的恶意行为和同源特征，即使在隔离网络条件下，也有良好的能力展现。

在实战攻防演练场景中，防守方需要面对攻击方持续多维的攻击，所以，充分地了解攻击方的整体情况，才能根据攻击特点建立完善的、能有效抵御攻击威胁的安全防护体系。针对攻防演练各个阶段中，专项威胁情报服务的价值如下。

1. 启动阶段：资产清查，暴露面情报收集

安天将基于防守客户单位的业务场景为客户做资产梳理和网络安全防护现状调研，并对客户的网络安全架构进行评估，给出优化方案。

期间可运用安天捕风蜜罐系统（以下简称“捕风”）在互联网部署 ERP、OA、VPN 系统、虚拟化桌面系统、邮件服务系统等高交互蜜罐资产，并选择部分蜜罐资产预置不同的弱口令、漏洞等诱骗攻击方；即使攻击方扫描蜜罐资产并进行漏洞利用，捕风亦可无感知的进行反制。同时，散播虚假信息“蜜饵”，干扰攻击方收集情报，使其选择攻击目标时产生误判，指数级地增加攻击方的攻击成本，延缓攻击进程的同时，将攻击方不断诱导引入蜜罐陷阱，从而诱捕攻击方，保护真实资产。

2. 备战阶段：结合脆弱性情报进行加固，并把情报消费能力落实进防护体系

安天会通过基线检查、漏洞扫描、渗透测试等各种方式对目标系统进

行安全检测和安全加固，并通过威胁检测与处置服务分析漏洞。

同时，还可利用排查到的资产及系统信息，通过威胁情报查询系统找到目标系统的暴露面，从而有针对性地进行加固。如交互式查询了解已知的威胁线索，包括可疑 IP、可疑域名、可疑 URL、可疑邮箱、以及可疑的文件 HASH，安天威胁情报综合分析平台（ATID）将展示详尽的威胁相关情报。帮助分析人员缩短情报搜集与分析处理的时间，提升工作效率。

1) 查询 IP：支持对亿级的互联网 IP 地址详细信息进行查询，包括 IP 的相关情报、地理位置、开放服务和端口信息、IP 反向解析域名等信息；

2) 查询域名：支持对数十亿的域名详细信息进行查询，包括域名的相关情报、Whois 信息、子域名、域名解析记录和开源情报等信息；

3) 查询 URL：支持对亿级的 URL 威胁情报进行查询；

4) 查询邮箱：支持对数千万左右的邮箱威胁情报进行查询；

5) 查询文件 HASH：支持对数十亿的样本详细信息进行查询，包括了样本的相关威胁情报、静态信息、动态行为信息、多引擎检测结果、数字证书等等。

3. 迎战阶段：在外部打通情报视野，在内部落实情报生产分发

正式进入实战攻防演练对抗阶段时，安天将基于自身的威胁情报平台和蜜罐系统为防守客户单位提供威胁情报服务，协助客户全方位掌握演练期间的攻击相关威胁情报：

1) 攻击 IP 情报：防守客户单位可以通过安天云端威胁情报中心实时获取最新的攻击 IP 威胁情报，同时可以将这些攻击 IP 更新到防御阻断策略里，起到提前防御阻断的作用，有效避免被使用这些攻击 IP 的攻击方入侵。

2) 攻击手段情报：每日提供最新的攻击手段威胁情报，包括 0Day 漏洞、远程控制木马、物理接触攻击手段、钓鱼攻击手段等，防守客户单位获得情报后可以提前防御，有效避免因这些攻击导致系统被攻陷，进而造成被

持续扣分出局的情况。

3) 溯源分析查询：当监测到可疑 IP、可疑域名、可疑 URL、可疑邮箱、未知文件时，可以通过安天追影威胁情报平台（TIP），快速查询分析得到详尽的威胁情报信息，帮助分析人员缩短情报搜集与分析处理的时间，提升工作效率。

4. 总结阶段：汇总情报

在实战攻防演练活动结束后的总结环节，安天将为防守客户单位复盘活动期间的攻防情况，对活动期间攻击成功的事件和防守成功的事件进行复盘。安天将根据活动过程中的工作记录，回顾演练工作的全过程，整理与安全事件相关的各种信息，进行总结，除了为客户提供网络安全方面的措施和建议，还将协助客户建立自己威胁情报库，完善安全防御机制，优化安全防护体系。

5. 安天专项威胁情报服务客户价值

1) 全量威胁情报获取，通过与安天威胁捕获系统联动，在发现攻击前期行为后，对攻击样本进行情报检索查询和关联，发现更多攻击线索。

2) 基于威胁情报关联分析与恶意代码同源性分析方法，结合海量威胁知识库，还原威胁事件和攻击手法等信息，支撑安全分析人员对事件追踪溯源。

在 2022 年大型实战攻防演练活动中，安天专项威胁情报服务为某客户单位监测并阻断网络攻击高达近 4 万起，溯源加分 500 分。

04 邮件安全监测：无通其使

《孙子兵法·九地篇》中提到的“是故政举之日，夷关折符，无通其使”。也就是说，在决定战争方略的时候，就要封锁关口，废除通行符证，不充许敌方通过往来。

邮件系统作为内外网间信息传递的重要渠道，拥有防守客户单位重要的敏感数据。员工邮箱账号作为经常需要暴露的重要信息，就不可避免的容易被攻击方获取并进行有针对性的社工攻击，进而成为攻击方的内网桥头堡，因此在实战攻防演练对抗场景中，防守方的邮件系统在一开始就需要严防死守重点保障，杜绝一切攻击方可利用为攻击入口的机会。

无论是常态的网络攻击，还是攻防演练对抗期间，攻击方均将社工邮件作为重要的攻击手法，挑战着防守方的防御水平。邮件攻击的形态也逐渐从单纯的含恶意附件、链接等传统社工攻击手法的基础上，逐渐迭代出了加密、混淆、二维码、网盘等多种形态的攻击手段。由于防守客户单位邮件系统承载的数据价值远高于其公网暴露的数据，同时又部署在服务器之上，并且一般是面向互联网开放的，所以，在实战攻防演练对抗场景中，防守方将面临复杂多样的攻击，如邮件应用漏洞、操作系统漏洞、弱口令暴力破解、泄露口令登录等。

综上所述，在实战攻防演练活动期间，强化邮件系统安全防护，实现邮件服务器安全防护、邮件信件监测、邮件登录监测、邮件异常发现、邮件漏洞检测、异常 IP 阻断等能力，致使攻击方无法将邮件作为攻击入口，至关重要。

安天实战攻防演练邮件安全监测服务（以下简称“安天邮件安全监测服务”，示意图详见图 4-1），可以有效帮助防守客户单位提升网络防御能

图 4-1　安天邮件安全监测服务示意图

力，达成以下目标：

1) 在准备阶段：开展开源渠道账户收集，发现网内重点被攻击对象。

2) 进入对抗时：通过邮件安全监测服务，发现社工邮件、发现网络入侵、处置已获得桥头堡、追溯攻击方攻击；通过部署的安全工具发现恶意邮件，安全专家深度分析样本，形成分析报告，提供确凿证据与详细分析报告（包含发送时间、IP、详细内容、处置结果等），协助上报攻防演练指挥部，获得加分；对于已发现成功入侵的系统，协助应急处置，获得处置得分；结合样本 IP，联合安天威胁情报中心，溯源攻击方，获得溯源加分。

3) 演练结束后：提供总结报告，协助完成总结工作。

1. 启动阶段：设计方案，制定预案

安天将深入了解防守客户单位业务系统，尽可能多的搜集被攻击目标信息，完成资产管理、配置管理、漏洞管理、身份管理等，做到知己知彼，直击最脆弱的地方。

1) 业务现状：了解邮件系统部署方式、架构、目标用户、规模，涉及到的关键技术等；

2) 资产管理：梳理邮件系统承载的系统软硬件信息，软件及补丁更新升级情况；

3) 配置管理：梳理邮件系统存在的管理员、用户、资产配置信息；

4) 漏洞管理：梳理邮件系统存在的安全漏洞，漏洞修补情况等；

5) 身份管理：梳理互联网公开的邮件账户信息；

6) 安全管理：梳理邮件系统安全策略：口令复杂度要求、口令更换周期、邮件加密策略、签名证书策略、邮件内容审查策略、账户定期清理策略等。

在掌握邮件系统现状基础上，梳理邮件安全防护方案，并根据在演练中可能发生的各种情形，制定响应预案。防护方案侧重于对邮件系统进行安全评估、检测和加固；响应预案则是对在演练中可能遭遇的相关的攻击类事件，如扫描事件、暴力破解事件、钓鱼事件、高危漏洞利用事件、木马事件等做好事前防御；与此同时，针对期间所有发现的安全问题，都及时组织技术专家与监测分析组进行同步处置，并实时上报现场指挥组。

2. 备战阶段：安全加固，有备无患

安天将在邮件系统前部署邮件安全防护系统，部署工作包括：设备上架、软件安装、网络 / 系统联调、安全策略配置和调优、综合测试、安全防护效果验证。实现对邮件来源、登录操作、邮件附件、邮件链接，以及可疑访问、暴力破解、异常二维码、异常图片等进行实时安全检测。

同时，基于启动阶段发现的防守客户单位网络和邮件系统中的存在安全隐患，设计有针对性的安全加固方案，并协助落实安全加固措施；制定加固设备需求清单，收敛暴露面；在邮件服务器开放诱饵邮箱，在网络中设置诱捕信息，并重点监控诱饵邮箱威胁事件，及时发现并阻断任何具有威胁性网络连接、邮件通信的 IP 通信。

在此期间，安天还将为客户开展攻防预演服务，以实战化、专业级的能力和不对实际目标系统进行破坏攻击为底线，进行针对社工邮件、钓鱼邮件、暴力破解邮件账户等场景的实战攻防对抗演练，检验客户协同处置等方面的综合防护能力。进而从安全技术、管理和运营等多个维度着手，进一步发现防守客户单位存在的安全防御能力问题和缺陷，并帮助客户完

善安全体系的建设，提升网络安全保障能力。

最后，安天将进行邮件安全培训，强化防守客户单位的安全管理和员工安全意识。

3. 迎战阶段：监测分析，事件处置

进入实战攻防演练正式对抗期间，安天将为防守客户单位邮件系统提供 7×24 小时值守和监测服务。

结合客户业务场景部署安全产品，全面监测发现威胁与攻击行为，检测内部失陷的主机、内外部存在的攻击、诱饵邮箱，及时发现安全风险，清除威胁，并针对发现的威胁进行分析研判。邮件安全防护设备通过串行部署，实现社工邮件威胁实时捕获和检测，定位威胁源头并监控各种攻击行为；通过对邮件数据、IP 信息、安全事件、运行状态、审计日志、威胁情报等信息的全要素、细粒度的记录，提升对定向攻击、高级威胁的发现和溯源能力，从而达到对潜在威胁、未知威胁的持续安全监测效果。安全专家结合 SaaS 平台对可疑文件采用动静态结合的深度分析方式，有效发现未知威胁，全面揭示分析对象的可疑行为，发现邮件安全事件及隐患。

3.1 对安全监测设备上报的事件进行取证分析

1) 安全事件上报：邮件安全防护系统在发现威胁、异常事件后，将关联日志与恶意数据上报 SaaS 服务平台，交由二线安全服务专家，深度研判。

2) 事件证据收集：对海量数据排查结果并提供可疑线索；对事件的分析预判，对客户系统的具体问题邮件及入侵主机进行定位，对问题主机的关键信息进行取证，包括邮件取证、网络取证、样本取证、日志取证、进程取证、内存取证等。

3) 事件证据生成：预处理后的事件样本，最后经过客户同意，将相应事件取证内容提交云服务平台，进行后续的人工事件分析等。

3.2 事件感染态势研判与恶意样本确认

基于事件前期取证分析的基础上，根据当前态势，对潜在威胁进行预估分析，预判感染数量、感染范围等情况。

3.3 事件样本人工深度分析

安全专家全面针对包括下载、启动、解密、加密、后门、远程控制、信息窃取、注入、劫持、替换、Hook 等功能在内的恶意代码进行语义分析、反汇编等静态分析，并结合系统监控、脱壳分析等动态分析，提取出样本中丰富的动静态信息，进而提供更加专业高效的处置处理方案。

3.4 事件溯源分析

基于事件深度分析的基础之上，利用安天海量病毒数据库和社会工程学、威胁情报分析、海量信息挖掘等手段对样本深度分析的结果进行关联分析，对关键信息进行搜索排查，针对威胁事件进行定位、追溯，并与其他事件进行关联分析，最终确认攻击链（攻击发起者、攻击对象、攻击时间、攻击表现形式、攻击方法等）。

3.5 事件威胁评估

在溯源分析的基础之上，对当前防守客户单位系统可能或者已经遭受的威胁进行说明，明确当前系统已经遭受到的威胁情况，并给出处置方法；同时，也对当前可能面临的潜在威胁进行预判分析。另外，基于网络威胁事件深度分析的基础之上，针对被攻击对象的身份、职责以及其他特别因素，结合样本功能和被窃信息以及攻击手法，分析攻击方的攻击动机，并提供防护方案。

事件处置与体系优化建议是基于事件深度分析基础之上，结合事件威胁评估，对当前客户系统给出相应的威胁处置方案与预防方案，包括手动对威胁事件的清除方案，如有必要可进场清除恶意事件。事件解决方案是事件深入分析中的最后步骤，也是关键的步骤，能为客户构筑良好的邮件应用环境打下坚实的基础。

4. 总结阶段：总结复盘，全面加固

安天将根据演练整体工作情况进行总结，针对演练过程中防守客户单位的邮件系统暴露出的各种问题进行复盘，并制定优化工作目标和工作计划，输出邮件系统安全加固建议。

5. 安天邮件安全监测服务客户价值

在整个攻防演练过程中，邮件安全监测服务可全方位对邮件系统进行安全防护和监测，确保实时对邮件来源、登录操作、邮件附件、邮件链接，以及可疑访问、暴力破解、异常二维码、异常图片等进行安全检测，并及时处置相关事件，进而全面提升邮件安全防御能力，有效抵御攻击威胁。

同时，邮件安全监测服务，可配合探海与安天追影威胁分析系统（以下简称“追影”）交叉部署在攻击方的必经之路上，全方位采集流量，在威胁抵达目标的路径上增加关隘进行智能化威胁响应，做到“关口前移，防患于未然”，让攻击方无所遁形、无处可逃、无计可施；期间，探海还可联动追影将还原的文件载荷进行深度分析，实现漏洞触发、细粒度行为揭示和威胁情报的输出，有效提升对未知威胁的发现、监测、阻断能力；最终，帮助客户构筑动态综合的网络安全纵深防御体系。

在 2022 年大型实战攻防演练活动中，安天邮件安全监测服务为某客户单位监测分析钓鱼邮件攻击时间 10 余起，溯源加分 720 分。

05 网站安全防护：以佚待劳

由于 DMZ 区面向公网开放，且无论是在日常时期还是在攻防演练期间，其承载的网站类应用一般都是可以被包括攻击方在内的公众访问的，也就形成了《孙子兵法·地形篇》中提到的“我可以往，彼可以来”的“通”，即我们可以去，敌人也可以来的区域。因此，攻击方势必会利用这种“优势”，通过信息收集、弱口令暴力破解、泄露凭证登录、webshell 投递、漏洞利用和创建 shell 等手段，通过 DMZ 区网站群向内网进行渗透。

《孙子兵法》针对“通”的对抗形势，也提出了“通形者，先居高阳，利粮道，以战则利”的应对办法。放在实战攻防演练对抗场景中，就是指防守方必须要事先加强 WEB 应用访问控制、漏洞利用检测和服务器终端威胁检测等方面的安全能力，通过全面的提升网站安全防护水平，配备足够的对抗资源（安全产品和安全专家）并形成有利的对抗态势，养精蓄锐，才能有效防御攻击方利用网站发动攻击，获得优势。

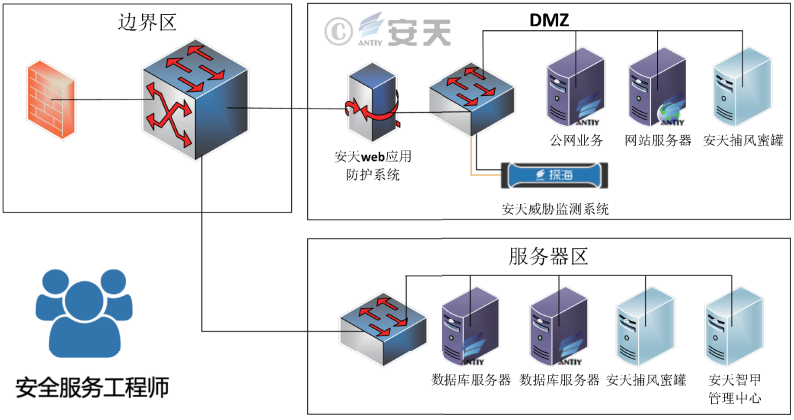


图 5-1　安天网站安全防护服务示意图

安天实战攻防演练网站安全防护服务（以下简称“安天网站安全防护服务”，示意图详见图 5-1），采用托管模式，可针对防守客户单位网站的安全性与可用性进行全面监测，针对影响网站及系统运行的安全隐患进行实时监控，监控内容包括网页篡改、挂马、暗链、域名劫持、后门、关键字等。服务基于安天安全产品防御能力结合安全专家现场响应共同支撑，可以帮助客户在短时间内发现网站存在的安全问题，并通过监测报告定制安全策略，调整相应安全措施，从而极速提高网站的安全防护水平，极大降低在攻防演练活动期间因网站安全缺陷或漏洞造成的失分风险。

安天网站安全防护服务，可为防守单位客户提供覆盖攻防演练“启动、备战、迎战、总结”全生命周期的解决方案。

1. 启动阶段：资产梳理，制定预案

安天将通过开展网站群资产细粒度梳理，制定网站安全应急事件处理和应对措施。

首先，安天安全专家将通过资产安全运维平台或其他扫描工具识别演练期间上线系统的关联资产；其次，通过现场调研的方式，利用资产调研表对扫描后的资产信息进行对比、合并、除错，补齐资产的详细信息；然后，对安全管理人员、网络管理人员、主机系统管理人员、应用开发和维护人员进行访谈，明确资产责任人；最后，针对演练中可能发生的扫描类、暴力破解类、高危漏洞利用类和木马类等安全事件，制定网站安全应急预案。

2. 备战阶段：部署产品，加固防御

通过安天智甲云主机安全监测系统（以下简称“智甲云主机”），开展安全配置核查，发现网站存在的安全漏洞和后门程序，协助落实加固措施；梳理公网开源账户及泄露口令，使用口令枚举、泄露凭证登录等方式评估口令安全状态，从事前分析并管理其中的潜在安全风险，提前防范风险并提高攻击门槛。同时自动学习梳理各业务之间的访问关系，使用微隔离将

各业务系统做不同细粒度的隔离策略，收敛业务暴露面减小攻击影响。

同时，安全专家结合漏洞扫描与渗透测试，发现网站存在的安全漏洞；通过部署安天下一代 WEB 应用防护系统（WAF）、安天应用威胁自免疫工具（Antiy RASP）与智甲云主机，实现流量侧与终端侧威胁捕获能力、威胁诱捕能力，通过安天智甲终端防御系统（以下简称“智甲”）安全管理中心收集 WAF、智甲防护客户端和流量监测设备日志，实现综合研判，发现入侵威胁。

3. 迎战阶段：实时响应，争取加分

通过人工监测威胁感知设备，发现针对 DMZ 网站的网络探测和网络入侵。对于发现的 Webshell、木马，安天安全专家将深度分析样本并形成分析报告（分析报告包含发送时间、IP、详细内容和处置结果等）。同时，协助客户上报分析结果至演练指挥部，获得加分；对于已发现成功入侵的系统，协助应急处置，获得处置得分；结合样本 IP，联合安天威胁情报中心，溯源攻击方，获得溯源加分。

4. 总结阶段：协助总结，提交报告

针对发现的网站攻击事件、发现的威胁文件提供总结报告，协助客户完成总结工作。

5. 安天网站安全防护服务客户价值

1) 预警网络攻击，使用威胁情报（TI），先攻击方一步而消除攻击威胁；

2) 检测并阻断网站威胁，积极应对各类攻击手段；

3) 超过 10 年实战经验安全专家支撑，助力调查溯源帮助获得加分。

在 2022 年大型实战攻防演练活动中，安天网站安全防护服务为某客户单位阻断 Web 攻击事件近 3 万起，监测入侵蜜罐事件 11 起，溯源加分 400 分。

06 网络边界防御：可使无斗

在实战攻防演练对抗中，攻击方对内网的攻击不可避免会通过网络边界。一般会利用系统的已知漏洞、未知漏洞或采用多种攻击 IP 组合作业等综合的体系化的攻击策略，对防守客户单位的网络构成强大的威胁；进而通过覆盖扫描、入侵、命令与控制、横向移动等攻击手段完成入侵。

因此，在攻防演练活动期间，防守方就必须要对网络边界流量进行深度监测分析，实时发现网络异常、漏洞利用、恶意 IP 和恶意文件，并联动防火墙及时对攻击方攻击 IP 进行阻断。通过动态综合的网络边界防御体系与制针对性的防护策略，全面阻断通过网络边界的攻击，致使攻击方不知从何攻击，不知如何攻击。犹如《孙子兵法·虚实篇》中提到的“善守者，敌不知其所攻”一样，才能有效应对攻击方对内网的威胁，降低失分风险。

图 6-1　安天网络边界监测服务示意图

针对防守客户单位在实战攻防演练中的网络边界防御场景，安天制定了实战攻防演练网络边界专项监测服务（以下简称“安天网络边界监测服务”，示意图详见图 6-1）。通过安天探海威胁检测系统进行网络全流量的

安全检测，可发现网络边界安全漏洞与异常流量并进一步提交安全专家威胁猎杀，精准定位攻击 IP，实时阻断攻击 IP。通过安全专家分析研判的攻击 IP 信息，生成面向客户的定制化威胁情报，进而将威胁情报 IP 地址同步至总部与二级单位的防火墙、WAF 和 IPS 等具备阻断功能的安全设备。

安天网络边界监测服务在实战攻防演练期间，可及时发现攻击方通过网络边界发起的威胁行为，实时阻断攻击，降低失分风险。

1. 启动阶段：定制防护方案

首先，安天会与客户深度沟通，深入了解开放服务系统业务现状及边界部署位置，梳理公网开放系统承载的资产信息和安全漏洞，形成网内对外开放服务的资产列表、域名列表和漏洞列表，进行资产管理和漏洞管理；然后，制定《网络边界监测分析防护方案》，对威胁情报详细分析，并就各类情报采取的预防措施，与防守客户单位人员协同进行流程和策略设计。

2. 备战阶段：部署安全产品

部署探海和安天下一代 WEB 应用防护系统（WAF），对网络边界流量进行深度分析，建立流量基线。通过探海以网络流量为检测分析对象，实现对网络扫描探测、远程漏洞利用、攻击载荷投放、僵尸网络活动、病毒扩散传播和木马远程控制等网络行为的检测和告警，精准检测已知海量恶意代码和网络攻击活动，有效发现网络可疑行为、资产和各类未知威胁。

3. 迎战阶段：封堵攻击，溯源得分

通过探海和 WAF，发现网络扫描、漏洞利用、异常流量和恶意文件，追溯攻击，形成威胁情报表单和详细分析报告。分析报告包含发送时间、IP、详细内容和处置结果等。同时协助客户封堵恶意 IP、向现场安全专家同步受入侵情况、开展取证分析，并将分析结果上报演练指挥部，从而帮助客户获得加分。

4. 总结阶段：分析总结

按启动阶段制定的工作目标和工作计划，根据客户具体需求输出《网络边界威胁检测分析总结报告》，阐述网络边界威胁监测及处置情况、威胁情报分析及预警成果。

5. 安天网络边界监测服务客户价值

1) 分析研判设备告警与可疑文件，监测客户网络中的各类安全事件；

2) 有效发现未知威胁，揭示分析对象的恶意行为，跟踪各类高级威胁和定向攻击；

3) 梳理并分析现网安全状况；

4) 监督网络安全制度落实情况，降低重大安全事件发生的风险；

5) 检测各类网空威胁，生成定制化威胁情报；

6)10 年以上经验安全专家团，助力调查溯源帮助得分。

在 2022 年大型实战攻防演练活动中，安天网络边界监测服务发现网络攻击事件高达近 80 万起，并有效阻断各类攻击行为。

07 终端威胁检查：乱生于治

如今，各个行业单位的业务系统经过多年的信息化建设，内部的终端数量也随之增多，导致安全管理的难度成倍增加。由于整个网内终端及其承载的系统、应用、数据的数量非常庞大，且部署架构相对错综复杂，一旦疏于管理，终端就容易成为整个信息系统安全体系中的明显薄弱环节，甚至被攻击方当作突防入口进行攻击与利用。特别是在实战攻防演练活动期间，终端始终都是攻击方重点攻击的目标。

《孙子兵法·势篇》有云“凡治众如治寡，分数是也；斗众如斗寡，形名是也”，是指治理大军团就像治理小部队一样有效，是依靠合理的组织、结构、编制；指挥大军团作战就像指挥小部队作战一样到位，是依靠明确、高效的信号指挥系统。

在实战攻防演练对抗场景中，如果把防守单位的终端看作是“大军团”，那安全管理就必须要是“合理的组织、结构、编制”与“明确、高效的信号指挥系统”，只有这样，防守方才能提高整个终端的防御能力，确保有效应对攻击方针对性的攻击威胁，真正降低失分的风险。

安天在“敌已在内”的敌情想定安全思想指导下，针对实战攻防演练期间，终端可能遭遇的各种攻击威胁的场景，制定了安天实战攻防演练终端威胁专项检查服务（以下简称“安天终端威胁检查服务”，示意图详见图 7-1）。安天首先会通过开展一系列针对终端威胁的检测工作，来避免攻击方在演练前实施预攻击；其次，是在演练正式开始前清除网内存留的威胁，避免在正式演练过程中，大量与演练无关的告警消耗值守人员精力。同时，通过部署智甲和智甲云主机，能够现场针对防守客户单位网络环境内的信息资产进行实时威胁检测、威胁取证、威胁清除工作。

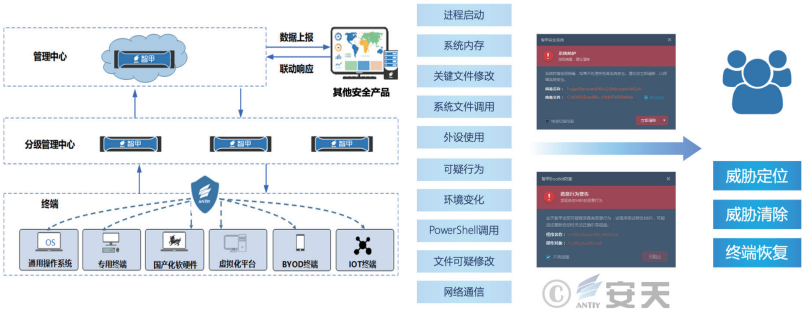


图 7-1　安天终端威胁检查项服务示意图

智甲管理中心可实现多类型终端一体化管理，能够实时了解网内终端安全情况，并可查看安全事件详情。同时，针对主机内的文件、程序行为、网络流量等支持威胁检测，可对发现的威胁对象或攻击行为进行清除和拦截，减少主机风险使用行为。一旦发现可疑威胁行为，可实时对攻击进行以“人”为主导的调查和反制；针对高水平攻击方有目的的威胁动作，可快速定位目标主机，并通过多种防护和管控功能进行发现、溯源、反制和形成价值情报，全面保障客户的信息系统与数据资产安全。

安天终端威胁检查服务可覆盖攻防演练全生命周期终端安全防护。

1. 启动阶段：清除潜在威胁，提前防范风险

在攻防演练对抗中，攻击方会使用多种攻击手段对主机进行入侵，如漏洞利用、暴力破解、摆渡攻击等，但无论使用何种手段，攻击方通常都要利用主机的暴露面达成连接，利用资产脆弱性获得执行攻击行为的资源。因此，在攻防演练开始前，就要对主机的暴露面、脆弱性、合规性等风险进行排查和处置。

所以，在攻防演练活动的一开始，安天就将为防守客户单位网内所有主机安装智甲，通过管理中心实现多类型终端一体化管理，帮助管理人员了解网内终端安全情况，查看安全事件详情；同时，通过智甲管理中心下

发指令统一对网内所有主机进行威胁排查，排查潜伏在主机上的高危文件和行为。

对于网内所有物理服务器、虚机、云主机等工作负载，运用智甲云主机，以前期摸清家底是安全防护的前提，通过自动化资产清点（兼容容器资产），帮助客户快速追踪、定位、研判受威胁的资产，协助客户开展针对性的资产审查。另外，主机内风险排查也是备战阶段不可缺少的一部分，通过智甲云主机持续识别主机的资产脆弱性（兼容容器），如：软件漏洞、弱口令、关键配置错误等，分析并管理其中的潜在安全风险，提前防范风险并提高攻击门槛，可有效减少主机 90% 被攻击面。

2. 备战阶段：全面安全加固，提高攻击门槛

安全专家将借助以上两套终端防御系统，为防守客户单位提供暴露面梳理、脆弱性检测服务，检测方法包括基线检查、漏洞扫描、渗透测试等，同时还提供威胁检测与处置服务。安全专家基于检测发现的网络和系统中的安全隐患，为客户提供安全加固，即根据客户的安全风险定制有针对性的安全加固方案，并协助客户落实。通过上述手段，全面提高主机安全性，使攻击方的攻击行为无法轻易达成。

3. 迎战阶段：实时安全监测，及时分析处置

智甲支持对各类木马、蠕虫、宏病毒、WebShell 等恶意代码进行实时安全监测，及时发现并处置在演练期间内网主机新出现的恶意文件和威胁行为。同时，智甲具有内核级防护能力，可对环境篡改、恶意代码执行、提权、启动项创建等行为进行拦截，使攻击方难以利用恶意代码对主机环境进行入侵和破坏。并将实时针对突发情况，进行事件分析和应急处置。

智甲云主机则提供多维度的入侵检测，快速发现和定位网络资产中的入侵事件以及失陷主机，提升安全分析与响应能力。从异常行为维度，通过全量行为检测引擎梳理出主机内异常文件、异常进程、异常网络连接等

可疑行为：

1) 从主机日志审计维度，对系统 / 应用全量日志进行采集分析，为入侵检测提供数据源；

2) 从威胁事件维度，通过内置威胁检测引擎 + 威胁情报，对采集到的数据做聚合分层分析有效安全数据，实现对工作负载中的各种安全事件与攻击指标进行快速研判和处置。

针对期间遭受的网络安全事件，可根据客户需求开展深度威胁事件响应。首先，根据事件特征以及安全设备监测结果快速定位可能存在风险的主机并进行取证分析；其次，通过预编排事件调查能力对可疑样本进行动静态分析、溯源分析、事件威胁评估；最后给出事件处置与体系优化建议。期间将进行持续性的威胁猎杀，威胁猎杀服务主要由五大子服务组成：

1) 威胁检测子服务：通过终端侧数据采集，发现当前设备存在的潜在风险；

2) 威胁巡检子服务：实时开展人工深度分析，发现网内异常数据，人工甄别研判；

3) 人工调查分析子服务：根据攻击方动机形成画像，提供知识情报；

4) 应急处置子服务：针对发现存在的安全威胁，采取缓解、抑制、根除措施；

5) 专杀开发子服务：对发现的威胁分类汇总、危害评估，并进行专杀工具的开发。

4. 总结阶段：全盘梳理分析，全面总结成果

在演练工作结束后的总结环节，安天将为客户复盘演练期间的攻防情况，对演练期间攻击成功的事件和防守成功的事件进行复盘。对事件原因、响应流程、处理方法、造成的后果等进行梳理和分析，并对所有产生的问题和情况提出合理高效安全的解决办法。全面总结终端威胁检查服务工作

成果，输出《终端威胁检查总结报告》。

期间，智甲云主机可通过自主算法将具有关联的多条告警生成一条入侵事件，按照时间顺序还原攻击过程，并以图形化的方式呈现攻击方入侵链路全景图，帮助安全人员识别攻击方使用的技战术以及触发的检测点，支撑安全事件的溯源调查。

5. 安天终端威胁检查服务客户价值

5.1 技术方面

1) 及时发现终端内的已知威胁与未知威胁；

2) 发现定向终端攻击，切断并清除攻击；

3) 治理网内恶意代码与网络攻击；

4) 通过威胁猎杀、攻击方画像、溯源、攻击动机分析形成私有情报和知识库；

5) 基于主动防御有效保护客户信息资产，有效降低失分风险。

5.2 管理方面

1) 指导作用：通过猎杀过程，“有的放矢”指导安全管理及技术体系改进。

2) 监督作用：帮助监督安全管理制度的落实情况，发现违法、违规行为。

3) 考核作用：检查结果作为证据，促进安全管理考核落地。

4) 提升作用：提升客户安全运营团队威胁发现与应急响应等能力。

在 2022 年大型实战攻防演练活动中，安天终端威胁检查服务为某客户单位排查发现终端威胁文件 200 余个（其中远控木马 18 个），并成功清除终端威胁隐患。

08 威胁诱捕分析：诱敌深入

“善动敌者，形之，敌必从之；予之，敌必取之；以利动之，以卒待之”是《孙子兵法·势篇》中的重要战术思想，是指在对抗中善于“调动”敌军的人，向敌军展示一种或真或假的军情，敌军必然据此判断而跟从；给予敌军一点实际利益作为诱饵，敌军必然趋利而来，从而被本方牵制。

随着网络环境日益复杂化，网络攻击行为趋于产业化，攻击手段也愈发多样化，根据经验构建防御策略、部署产品的传统方式在面对层出不穷的新型、持续性、高级威胁时，难以及时有效的检测、拦截、分析和响应。特别是在实战攻防演练这种高烈度的对抗场景中，防守方并有太多的办法可以让攻击方停止攻击，因此，就必须要采用一些“非传统的新型”防护方法来提升攻击方的攻击成本和门槛，或致使其进行无效攻击，从而降低攻击的数量和质量，进而释放出更多的防护资源去做更有针对行的对抗动作。即《孙子兵法·势篇》中同时提到的“凡战者，以正合，以奇胜”，即用“奇兵”去出奇制胜。

在实战攻防演练对抗场景中，防守方通过构建欺骗式防御体系，就是上述两大重要战术思想的落实体现。通过主动投放“利益”作为诱饵，诱导攻击方对设有“陷阱”的仿真虚假资产目标进行攻击，并进行威胁捕获，进而对事件深度分析、研判并反制，以守转攻，实现从被动防御向主动防御的转变，从而有效保护真正资产，即是提升防御能力，降低失分风险的妙计。

安天实战攻防演练威胁诱捕分析服务（以下简称“安天威胁诱捕分析服务”，示意图详见图 8-1），是为满足防守客户单位实战攻防演练高烈度对抗场景需求，基于捕风和追影制定的欺骗式防御体系。可有效提升防

守客户单位的威胁防御能力，及时发现网内未知威胁，争取被攻击后的响应处理时间，掩护真实的信息资产。通过自带的反制措施及溯源分析，形成自有情报的积累；诱捕到攻击方的丰富信息，做到清晰“知彼”。

同时，可从内网、外网、隔离网等场景捕获威胁，生成针对威胁事件、攻击链等攻击行为的溯源信息，协助客户及时发现安全风险、清除威胁，并提供修复建议，保障网络与系统能够安全、稳定、持续的运行。

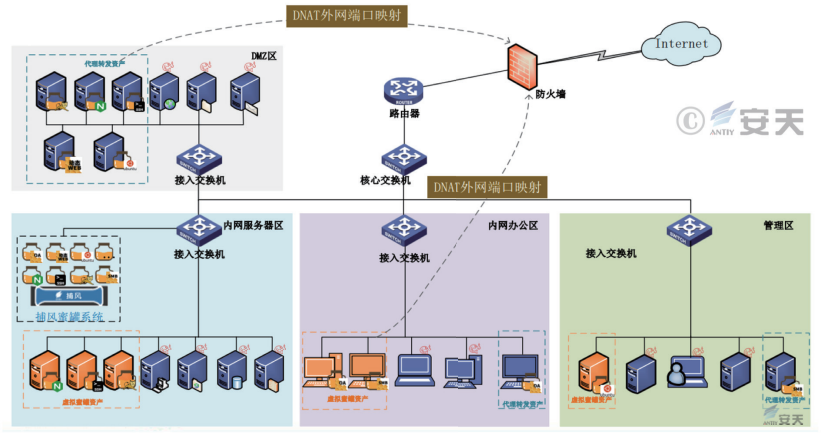


图 8-1　安天威胁诱捕分析服务示意图

安天威胁诱捕分析服务可覆盖攻防演练全生命周期信息系统安全防护。

1. 启动阶段：事先部署产品，及时获取线索

在实战攻防演练对抗场景中，防守方需要面对攻击方持续多维的攻击，充分的了解攻击方的整体情况，才能根据攻击特点建立完善的安全防护体系。所以，需要在事前部署捕风和追影，协助防守客户单位及时获取攻击方的关键性“线索”。

2. 备战阶段：拆解攻击链路，部署蜜罐诱捕

攻击方在入侵攻击之前，通常会制定攻击策略、规划攻击线路、明确

分工合作，力争在最短时间内取得最大战果（详见图 8-2），常见的攻击链条分为三个阶段：

图 8-2　攻击方思路导图

1) 情报收集：搜集关于目标组织的人员信息、组织架构、网络资产、技术框架及安全措施信息，为攻击决策提供支撑；

2) 建立据点：通过分析漏洞，发起定向攻击，同时也会对目标现有安

全措施进行突破；

3) 横向移动：通过在被攻陷的目标内网进行横向移动，尽可能的获得更多权限；同时，对目标进行内网情报收集，主要包括当前主机情报与内网扫描探测情报。

针对上述攻击链条与思路，可利用捕风在互联网部署 ERP、OA、VPN 系统、虚拟化桌面系统、邮件服务系统等高交互蜜罐资产，并且选择部分蜜罐资产预置不同的弱口令、漏洞等诱骗攻击方；同时散播虚假信息“蜜饵”，干扰攻击方收集情报，使其选择攻击目标时产生误判，指数级地增加攻击方的攻击成本，延缓攻击进程的同时，将攻击方不断诱导引入蜜罐陷阱，从而诱捕攻击方，保护真实资产。

3. 迎战阶段：五大防御动作，有效牵制攻击

在实战攻防演练正式对抗期间，安天将通过五项重要防御动作，有效牵制攻击方。

3.1 产品运行及安全状态监测

通过捕风和追影开展周期性的检查，可实时了解整体的网络状况，及时发现网络中存在的问题，快速有效的制定相应的安全处置策略，从而降低网络中的安全威胁。巡检包括但不限于：

1) 安全设备状态检查：对网内设备进行健康状态检查，包括系统引擎、CPU 占用率、内存占用率、接口状态、证书授权状态等内容。

2) 安全日志分析：定期为客户信息系统内安全设备产生的日志进行挖掘和分析，从事件类型分布、事件发展趋势、事件频率、源地址、目的地址等五个维度进行详细梳理，发现潜在的风险点，并提供分析报告，及时掌握网络运行状态和安全隐患。

3.2 设备告警分析

对威胁事件深度分析、研判并反制，具体步骤为：

1) 事件证据收集

2) 事件证据识别

3) 事件证据生成

4) 事件感知、态势的研判与恶意样本确认

5) 事件样本人工深度分析

6) 事件溯源与反制

3.3 威胁排除

在溯源反制的基础之上，通过事件威胁评估明确防守客户单位信息系统安全情况，对已发生的威胁及时处置，对可能面临的潜在威胁进行预判分析，提前防御。事件威胁评估基于网络威胁事件分析，针对被攻击目标的身份、职责以及其他特别因素，结合样本功能和被窃信息以及攻击手法，分析攻击方的攻击动机，并提供有针对性的防护方案。

3.4 威胁清除

1) 分析清除：根据对系统威胁预警的研判结果，进一步开展溯源或策略优化工作。如果威胁预警存在误报则优化其相关安全策略；如果威胁预警真实存在，则根据攻击行为采集功能，确定客户受影响的范围以及主机，并对攻击方遗留的攻击痕迹进行清除，痕迹包括但不限于后门、启动项修改、命令行修改等。

2) 安全加固：根据威胁多维度的展示功能，从多角度、多方位来制定相应合理的安全加固方案，清除客户目前存在的安全风险。方案包括但不限于客户架构、管理方式、人员安全素质、技术手段等。

3.5 策略调优

根据网站监测误报情况、近期漏洞通报情况对客户相关安全策略进行优化升级。

4. 总结阶段：回顾演练全程，输出分析报告

在总结环节，安天将对演练期间攻击成功事件和防守成功事件进行复盘，并根据演练过程中的工作记录，回顾演练工作的全过程，整理与安全事件相关的各种信息，全面总结服务工作成果，输出《威胁诱捕分析总结报告》。

5. 安天威胁诱捕分析服务客户价值

1) 全网威胁诱捕：对客户目标资产进行探测并利用空闲 IP 资源自动创建仿真资产，充分扩大威胁感知范围，及时了解客户整体网络安全态势，降低安全风险，保障自身业务可持续性。

2) 保护真实资产：明确业务系统安全现状，分析当前应降低的安全风险，保持蜜罐资产与环境资产高度仿真，使攻击方真假难辨。

3) 增强诱捕能力：检验信息安全基础设施的有效性，针对发现的安全隐患提供专业解决方案，用仿真资产代理取代真实资产暴露在网络中，使攻击认为攻击的是真实系统。

4) 赢得响应处置时间：投放“诱饵”，将攻击方引致蜜罐中，拖延攻击方时间和精力，为安全加固和溯源赢得宝贵时间。

5) 情报生成与溯源能力：对各安全设备进行安全事件日志分析，通过关联分析，使安全事件有理有据，还原安全事件链条。

在 2022 年大型实战攻防演练活动中，安天威胁诱捕分析服务为某客户单位捕获攻击事件 70 余起，溯源加分 900 分。

09 靶标系统防护：靶标如磐

在实战攻防演练活动期间，靶标系统从始至终都是防守单位整体防守工作的重中之重，在攻防对抗过程中倘若靶标系统一旦失守，防守单位将直接面临沉重打击，甚至因此带来牵一发而动全身的全面败退。可以说，靶标系统防护策略与防御体系的完备程度，对防守单位的最终演练成绩有着最直接的决定性影响。

所以，针对这一事关胜负的“关键阵地”，攻击方势必会无所不用其极的利用各种攻击手段，极尽所能展开风行雷厉的攻击。因此，防守方就必须要通过全面布防基础安全产品防御能力联动安全专家现场响应能力，构筑起动态综合防御体系，并以《孙子兵法·军争篇》所述之“其疾如风，其徐如林，侵掠如火，不动如山，难知如阴，动如雷震”重要战术素养“风林火山”展开对抗态势，力保靶标系统坚如磐石，牢不可摧，方能确保立于不败。

安天作为引领威胁检测与防御能力发展的“网络安全国家队”，依托前沿安全理念的安天防御框架（ISPDR），基于近二十三年的高级威胁对抗经验、自主先进核心技术的产品生态体系、千万级情报数据的威胁情报、亿级病毒特征库的威胁检测引擎、以及国家级应急支撑经验的威胁猎杀等“能打仗，打胜仗”的安全实战能力，结合在多年实战攻防演练活动中为政府、教育、交通、金融、通信、能源电力等重要行业客户执行防守任务的安全实战经验，针对靶标系统的防护，定制了以实战化、体系化、常态化的能力型网络安全防御体系建设思想的专项精细化防守解决方案：安天实战攻防演练靶标系统防护专项服务（以下简称“安天靶标系统防护服务”，示意图详见图 9-1）。可实现动态防御、主动防御、纵深防御、精准防护、

整体防控、联防联控的安全防护效果，为防守客户单位在攻防演练过程中的组织和防护提供有效保障，力保靶标系统不被击破。

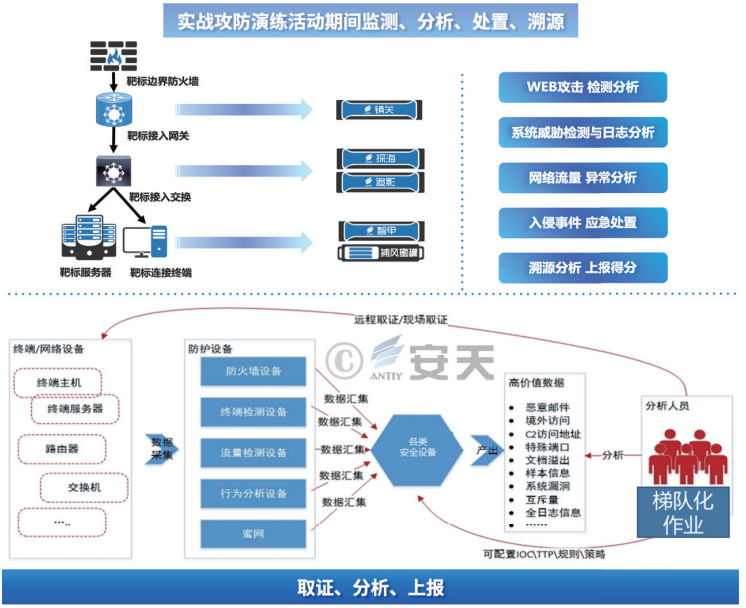


图 9-1　安天靶标系统防护服务示意图

安天靶标系统防护服务可支撑攻防演练全生命周期靶标系统安全，不被攻陷。

1. 启动阶段：上报靶标系统，健全协同体系

安天首先会协助防守客户单位根据网络现状和业务场景确立并上报靶标系统，然后进行靶标系统关联信息资产梳理和网络安全防护现状调研，并同步协助建立健全攻防演练组织和管理规划，明确演练期间的各项工作机制，最终形成全面的靶标系统防护工作部署方案。

2. 备战阶段：细化安全方案，深入攻防预演

安天将协助防守客户单位做好靶标系统的全面资产、配置、漏洞、补

丁梳理工作，并同步进行风险排查，确保在进入正式对抗前发现、清除潜在风险并做好安全加固：

首先，组织安全专家团队通过基线检查、漏洞扫描、渗透测试等手段为靶标系统提供脆弱性检测服务，并协助客户对靶标系统进行漏洞修复、安全加固和策略优化。

其次，进一步对承载靶标系统的主机进行威胁检测与处置。

同时，根据客户实际情况，针对靶标系统制定专项防护方案，并在多个关键节点部署含安天核心技术的自研安全产品，包括安天下一代 WEB 应用防护系统、捕风等。若靶标系统已上云，也可由智甲云主机进行防护，切实做到全方位有效保护靶标系统安全。

最后，在演练正式开始前，协同客户制定演练期间的靶标系统安全监测值守方案，并确保方案可有效落地执行；在演练临近时，组织多场景的攻防预演，以此验证安全加固和优化工作的有效性、各项工作机制的可操作性、安全产品的检测和监测能力，以及防守人员间的协同配合程度。

3. 迎战阶段：全时安全值守，实时应急处置

安天将基于自身的威胁情报分析平台和威胁捕获系统为防守单位提供专项威胁情报，并集中优势力量基于自研安全产品和客户已有的第三方安全产品，为靶标系统提供 7×24 小时的安全监测值守服务。

安全监测值守期间，组织专项团队对靶标系统相关的安全告警和威胁情报等进行分析确认，在确认发现安全事件时，安天将及时协调安全专家进行事件分析与应急处置，并协调相关资源进行追踪溯源，协助防守客户单位撰写防守成果报告并及时向上反馈，获得加分。

4. 总结阶段：梳理工作成果，输出总结报告

演练结束后，安天将全面总结演练期间涉及靶标系统的防护工作和成果，输出《靶标系统防护总结报告》。

5. 安天靶标系统防护服务客户价值

1) 专项威胁情报：通过安天威胁情报分析平台和专项威胁情报服务，可为防守客户单位提供攻防演练期间的高价值威胁情报，助力靶标系统安全防护。

2) 专业防护方案：安天为防守客户单位针对靶标系统制定专项防护方案，从“边、端、人、体系”等多方面为靶标系统制定细粒度的防护措施，通过全方位的风险检测和加固优化，全面提升靶标系统安全属性。

3) 全程监测值守：安天在攻防演练期间通过对靶标系统进行 7×24 小时的实时安全监测值守，可快速发现威胁事件，并及时协调安全专家力量进行研判处置和追踪溯源，收集相关证据并形成防守成果进行上报，力保靶标系统不失守的同时获得加分。

4) 经验积累与知识传递：攻防演练结束后安天将协助防守客户单位总结靶标系统的防守内容和成果，将靶标系统的防守优势推广到全网，形成实战化、体系化、常态化的动态综合防御体系。

自 2016 年以来，由安天提供防守服务的靶标系统均未被攻破。

10 结语

网络安全实战攻防演练活动是目前通过发现各行业重要信息系统的安全风险与隐患、考察网络安全责任落实情况、检验防守单位的安全防护能力，进而系统提升安全防护水平和技术对抗能力的重要手段。安天基于近二十三年持续参与重大应急响应支撑的专业积淀，提供的实战攻防演练保障服务，经过连续多年在攻防演练活动中为国家部委、能源电力、交通运输、金融、大型国企等客户单位执行防守任务的安全实战验证，不仅可有效帮助客户不丢分、少失分，争取多加分，在保障客户的安全信誉的同时，更能支撑客户构筑起能抵御复杂攻击和应对高级威胁的动态综合防御体系，共同达成有效安全价值。

微信扫描右侧二维码，即可观看 2023 安天网络安全实战攻防演练系列视频。

《2023 安天实战攻防演练防守指南》

《实战攻防演练的十大防守要点盘点》

《实战攻防演练的七大防守成果概览》

11 附录：关键产品价值简介

安天充分发挥下一代威胁检测引擎和安全内核的基础优势，自主研发了可覆盖信息安全领域全场景的安全产品生态体系，为攻防演练防守任务的落地与实施提供了更直接、更便捷、更有效的安全实战支撑。安天多款产品可实现威胁情报协同共享，有效拓宽防御覆盖面与纵深度，共同发现和阻断攻击。

2023 年安天产品攻防演练防守实战价值列表

防护类别	安全产品	产品价值
威胁统一监控与处置	安天可扩展威胁检测响应平台 XDR（安天 XDR）	安天 XDR 是通过平台化整合对接端、网等安全产品，采集遥测数据进行深度关联分析，实现对网内威胁的智能发现，并还原攻击事件，帮助用户高效完成调查处置的统一的安全运营系统。在攻防演练实战场景中，平台能够满足对网内威胁的集中监控，并通过安全数据的智能关联分析和多设备联动处置，提高威胁发现和预警能力、提升威胁处置效率。
终端防护	安天智甲终端防御系统（EPP+EDR）	智甲是安天自主研发的终端安全防护产品，拥有资产管理、威胁防护、主机管控、安全响应等多种管控与防护能力，可以有效保障用户的系统与数据安全。在攻防演练实战场景中，事前可帮助用户对主机身份、资产配置、暴露面、脆弱性等关键部位进行排查和处置，并通过端点安全统管加固防御能力，使攻击者难以获得攻击入口，无法执行攻击行为；事中可支撑用户对主机进行全方位的实时监控，并及时拦截、清除和处置各类恶意代码、攻击工具、入侵与破坏行为，致使攻击难以突防，保障主机不被攻陷。同时，智甲创新升级的可编排调查能力，能快速定位风险主机，实现安全事件的快速响应，缩短风险隐患的窗口时间。

2023 年安天产品攻防演练防守实战价值列表		
防护类别	安全产品	产品价值
云主机防护	智甲云主机安全监测系统	云主机安全监测系统针对各种异构、海量的主机、虚拟主机、容器等工作负载，可提供包含资产清点、风险评估、合规基线、微隔离、入侵检测、防病毒、威胁猎杀、威胁溯源等多种安全能力的统一安全防护。通过细粒度的资产清点和持续的风险监测与分析，主动发现业务系统的资产脆弱点，并基于微隔离的精细化访问控制，收敛业务暴露面减小攻击影响；同时运用多维度的入侵检测，快速定位发现入侵行为并追踪还原攻击入侵路径，实现自动化入侵检测响应闭环。在攻防演练实战场景中，可高效支撑现代混合数据中心架构下的主机安全需求，协助用户建立符合组织内部规范的云安全管理平台。
全流量威胁检测	安天探海威胁检测系统（NDR）	探海基于自研的多维度检测引擎，能够精准检测出已知海量恶意代码和网络攻击活动，有效发现网络攻击行为、高危资产和各类未知威胁，如恶意邮件、可疑外联等恶意行为；同时，与安天威胁情报服务的结合，可对攻击者、攻击载荷、攻击组织进行有效的监控，发现具有针对性的攻击活动；基于与防火墙的联动，可以实现威胁发现后的及时阻断，减少威胁事件的影响面。在攻防演练实战场景中，探海可帮助用户及时全面的发现威胁，并进行有效的溯源分析与响应处置，实现不失分、少丢分、多拿分。
威胁分析	安天追影威胁分析系统	追影借助包括安天下一代检测引擎在内的多组鉴定机制组合对输入对象进行判定分析，可有效检出分析鉴定各类已知与未知威胁，尤其对基于格式文档的 0Day 漏洞攻击具备优秀的检出能力，深度揭示威胁行为细节，输出详实报告。在攻防演练实战场景中，追影可有效检出高级威胁，并与安全产品联动，增强整体安全防护能力。

2023 年安天产品攻防演练防守实战价值列表		
防护类别	安全产品	产品价值
威胁捕获	安天捕风蜜罐系统	捕风是部署在网络环境中用于诱骗攻击者的设备级主动防御型网络安全系统，内置多种流行服务和漏洞，支持全场景仿真模拟诱骗。捕风创建的仿真环境在吸引攻击者注意力，保护真实资产的同时，可以及时感知攻击并进行预防，能够捕获攻击者利用的攻击工具并记录攻击全过程。在攻防演练实战场景中，捕风可诱捕攻击方的攻击行为，获取攻击者社交 ID、设备指纹等信息，建立攻击者画像，为反制攻击方提供有效支撑。
威胁情报	安天威胁情报综合分析平台	安天威胁情报综合分析平台可以有效支撑安全事件分析工作，针对攻击者的攻击工具、攻击资源、攻击手段进行全面揭示，形成追踪溯源的能力，最大程度地减少搜集情报和威胁分析时间。该平台集成探针进行联动和采集，能够高质量联动多种安全产品。客户可以将不同安全产品作为消费情报的节点，对该节点的情报命中进行检测和响应。也可以将各节点作为威胁信息生产点，在本平台上结合自带情报进行调查分析。在攻防演练实战场景中，把检测和响应的情报知识第一时间下发至客户的防御体系。
应急处置	安天拓痕应急处置工具箱	拓痕作为便携式工具，内置安天下一代威胁检测引擎，集成了安天多年系统安全监测与处置、流量安全分析、恶意代码行为分析及应急响应积累的技术和能力，能够实现安全运维的日常检查和快速的应急处置。在攻防演练实战场景中，拓痕可协助安全分析人员快速取证，高效定位事件目标，为应急处置提供支撑。
边界阻断与入侵防护	安天镇关下一代防火墙	镇关防火墙从用户、应用和行为的角度出发，在传统防火墙功能基础上，提供用户策略、应用策略和行为策略等智能控制手段，有效解决了传统防火墙无法解决的问题。在攻防演练实战场景中，镇关可以有效的补充边界防护，在边界形成综合的深度防御，阻断攻击行为。

2023 年安天产品攻防演练防守实战价值列表		
防护类别	安全产品	产品价值
网关病毒防护	安天镇关防病毒网关系统	镇关防病毒网关系统是专注于安全威胁防御的新一代专业防病毒产品，结合安天高性能软硬件架构和独特的模块化设计理念，具有高效能、高检出率的特点。产品支持对 ZIP、RAR、TAR 等压缩及打包文件的病毒查杀，支持超百种文件格式查杀，实现高效能的病毒检测和防护功能，能够对日益增强的混合型攻击进行有效防护。在攻防演练实战场景中，防病毒网关系统可以有效检测并阻断网络中的病毒攻击行为，有效抵御网络中的安全威胁。
入侵防护	安天入侵防御系统	安天入侵防御系统是一款全面保障 L2~L7 层安全的应用安全网关产品。PTF-IPS 通过采用串联部署方式，能够及时识别和阻断网络中的溢出攻击、RPC 攻击、WebCGI 攻击、拒绝服务攻击、僵尸主机、木马、蠕虫、系统漏洞等在内的网络攻击行为。安天入侵防御系统还具有 DDoS 防御、ARP 检测、CC 攻击检测、加密流量识别、病毒防护等功能，在攻防演练实战场景中，帮助客户阻断外来攻击。
脆弱性发现	安天漏洞扫描系统	安天漏洞扫描系统具备完善和高效的脆弱性扫描能力，可通过集中管理、周期性扫描等，从多个维度对网络环境中所有系统或网站进行脆弱性扫描和整体评估分析，并提供加固方案。在攻防演练实战场景中，漏扫系统可有效开展大范围安全检查，帮助用户快速检测资产漏洞。
供应链安全（防止开源组件集成漏洞入侵）	安天代码安全检测系统 Antiy SCS	安天代码安全检测系统可以帮助企业识别和防止软件供应链中的安全威胁。在攻防演练实战场景中，攻击者可能会利用软件供应链中的漏洞入侵企业系统，而代码安全检测系统可以通过同步软件漏洞信息，全面掌控软件生命周期的安全，从而有效识别和防止这些潜在的安全威胁。此外，该产品还具有专业的漏洞检测能力和高准确性的检测结果，可以快速响应安全威胁，为企业提供全方位的安全保障。

2023 年安天产品攻防演练防守实战价值列表		
防护类别	安全产品	产品价值
网站安全防护	安天下一代 WEB 应用防护系统（WAF）	安天下一代 WEB 应用防护系统（WAF）基于主动防御理念，从业务安全出发，是集 WEB 安全防御、机器人攻击防护、用户业务访问控制、业务逻辑异常检测、业务威胁评估以及业务数据分析为一体的综合业务安全分析 WEB 应用防护产品。在攻防演练实战场景中，可针对 WEB 业务应用进行有效防护，发现和阻断机器人攻击、信息泄露、用户越权行为等 WEB 攻击。
	安天应用威胁自免疫（Antiy RASP）	Antiy RASP 与应用紧密结合，在关键函数执行前进行安全检测，为应用自身赋能安全防护能力；低误报、高检出地智能拦截各类已知及未知漏洞，并提供漏洞成因管理、报警通知、安全检查等多种能力。具有高性能、高兼容性，部署便捷的特性。在攻防演练实战场景中，可以在 WAF 基础上补充自我免疫“威胁”的能力，形成双重防护模式，切实有效地阻止“远程命令执行”、“上传 WebShell”等重症的发作。
威胁猎杀	安天持续性威胁猎杀服务	威胁猎杀是深入的以“人”为主导的调查反制过程，旨在针对高能敌对方有目的的投放在关键信息资产中潜伏的、隐蔽的威胁攻击进行发现、溯源、反制并形成价值情报等。是积极防御体系当中的一种主动和迭代的威胁检测方法，其作用是在攻击者对关键信息资产造成任何损害之前发现并阻止它们。通过部署威胁诱捕设备与终端防护软件，实时分析信息系统与网络内的数据，结合设备检测能力与数据采集能力，对网内的数据不断进行检索与分析，发现存在的高级威胁，将高级威胁从网内移除。

北京运营总部
地址:北京市海淀区闵庄路3号
清华科技园玉泉慧谷一期1号楼
邮编:100195

哈尔滨总部基地
地址:哈尔滨市松北区世坤路838号
科技创新城7号楼
邮编:150028

哈尔滨、北京、武汉、深圳、成都、南京、上海七地研发中心

内部资料　赠阅参考

安天微信公众号

安天微信视频号