( 上接第一版 )

《突破“赛道”的禁锢，网络安全产品价值的重定义——探索基于防御动作框架的关键安全能力拆解与整合》。

**3. 嘉宾报告版块**

来自工银科技、中资网安的两位嘉宾，分别聚焦银行信息安全、网络安全运营数字化，带来相关议题。

**4. 威胁挑战版块**

安天副总工程师李柏松对 2020 年网络安全威胁进行全面回顾，发布《2020 网络安全威胁年报（预发布版）》；安天研究院对两种主流的威胁框架：ATT&CK 威胁框架和 SHIELD 积极防御模型的构建、内容、实践应用等进行详细的介绍；安天应急响应中心带来《高级威胁组织渗透隔离网络能力分析与年度案例》分享。

**5. 客户价值与安全场景版块**

- 《容器与微服务安全的对抗实践》
- 《专杀工具在应急响应服务中的价值》
- 《邮件安全的威胁认知与防御关口设置》
- 《安天智甲防勒索病毒解决方案》

**6. 探索与技术创新版块**

- 《引擎优化之路与“芯”探索——安天引擎的效率改善回顾与展望》

**7. 安全能力支撑版块**

- 《威胁情报和检测引擎结合，有效提升安全防护能力》
- 《安天下一代引擎结合知识库，如何揭示载荷的 ATT&CK 战术能力》
- 《探海 + 追影，威胁流量检测与文件深度分析的最佳实践》
- 《SOAR 如何编排指引细粒度的端点处置》
- 《智甲如何实现端点侧细粒度防御与处置》
- 《从捕风蜜罐到无所不在的欺骗防御》

## ■ 往届冬训营回顾

自 2014 年起，在相关主管部门和职能机构指导下，安天以“直面实际威胁，形成价值落地”为导向，已经连续在哈尔滨承办了七届网络空间威胁对抗与防御技术研讨会，内容每年聚焦专业主题，深入分析高级威胁事件，研讨有效防御价值落地，已逐步发展成为集安全前沿理论探讨、产品技术创新、网安人才培养、行业实践分享等方面的一个高水平的、全方位的行业性活动。

根据年度网络安全形势和工作主题，安天为每届冬训营设定了四字营语，分别是：“凛冬将至”、“北风乍起”、“朔雪飞扬”、“冰峰屹立”、“红旗漫卷”、“铁流鏖战”和“寒夜远征”。本届冬训营，营语为“长缨待展”。

从 2016 年开始，为了让议题内容更为聚焦，安天决定每届冬训营围绕一个核心主题进行。第三届冬训营主题为“情报的支撑，塔防的实践”，探讨了如何构建有效的纵深防御体系；第四届冬训营以“有效防护，价值输出”为主题，自我批判作为安全厂商和研究者的主观局限和技术优越感，回归安全技术为用户提供有效的防护能力和价值保障的本质；第五届冬训营主题为“敌情想定是前提，网络安全实战化”，旨在以客观充分的敌情想定为前提，以实战化作为网络空间安全防御的要求，让安全技术、产品与服务能够随时应对真实的威胁，为客户实现有效的安全价值。第六届冬训营主题为“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”，分享战术型态势感知的探索实践，以及在客户侧安全规划、能力集成、威胁应对、应急响应等方面的经验。第七届冬训营主题为“威胁框架：认知与实践”，分享和共商对威胁框架安全价值的理解和实践思考，围绕用户的关切，分析来自不同层级威胁行为体的攻击事件；介绍了在检测引擎、端点防护、流量监测、深度分析、态势感知等方面威胁框架的结合进展，以及在重要信息系统和关键基础设施中建立有效防御体系的探索实践。

在过去的几届冬训营上，来自政企机构、安全研究机构、知名大学和安全厂商的演讲嘉宾与安天的工程师，共同分享研讨网络安全领域的前沿探索和工作心得。相关议题对充分认识网空敌情，深入了解高级威胁，让网络安全技术能力转化为有效客户价值，产生了积极的作用，受到相关机构和行业领域专家的好评。

**点击地址回看视频（地址：http://live.163.com/room/235103.html）**

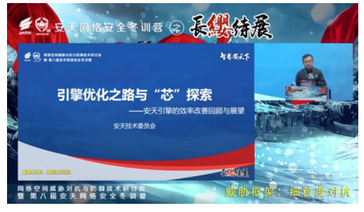
( 上接第三版 )

介。在第八届安天网络安全冬训营上，安天安全服务中心带来了《邮件安全的威胁认知与防御关口设置》的报告。

## ■ 探索与技术创新

**• 引擎优化之路与“芯”探索——安天引擎的效率改善回顾与展望**

作为安全产品和安全体系的关键组件，威胁检测引擎是各种安全机制手段中，最为庞大、最为复杂的技术之一。二十年来，安天在反病毒引擎的工作机理和检测方法上，持续地探索和创新。随着网络流量和威胁复杂性的爆炸式




增长，基于通用计算平台性能提升和算法改进已经难以满足需求。在“摩尔定律”即将终结的时期，我们尝试突破现有引擎软硬件架构，探索新的检测技术。安天技术委员会回顾了安天威胁检测引擎的发展历程，分析各阶段软硬件技术的挑战和突破，并对基于专用加速芯片的异构计算威胁检测技术进行展望。

**扫描二维码或点击地址回看视频**

**地　址：**http://live.163.com/room/235103.html



安天周观察
主办：安天　2021 年 02 月 08 日 ( 总第 266 期 ) 试行　本期 4 版　冬训营特刊　扫描上方二维码查询安天所有对外开放资料
安天对外开放资料平台　安天官方微信

# 第八届安天网络安全冬训营上线首播
# 累计 55 万人在线关注


2021 年 2 月 3 日，网络空间威胁对抗与防御技术研讨会暨第八届安天网络安全冬训营（以下简称：冬训营）于线上开幕，在长达 9 个多小时的分享中，在线观看累计人数已近 55 万。

本届冬训营由中共黑龙江省委网络安全和信息化委员会办公室发起，省科技厅、省公安厅、省国家保密局等多家厅局委办联合主办，中国信息安全测评中心提供技术指导，哈尔滨市松北区人民政府、安天科技集团股份有限公司、中国网络安全产业联盟承办。

面对网络安全的最新趋势和技术动向，本届冬训营以“威胁框架：细粒度对抗”为主题，分享最新学术研究成果和前沿探索，威胁框架和防御的最新国际动态，分析全球抗击疫情背景下网络威胁活动的新情况，介绍安天引入威胁框架全面提升产品和服务能力的新进展，特别关注如何根据攻击技术和子技术遍历，细粒度的改善各防御环节。

黑龙江省委网信办副主任王希忠发表开幕致辞。他表示，网络安全牵一发而动全身，深刻影响社会各领域安全。以安天为代表的网络安全企业，积极履行维护和保障国家网络安全的职责和使命，成为国内网络安全威胁对抗的重要力量。由安天公司承办的网络安全冬训营活动，为网络安全前沿理论探讨、应用技术创新、网安人才培养、行业实践分享提供了一个高水平的、全方位的学习交流平台。

## ■ 七个议题版块

本届冬训营分为了特别议题、安全框架方法与产品图谱、嘉宾报告、威胁挑战、客户价值与安全场景、探索与技术创新、安全能力支撑七个议题版块。


**1. 特别议题版块**

安天应对新冠疫情应急指挥部讲述了安天是如何用网络安全能力支持抗击疫情。

**2. 安全框架方法与产品图谱版块**

安天创始人、首席技术架构师肖新光带来

( 后续内容转第四版 )

尊敬的读者：
2021 年春节即将来临，《安天周观察》于春期间休刊两期，恢复出版时间为 2021 年 3 月 1 日。感谢所有读者对《安天周观察》一直以来的支持与关注！
祝大家春节快乐！
2021 年 2 月 8 日

# 安天冬训营 7 个议题板块 18 个议题内容介绍

2021 年 2 月 3 日，第八届安天网络安全冬训营于线上成功举办，当日累计 55 万人在线关注。本届冬训营营语为“长缨待展”，以“威胁框架：细粒度对抗”为主题，设置 7 个议题版块，18 个议题。

## ■ 特别议题篇

- 我们用网络安全能力支持抗击疫情


2020 年初，新冠疫情发生后，安天迅速启动重大社会事件网络安全应急值守制度，研判安全风险。各地研发中心和应急响应站第一时间启动，有效支撑了客户网络安全保障工作。安天发挥自身在数据分析、安全可视化等方面的技术优势，为政企机构做好防疫保障工作，免费提供了分析员工分布与防控风险、有效安排返程的可视化分析工具。

## ■ 嘉宾报告篇

- 于细节处见精神——从几个细节出发，也谈银行信息安全工作实践


工银科技有限公司安全总监王贵智从几个具体安全工作实践出发谈银行信息安全工作，带来了题目为《于细节处见精神——从几个细节出发，也谈银行信息安全工作实践》的报告。

- 网络安全运营数字化


中资网安总经理助理杨春尧发表《网络安全运营数字化能力思考》的演讲，并从全数字化时代对业务模式要求、网络安全运营对数字化的需求、网络安全运营数字化能力框架、网络安全运营数字化实践运用四个方面来介绍数字化运营怎么做。

## ■ 主旨演讲

- 突破“赛道”的禁锢，网络安全产品价值的重定义——探索基于防御动作框架的关键安全能力拆解与整合


安天创始人、首席技术架构师肖新光分享《突破“赛道”的禁锢，网络安全产品价值的重定义——探索基于防御动作框架的关键安全能力拆解与整合》，提出按照有效安全价值导向，深度融合资产场景，按照位置特点，实现关键防御动作的按需定制重组，突破赛道羁绊，从安全价值重新定义产品。

## ■ 网络安全威胁年报—《2020 年网络安全威胁回顾》发布


在每年冬训营上发布前一年度安天网络安全年报的预发布版，是安天一直以来的传统。网络安全威胁年报是安天对上一年度的代表性威胁事件、流行的攻击手法、最新的威胁趋势等进行梳理和总结。在第八届安天网络安全冬训营上，安天副总工程师李柏松带来了《2020 年网络安全威胁回顾——安天 2020 年网络安全年报 ( 预发布版 ) 内容提要》的报告。

## ■ 威胁事件篇

- 威胁框架的发展与深化

当前网络安全正在经历能力导向建设模式的变革。网络安全规划方法不断系统化和完善；安天研究院对两种主流的威胁框架：ATT&CK 威胁


框架和 SHIELD 积极防御模型的构建、内容、实践应用等进行了详细的介绍。

- 高级威胁组织渗透隔离网络能力与年度案例

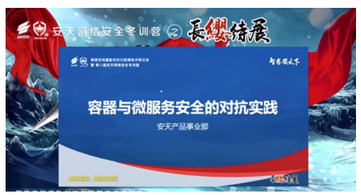

在今年安天发布的网络安全威胁年报中，安天提出了“突破物理隔离已经成为高级威胁组织的普遍能力”的观点。在第八届安天网络安全冬训营上，安天应急响应中心带来的《高级威胁组织渗透隔离网络能力分析与年度案例》议题，详细剖析隔离网入侵方案、控制与回传信道建立方法和经典攻击案例，以及 2020 年新增的代表性隔离网攻击案例。安天再次提醒：不能因“隔离”而忽略建设安全监测与防护体系。

## ■ 主机安全篇

- 安天智甲防勒索病毒解决方案


目前勒索病毒已经成为全球性威胁，给用户的数据安全带来了巨大挑战，2020 年勒索病毒更是呈现迅猛增长态势，并且勒索方式也开始由简单的恶意数据加密转变为危害更高的“定向攻击 + 数据窃取 + 数据加密”的新作业模式。安天是国内较早开始关注并且持续在防勒索领域投入的安全厂商之一，安天产品事业部对勒索病毒现状以及安天智甲系统的防御方案进行了分享。

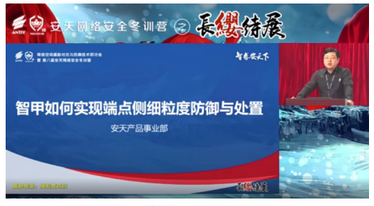
- 容器与微服务安全的对抗实践




容器和微服务是当前互联网的热点技术，这些技术推动了应用构建和运行方式的重大变革，同时 CI/CD 这种持续集成、持续交付的研发模型，满足了互联网企业产品快速迭代的需要，从应用开发阶段到交付阶段，可以实现自动化、高频的向客户交付应用。而这种新的云模式下的安全问题并没有得到大家关注。安天产品事业部带来的《容器与微服务安全的对抗实践》报告，分享了近期安天针对容器和微服务做的安全方面的对抗实践，并给出新的云模式下的一些安全建议。

## ■ 响应与编排篇

- 智甲如何实现端点侧细粒度防御与处置

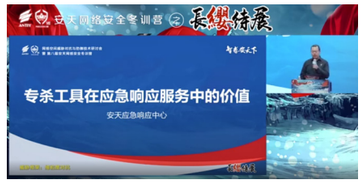



端点一直是网络威胁对抗的主战场，用户对于端点安全防护工作也越加被重视，安天认为未来端点安全防护必将由多产品集中部署转变为端点一体化安全防护，智甲终端防御系统就是一款面向端点提供一体化安全防护的优秀产品。

关于一体化防护，我们认为要想实现端点一体化防护，利用威胁框架进行细粒度防御是关键，那究竟什么是细粒度防御？又如何实现细粒度防御？安天产品事业部为我们带来了《智甲如何实现端点侧细粒度防御与处置》的报告。

- 专杀工具在应急响应服务中的价值

议题针对在客户网络安全应急响应工作中遭遇的业务痛点和由此引发的迫切需求，来具体的阐释专杀工具在应急响应工作中发挥的积极作用，并深入探讨安天专杀工具对应急响应工作的重要价值。安天应急响应中心带来了《专杀工具在应急响应服务中的价值》的报告。




- 威胁情报和检测引擎结合，有效提升安全防护能力


面对 APT 攻击组织的高级攻击手法和极强的隐蔽性，对于威胁的检测和发现带来极大难度。威胁情报在实践落地中遇到很多挑战，安天以威胁引擎为基础，叠加整合威胁情报，有效提升客户的精准威胁检测、攻击者识别、追踪溯源、威胁预警等安全防护。安天研究院威胁情报部带来了《威胁情报和检测引擎结合，有效提升安全防护能力》的报告。

- 探海 + 追影，威胁流量检测与文件深度分析的最佳实践

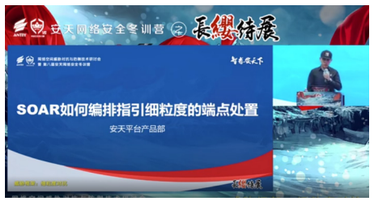

基于“探海”威胁检测系统与“追影”威胁分析系统在客户的部署实践，总结流量检测与文件分析两种设备的实战能力要求，并结合威胁框架展开，分享实战中有效发挥两类产品的最佳模式，安天产品事业部带来了《威胁流量检测与文件深度分析的最佳实践》的报告。

- 从捕风蜜罐到无所不在的欺骗防御

欺骗作为一种威胁对抗能力，与威胁检测、拦截、处置具有同等重要的地位，也可以融入各种安全产品，如防火墙、WAF、终端安全、网关等安全产品，这些产品的欺骗能力与蜜罐结合构成深度欺骗体系，从攻击不同方向路径进行欺骗，


包括外部攻击欺骗，主机欺骗，横向扩散欺骗、外联欺骗等。安天安全服务中心带来了《从蜜罐捕获到无所不在的欺骗防御》的报告。

- SOAR 如何编排指引细粒度的端点处置




几年前，Gartner 提出了 SOAR 这个概念，几年间，SOAR 的概念经历了很大转变。SOAR 包含了对于事件响应、安全自动化、案例管理和其他安全工具的一系列平台实践。安天将对 SOAR 的认知和安天 SOAR 系统的特点进行了介绍，并通过一些典型案例展示了安天 SOAR 系统进行威胁处置的功能特点和操作流程。安天平台产品部带来了《SOAR 如何编排指引细粒度的端点处置》的报告。

## ■ 布防与环境塑造篇

- 邮件安全的威胁认知与防御关口设置


1987 年的北京发送了一封主题为《跨越长城，我们可以到达世界的任何角落》的电子邮件，这是我国第一封邮件，预示着互联网时代悄然叩响了中国的大门，也预示着对中国的网络攻击不期而至。每年政企面对数亿计的钓鱼邮件，新冠疫情加速远程办公的信息化需求，邮件在其中充当了重要的信息传递媒

（后续内容转第四版）