（上接第一版）

席架构师肖新光通过反思安天在态势感知技术解决方案研发和推广实践中的经验教训，说明了为什么需要实战化运行的战术型态势感知平台，并从四个方面的变化阐述如何开展网络安全态势感知工作。

安天创始人、首席架构师肖新光解读做好网络安全态势感知工作应把握的四种变化

对手的变化：从应对单点威胁到应对高级网空威胁行为体，网空防御者不能脱离具体的防御场景和其所承载的信息价值。

视角的变化：从自我闭环走向赋能客户，实现与攻击者的对抗闭环，客户侧安全防御人员最熟悉自身的信息系统，是网空防御工作的主角，应将客户置于闭环上。

思路的变化：从网络安全监测平台走向战术型态势感知平台，安天在监测型态势感知平台基本研发成熟的情况下，正在紧锣密鼓的加快研发实战化运行的战术型态势感知平台。

效果的变化：从单点防护能力到动态综合防御能力，坚持实战化的导向，构建动态综合网络安全防御体系。

他表示，应在深刻掌握这些变化的基础上，遵循网络强国战略指导思想，以网络安全能力叠加演进为导向，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。这些工作仅靠一个厂商无法完成，而需要由多个能力型厂商组成良性生态体系，安天同样愿意为这个生态体系的形成做出自己的贡献。

■ 业内专家关于网络安全态势感知研判工作的思考

天津理工大学教授、中国网络空间安全协会副秘书长张健与参会嘉宾共同分享了他关于网络安全态势感知研判工作的一些思考。为应对当前日趋复杂的全球网络安全形势，中国网络空间安全协会在态势感知方面做了较多的工作，包括初创网络安全态势行业会商机制，成立网络安全态势研判工作组；充分发挥协会桥梁纽带作用，为政府部门提供有力支撑；并在协会成立期间超额完成合同规定报告数量。后续，协会将继续在牵头组织起草网络安全态势感知相关标准、深化完善网络安全态势行业会商机制、拓展国内外网络安全信息渠道、推动网络安全态势感知平台建设等方面进一步展开工作。

天津理工大学张健教授分析当前态势感知工作中存在的问题

■ 安天工程师分享战术型态势感知的实践与应用

安天研发工程师解读战术型态势感知和监测型态势感知的区别

安天态势感知产品线的工程师带来了题为《战术型态势感知的探索与实践》的分享。他表示，自安天分享实战化态势感知至今已过去一年时间，在战术型态势感知相关项目的建设过程中，安天作为能力型厂商，进行了一些探索也形成了一些经验总结和教训思考。根据与被监测资产的关系，不同类型的态势感知需要不同的能力，特别是战术型态势感知，需要以全面覆盖的持续监测为基础，面向任务、基于知识形成有效的理解力，借助信息融合实现有效的理解和预测，并联动指控积极防御体系实现实战化的运行。

安天解决方案工程师解读何为“三高”网络

当前，在监测型态势感知平台基本研发成熟的情况下，安天将保障“三高”网络的安全作为战术型态势感知平台体系的主要应用场景。“三高”网络具有“高信息价值、高防护等级、高威胁对抗”的特点。来自安天方案规划设计咨询部的工程师在《“三高”网络动态综合安全防御体系》的分享中指出，“三高”网络信息系统，应以敌情想定为前提，参考叠加演进的层次化网络安全能力模型，建设动态综合网络安全防御体系；遵循三同步原则，从网络信息系统的规划设计开始，充分考虑基础结构安全，增强网络可管理性、提升可防御性，做好大量扎实演进的基础环节、基础能力支撑工作；在此基础上，叠加可提供持续威胁防御和洞察能力的纵深防御，进一步建设威胁情报驱动的战术型态势感知指控积极防御，并在叠加演进的各个安全能力方面均配套实战化的网络安全运行机制，以应对高级网空威胁行为体的体系化攻击。

冬训营首日现场气氛热烈，茶歇期间还向参会来宾分享了业内资深专家黄晟和安天研究院协同翻译的《网络空间安全防御与态势感知》一书，该书已由机械工业出版社在国内出版发行。

安天参译文献《网络空间安全防御与态势感知》已在国内出版发行

安天周观察
主办：安天 2019年01月14日(总第168期)试行 本期4版 冬训营特刊 内部资料 免费交流
安天官方微信

战术型态势感知指控积极防御

——安天冬训营首日纪实

2019年1月8日-9日，网络空间威胁对抗与态势感知研讨会暨第六届安天网络安全冬训营在哈尔滨召开，本届冬训营以“战术型态势感知指控积极防御，协同响应猎杀威胁运行实战化”为主题，并有多位业内专家与安天工程师一同深入分析来自不同层级网空威胁行为体的攻击事件，进一步完善网络空间的敌情想定；共同分享网络安全实战化运行的心得体会和战术型态势感知平台的实践探索，研讨如何协同响应猎杀高级威胁。

在首日的开幕式上，来自中央网信办网络安全协调局和黑龙江省委网信办等国家和地方主管部门的领导与专家出席并致辞。

第六届安天网络安全冬训营开幕现场

■ 安天发布新版解决方案、产品和服务体系

安天从上游核心技术供应商转型为前台综合型网络安全厂商的过程也是一个持续自我批判和创新演进的过程。继上届冬训营上，安天公开发布了技术工程体系和产品图谱后，安天结合过去一年的工程实践和思考，在本届冬训营上发布了新版解决方案、产品和服务体系。

安天集团CTO、安天移动安全CEO潘宣辰进行了发布宣讲，他指出，安天坚持以敌情想定为前提，以长期威胁对抗经验积累为基础，以自主先进为标尺，坚持创造有效的客户安全价值。安天正在持续推动面向不同客户场景的敌情想定的系统化和具象化落地，在国际知名的“滑动标尺模型”基础上演绎和完善了“叠加演进安全能力模型”，产品体系、服务体系更为系统化。同时，安天本次正式首发了四个创新型解决方案，分别为“对抗式威胁评估服务解决方案”、“三高网络场景安全整体解决方案”、面向网信主管部门和职能部门的“监测型态势感知解决方案（新版）”和面向重要信息系统及关键信息基础设施的“战术型态势感知平台体系解决方案”。在2019年，安天将继续坚持以敌情想定为前提，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用客户筑起可对抗高级威胁的网络安全防线。

同时，作为全球重要的安全赋能方，安天将进一步加强对供应链的安全赋能工作，促进安全能力有效下沉，形成基础安全能力和感知能力的“关口前移”。

安天集团CTO、安天移动安全CEO潘宣辰介绍解决方案、产品、服务和支撑体系

■ 2018年网络安全威胁年报发布

在每年的冬训营上发布年报的征求意见稿，征求参会专家的意见建议，是安天一直以来的传统。安天副总工程师李柏松在冬训营上发布了2018网络安全威胁年报——《2018年网络安全威胁的回顾与展望》，并对其主要内容进行了介绍。他从APT年度情况、漏洞的响应与处置、勒索软件与挖矿木马、数据泄露、供应链安全和威胁泛化等几个方面，回顾了2018年的网络安全热点，介绍了安天重点跟踪分析与曝光的APT攻击事件。讲解了“地缘政治和国家利益竞合是APT攻击的主要源动力”、“以敌情想定为前提更好地完善漏洞响应与处置机制”、“勒索软件和挖矿木马的爆发暴露了端点无效防护的问题”，“警惕隐私泄露带来的安全风险”，以及“供应链环节成网络攻击中关键载体”等多个年报核心观点，强调“以全面能力导向推动动态综合网络安全防御体系建设”的思路。

安天副总工程师李柏松讲解年报中“供应链安全”有关内容

■ 安天人反思，为什么我们需要“实战化运行的战术型态势感知”

在技术分享环节，安天创始人、首

（后续内容转第四版）

协同响应猎杀威胁运行实战化——安天冬训营次日内容回顾

第六届安天网络安全冬训营开幕第二天，网络安全研究者和工程师继续围绕会议主题，分享网络安全实战化运行的心得体会和战术型态势感知平台的实践探索，研讨如何协同响应猎杀高级威胁。

■ 神州网云 CEO 宋超：主动防御在威胁狩猎中实战应用

宋超在报告中指出：随着大量网络军火泄露和商业军火的泛滥，目前攻击者的能力和手段越来越强大，传统的被动防御已经不足以做到全面的监测，主动防御的出现以及主动加被动防御相结合，对攻击者的主动监测、溯源分析和威胁狩猎服务提供了有力的支撑。

■ 安天捕获分析技术中心：网空威胁事件模型及应用

安天对 NSA/CSS 技术网空威胁框架进行了分析解读，并对如何根据威胁框架建立有效布防点、组织防御体系提出了思考。安天认为在战术型态势感知中，针对各种安全设备来源数据需要统一的威胁事件的表达和威胁事件关联关系的表达；需要能够融合非威胁事件和威胁事件，并灵活表达攻击链、网空实体和行为的关系图谱；能够对各种数据进行融合、关联、表达攻击链，从而建立统一的框架和行为描述，方便威胁展示、决策、上层数据交互。

■ 安天端点安全产品研发部：铁流铸智甲—战术型态势感知指导下的终端威胁防御体系

终端作为威胁对抗的主战场，同时也是安全防御的最后一道防线，其面临着十分严峻的安全挑战。过去的一年，安天全面适配了多种终端操作系统，特别是国产化系统，进一步提升了主动防御、配置加固、信息采集、行为画像以及系统深度分析与应急处置的能力。但仅靠累积终端的防御能力，是难以有效应对高能力攻击对手的，终端需要与战术型态势感知平台协同联动，提前发现网空安全风险并开展有效防御。

■ 安天流量监测产品部：无所遁形—战术型态势感知中的全方位流量监测

战术型态势感知必须以可靠的数据留存采集和基础威胁监测发现等能力为基础，融合客户业务在网络空间的投影，对流量持续监测、发现威胁，提供感知网络空间态势的手段，帮助客户理解业务的实际运行过程，发现异常行为。安天通过沙箱和蜜网的结合，产生私有化威胁情报，将其作为基础设施的一部分。流量控制设备接收指控，诱导威胁，达到化被动为主动的目的；监测设备接受态势感知系统的指控，快速响应，按需获取细粒度解析行为和原始流量，为威胁研判做出支撑。通过在流量侧、情报侧与态势感知系统的紧密结合，达成发现威胁、理解威胁、预测威胁、挫败威胁的目的。

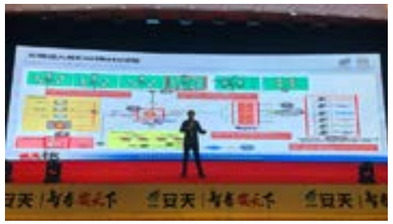
■ 安天应急响应中心：“三高”网络环境中与敌手的隔空对决

网络空间的对抗是一场无硝烟的战争，在这场战争背后是攻防两端技术和人才的对决。如何在高等级、高防护、高价值的网络环境中与对手进行隔空对决，进而在未来的网空对抗中实现运筹帷幄猎杀敌手于千里之外？安天是多年持续防御、捕获、分析敌手，与敌手正面交锋的团队。安天分享了多次在网络空间与敌手较量，捕获分析溯源多个境外高级网空威胁行为体的实例。

■ 安天基础引擎研发部：下一代威胁检测引擎—赋能威胁情报

安天是全球重要的威胁检测引擎赋能方，有上百家合作伙伴使用安天的引擎，覆盖超过十五亿部智能终端设备和超过三十万台网络设备。安天下一代威胁检测引擎，立足于攻击方可以获得防御方引擎，并可以绕过引擎检测机制的假想下进行设计，将传统反病毒引擎的检测器作用，提升为“识别＋检测＋拆解”的综合模块，并支持多种场景化的检测，为态势感知供应向量数据与标签。安天将下一代威胁检测引擎应用于威胁情报生产的整个生命周期，深度赋能威胁情报系统，生产具备战术价值的威胁情报，支撑态势感知系统。

■ 安天应急响应中心：从“绿斑”和“方程式”组织看不同等级威胁行为体的攻击能力



安天始终致力于网空安全的对抗，数年来持续跟踪和研究高级网空威胁行为体，陆续发布数十篇各等级网空威胁行为体研究报告。2015 年安天发布了“方程式”系统分析报告，2018 年安天曝光了“绿斑”组织。本次通过复盘"绿斑"和"方程式"的攻击行动，以探讨不同等级网空威胁行为体的能力体系的差异，从多种维度分析对比不同等级网空威胁行为体的能力，从应对超高等级威胁行为体的角度展示做好实战化运行的战术型态势感知平台和动态综合防御体系的重要性。

■ 安天网络安全服务部：人机协同态势感知运行能力建设

围绕战术型态势感知形成的防御模式中，网空安全防御人员是态势感知不可或缺的“系统组成部分”，人机协同才能充分发挥态势感知网络安全防御能力。安天在态势感知建设过程中，为实现客户侧有效防护的价值落地，从赋能客户角度出发，思考人员如何有效使用态势感知，如何结合态势感知实战化应对网络安全威胁，经过一定的工程化实践，不断总结与验证实战化运行经验，为客户建立实战化的网络安全运行机制，赋能客户侧人员结合态势感知发现威胁踪迹，并针对潜伏威胁展开“猎杀”行动。

■ 安天微电子与嵌入式安全研发部：接触式攻击和电磁装备在网空攻防中所带来的威胁

物理隔离长期被视为关键性的安全屏障。但对于高级网空威胁行为体来说，接触式攻击、供应链攻击与一些电磁手段结合，让物理隔离形同虚设。通过接触式攻击（包括供应链和物流链劫持等手段）和电磁装备能够有效地突破隔离网络，进行横向移动，构建第二信道，完成控制、下载、数据的回传以及远程控制。安天通过对外方泄露装备的研究，分析了我国重要信息系统面临的相关风险，提出做好人防、物防、技防工作，用体系化防御应对体系化攻击的观点。

两天来，十余位研究者和工程师的演讲，对态势感知技术体系在积极防御体系中的作用做了详尽的分析，指出了当前在态势感知实践中所遇到的问题，以及构建实战化的战术型态势感知的必要性和紧迫性。“网络空间威胁对抗与态势感知研讨会暨第六届安天网络安全冬训营——铁流鏖战”的公开报告部分至此也圆满结束，安天将坚持以敌情想定为前提，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

网络安全是当前大国博弈的焦点领域，是持续性对抗的领域。在网络强国战略思想的指引下，安天将与客户一道，携手共进，将网空防御力量打造成滚滚“铁流”，不惧艰险，“鏖战”强敌。

安天参研相关项目获国家科学技术进步二等奖

大规模网络安全态势分析关键技术及系统 YHSAS 获奖

2018 年国家科学技术奖名单出炉！安天参研相关网络安全态势分析关键技术项目获科技进步二等奖。

1 月 8 日，中共中央、国务院在北京人民大会堂隆重举行 2018 年度国家科学技术奖励大会，对为我国技术研究、技术开发、技术创新、推广应用先进科学技术成果、促进高新技术产业化，以及完成重大科学技术工程、计划等过程中做出创造性贡献的中国公民和组织授予奖励。此次奖励大会上，由国防科技大学牵头，主要是由哈尔滨安天科技集团股份有限公司等四家单位参研的“大规模网络安全态势分析关键技术及系统 YHSAS”获国家科学技术进步奖二等奖。

2018 年度国家科学技术进步奖完整名单详见：http://www.nosta.gov.cn/WEB/detail1.aspx?menuID=163&contentID=1572