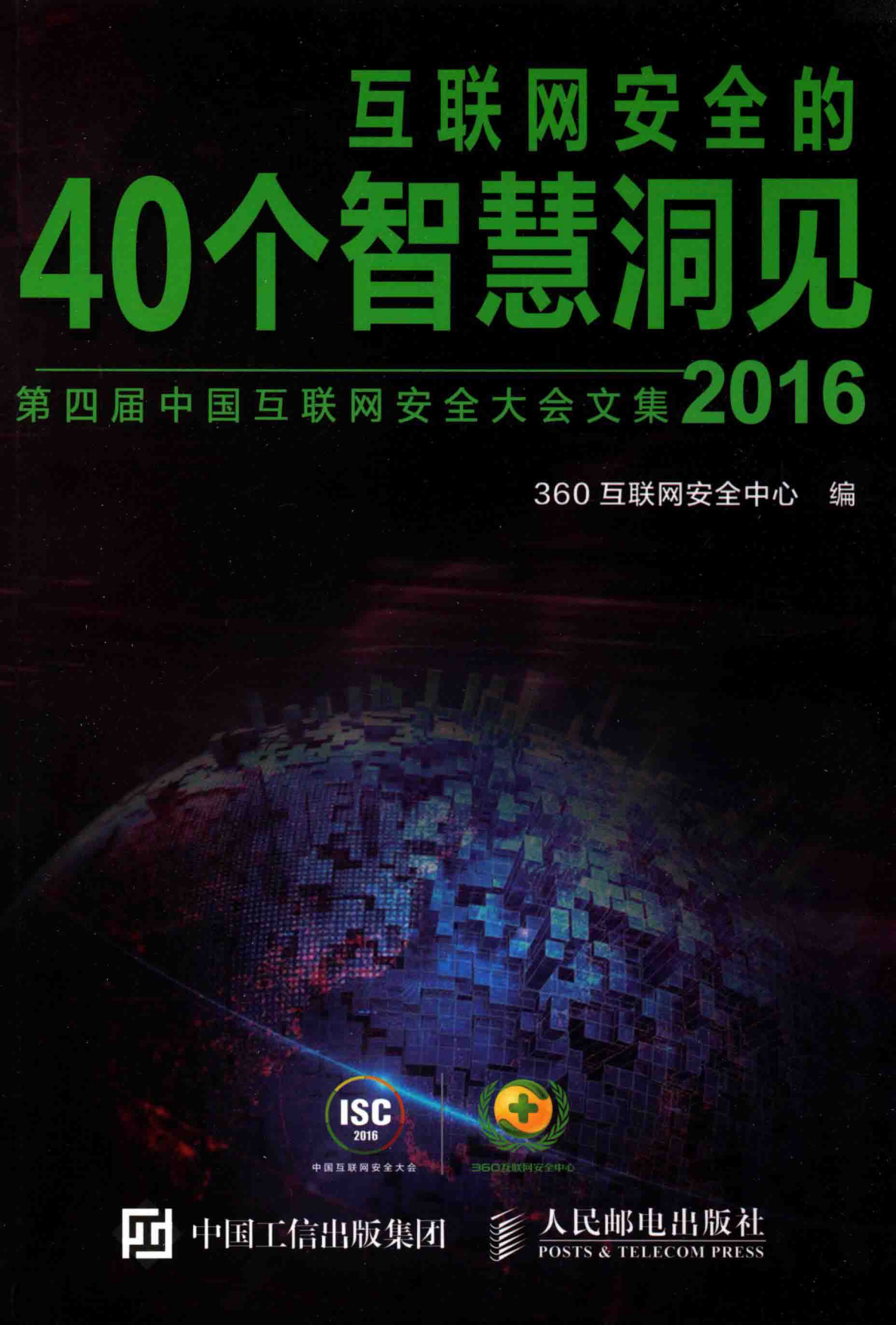
互联网安全的40个智慧洞见

第四届中国互联网安全大会文集 2016

360 互联网安全中心 编



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

互联网安全的40个智慧洞见（2016）

360互联网安全中心　编

人民邮电出版社
北　京

图书在版编目（CIP）数据

互联网安全的40个智慧洞见. 2016 / 360互联网安全中心编. -- 北京 : 人民邮电出版社, 2017.1
ISBN 978-7-115-44444-8

Ⅰ. ①互… Ⅱ. ①3… Ⅲ. ①互联网络－安全技术－文集 Ⅳ. ①TP393.408-53

中国版本图书馆CIP数据核字(2016)第295833号

内 容 提 要

本书站在互联网安全理论与实战的前沿，分别从网络空间安全战略、治理、产业和技术4个角度为读者透析2016年中国及全球互联网安全的发展状态和演变形势。

本书可供网络与信息安全相关科研机构以及高等院校研究人员、互联网安全领域企业技术与研发人员，以及对网络空间安全感兴趣的自学者参考。

◆ 编　　360互联网安全中心
责任编辑　李　静
执行编辑　乔永真
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京缤索印刷有限公司印刷

◆ 开本：690×970　1/16
印张：30.5　　2017年1月第1版
字数：333千字　　2017年1月北京第1次印刷

定价：158.00元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

协同联动，共建安全＋命运共同体

齐向东

360公司总裁

一年一度的中国互联网安全大会，已经成为一个盛会。它不仅集合了世界范围内的业界领袖和精英，而且每年的大会对未来一年的网络安全趋势都有一个比较准确的预测，越来越多的安全企业已开始按照这个预测的趋势来把握自己技术研发的方向。

2014年，大会提出“万物互联，安全第一”，引爆了中国市场对IoT安全的关注，对智能家居、车联网，以及智能/自动驾驶、机器人和工业控制安全的关注。这些领域的网络安全工程师的努力工作产生了许多成果，对IoT的快速发展起到了很大的推动作用。

2015年，大会的主题“数据驱动安全”，快速推动了安全行业对“数据＋安全”技术的研究。自2015年以来，无论是在中国政府出台的大数据发展纲要里还是在贵阳大数据产业博览会上，安全都是重要的篇章和

话题，大家都在探索如何通过大数据快速发现威胁。

比如360公司自主研发的网络安全态势感知系统，就受到了包括中共中央领导在内的各级政府相关负责人的好评。这个系统能够利用大数据自动感知预测网络攻击，评估网络安全态势，对相关机构防范和响应网络攻击起到了重要作用。

2015年，360公司还向全球开放了威胁情报中心，全球知名的互联网公司、IT公司及众多世界500强企业的安全主管都注册成为它的会员。我们这个威胁情报中心在过去的12个月里，通过对威胁情报的大数据分析，共计发现并跟踪了72个安全事件，其中APT的55个；已经梳理成报告的达29个，公开发布6个。

2016年，ISC大会的主题是“协同联动，共建安全＋命运共同体”，因为在网络威胁越来越大的今天，从政府到企业，都表现出了强烈的联动意愿，单一的政府部门和企业如果不进行数据共享和情报共享，几乎无法更好地解决现在的网络安全问题。

协同联动思想的提出，其更加深刻的时代背景是网络安全所面临的矛盾与困境。一方面，从中央到地方，从企业到个人，网络安全都在受到越来越多的关注，人们对网络安全发展的期待也越来越高。但另一方面，受到传统技术方法，甚至是商业体系的局限，安全产品与安全服务的发展却都面临重重困境。

第一，信息安全是一场无休止的战争。

信息安全和信息化存在根本性的不同。信息化的重点在于初期建设，就像是建筑师建一座大楼；后期的维护工作则相对简单，就像是公寓的

物业管理。而信息安全则不同，初期建设只是一个开始，真正的考验在运维阶段。信息安全是一场战争，它是一个持续的过程，只要信息系统存在一天，战争就不会停止。信息安全是一场战争，需要一群勇敢的武士面对敌人，但是更需要战友间的信任和军事化的组织。敌人不只是阴影中的黑客，队友间的怀疑才是最可怕的敌人。这是信任的纪元，这是怀疑的纪元。可惜的是，在这场战争中，我们并非优势的一方，诸多困境正横亘于前。

第二，未知威胁挑战传统的检测方法。

在战场上，最令人恐怖的不是强大的敌人，而是未知的敌人。网络中的攻防也是如此，企业如果无法发现入侵，就无法有效地防护和响应。使用传统技术的入侵检测系统和防病毒软件正面临越来越多的诟病。主要的问题有两点：一个是新型攻击无法被发现，另一个是大量误报信息淹没了真实报警。

从攻击者一方来看，攻击脚本和恶意程序的增长速度太过迅速，例如 360 积累的恶意样本库已经达到百亿条规模。从检测方法来看，如果没有创新的技术，传统的特征库已经无法保证恶意代码的检出率。在这种情况下，新型攻击难以被发现也是必然的结果。

对于从大量报警中发现真实攻击的线索的问题，传统 SIEM 和 SOC 产品通常提供各种关联算法和定制规则来解决，但长期以来实用性并不好。现在看来，这个问题的本质是“从稻草堆中寻找一根针”。所以，只有两类相关技术成熟起来，才有可能真正解决这个问题。第一项技术是大数据分析技术，为海量报警和相关信息的复杂分析提供基础支持，第

二项技术是威胁情报，能够从外部提供准确的威胁信息，与内部疑点进行对比分析。

第三，安全事件挑战企业的响应能力。

对一个企业来说，安全事件的响应能力是安全团队最重要的能力之一。但是近年来，这项工作的难度越来越大了。一方面，企业的 IT 规模在不断扩大，业务种类也在不断增加。而云计算、虚拟化、SDN 等新兴技术的采用，也给 IT 架构带来了变革期的阵痛。这些因素都导致了安全边界的扩大。另一方面，攻击者使用的攻击手法种类越来越多，也越来越复杂，往往需要多个安全产品的配合才能发现和处置，企业部署的安全产品种类和复杂程度也在增加。

其结果是，安全团队的工作量越来越大，需要的专业化程度也越来越高。有的安全团队会长期超负荷运转，应付各种重复工作；也有的安全团队采购了先进设备之后，由于使用太复杂而难以发挥其效果。所以对用户来说，最有效的网络安全设备，应该是能减少运维工作的产品。整个信息化工作正从劳动密集型向技术密集型转变，用自动化工作代替重复、简单、枯燥的工作，才是理想的安全解决方案。

第四，应用环境的安全越来越不可控。

漏洞管理是安全团队的另一项重要能力。然而近年来这一任务变得越来越艰巨，漏洞数量越来越多，影响范围也越来越大。从 SandWorm 到 WireLurker，从 HeartBlood 到 ImageMagick，基础组件和平台的漏洞影响不断引发关注。然而，这些威胁影响虽广，却只是冰山一角。因为备受关注，其补救措施也会快速出现。对单个企业而言，造成严重损失的，

往往是大量已知漏洞没有及时修复，以及业务应用开发中产生的应用层漏洞。这些漏洞很难被发现，又和直接业务相关，最有可能被攻击者长期利用来获利。

应用层漏洞的数量在快速增加，这一现象背后的原因是IT环境和开发模式的变化。云计算、虚拟化、SDN、移动设备等技术的兴起，导致应用程序需要适应多样化的环境，应用本身也越来越复杂。与此同时，当前业务上线和更新的速度也远远超过以前，大部分开发团队都采用敏捷开发模式，需求和实现在一轮轮迭代中快速改变，安全很容易被归入次要特性。此外，业务快速上线的压力导致测试阶段被压缩，安全测试也往往成为牺牲品。以上这些因素导致了应用上线前的漏洞远比以前更多。

那么，应用上线之后，这些漏洞是否真的会被攻击者发现和利用？能否由安全团队逐步发现和修复呢？不幸的是，这些漏洞会被攻击者利用。如果一个应用有成为非法盈利渠道的潜在可能，攻击者在利益驱动下，就会寻找其漏洞。而他们所拥有的经验和投入的资源在单点上会远超一般的安全团队。这使得企业自身早于攻击者发现并弥补漏洞的可能性非常之低。

怎样解决上述的安全困境？ Gartner曾经提出了自适应安全架构，其中的核心是持续检测和分析，包括12种具体的安全能力。然而企业怎样实现这一架构，却是一个难题。很少有安全供应商具备如此全面的能力，可以在预测、防护、检测和响应方面都有完整的解决方案，并提供持续检测和分析平台。于是，多数用户只能采购不同来源的产品和服务，来

自行拼接出适合的平台。这是一项艰巨的任务，如果没有安全供应商间的协同，近乎是不可能完成的。信息安全是一场战争，缺乏组织的战士，无法与军队抗衡。各方力量的协同，才是信息安全制胜之道。

而协同的能力，又可以分为三个基本的层面：数据协同、产业协同和智能协同。

一、数据协同：全新的安全驱动力

数据协同是所有协同的基础。是希望能够打破数据的孤岛和数据的鸿沟。长期以来，在信息安全的攻防对抗中，防守一方总处于被动，其根本原因是信息的不对称。攻击者可以自由选择入侵的对象、时机和方法，而防守方却对这些一无所知。数据协同，就是减少这种不对称，从而提升检测能力的重要途径。

网络攻击者为了隐藏身份通常使用代理服务器作为跳板。这个跳板的更多数据，可能在另外一个国家，也可能在另外一个企业机构，没有数据协同，对攻击溯源和打击将无法彻底进行。还有，很多网络攻击如果不能对它进行深入的同源性分析，很可能会被我们忽略掉。这种分析涉及同源的样本、攻击方法、IP、URL、邮件、电话号码、联络地址以及人和机构。

前不久，360 发现并溯源了一个黑客组织对中国一些政府机构的 APT 攻击事件，就能看到这种协同的重要性。这个事件的追踪从一封含有一种漏洞攻击木马的邮件开始。表面上看这只是一种简单的威胁，在没有

情报时被当作一般病毒杀了就行。但是，当分析人员将这个木马样本通过360威胁情报中心的大数据平台进行样本同源分析后，发现了13个相关样本；又通过360多维线索分析平台，对C&C服务器及相关数据分析之后，从一批可疑的IP、URL、e-mail又关联发现了69个不同种类的同源样本，以及基于即时通讯工具和社交网络的3种攻击方法，新增受害人131个。再利用受害人的更多数据分析，一个黑客组织针对中国政府特定机构及相关人员的APT攻击全貌就还原了。这个溯源的过程就是典型的数据协同的结果，也足可以证明，数据的协同和共享，是数据驱动安全体系里最关键性的基石。

从细分的角度来看，数据协同又可以分为以下三个层次。

第一个层次是海量数据的协同。因为即使同样的数据，量级不同时，处理的方法也不同。传统的安全检测以特征和规则为基础，需要一个特征提取和规则编制过程。但随着攻击方法的丰富和复杂，这个过程的成本越来越高。大数据技术的发展，使得汇集海量数据协同分析，省略人工提取过程，成为了一种新思路：数据量级协同。例如，360的QVM杀毒引擎，采用了有穷向量机的机器学习方法，在超过100亿条样本库的基础上，不断进行迭代学习。新出现的恶意样本会被引擎自动识别，并成为下次迭代学习的基础。

第二个层次是异构数据的协同。传统SIEM和SOC产品提供关联算法和规则来检测高级威胁，同样需要人工定制的先验知识。但是以APT为代表的外部威胁越来越复杂，隐蔽性也越来越强。对企业的安全团队来说，新型攻击出现太快，使得先验知识难以获取。异构数据协同的思

路是将多个安全检测设备同时作为数据来源，进行多源数据协同分析，利用部分先验知识将微小的线索联系起来，由点及面，发现攻击行为。例如，安全业界普遍认为，传统的边界防御很难彻底地抵御入侵者。将边界和内网中的终端、应用、网络等各种行为建立画像和基线，以用户和实体为核心，使用 UEBA（User and Entity Behavior Analytics），综合利用统计模型和机器学习等方法，发现异常行为，将是更为有效的方式。

第三个层次是云地数据的协同。本地安全设备与云端威胁情报进行协同，以获取最新的先验知识。攻击者也需要考虑成本和收益的问题，一种新的攻击方法，不会只出现一次，而是会被反复使用。对于特定企业第一次遭受的攻击，在网络中可能已经反复出现并被多次发现。所以，对于本地的安全防护系统，从云端获取最新的威胁情报，将会成为基本的安全能力之一。

二、产业协同：数据驱动的安全生态体系

数据协同和智能协同可以带来安全能力的提升，但更为重要的革命将来自产业协同。协同带来的利益是双向的，一旦实现这种协同，安全供应商可以更专注独有的功能或服务，而用户将得到更强大的安全能力。

当今的战争，已经不是一个单兵作战和个人英雄主义的战场了，需要大兵团协同作战。网络安全不仅仅是一个人、一个企业的事，也不仅仅是一个国家的事。这是人类在迎接一个全新的有诱惑力的网络文明时代所共同面对的严峻问题。产业协同需要政府和企业共同推进，达成政

府间、企业间包括政府和企业间透明的、互信的协同，从而形成更安全的产业生态。

产业协同可能有以下多种方式。

第一，自发式协同，各个厂商提供 API 接口，供其他厂商和客户直接调用，目前多数国际安全企业的协同是采用这种方式。这种方式的优点是形式灵活；缺点是接口和服务质量不统一，容易造成混乱。

第二，联盟式协同，几个厂商组成对等的联盟，协商彼此交换的内容，如 PaloAlto Networks 等厂商共享威胁情报的 CTA 联盟。这种方式的优点是接口统一，缺点是同质化和封闭性。

第三，生态式协同，不同类型的厂商，有组织地形成一个生态系统，采用开放透明的平台提供服务。这种方式的优点是稳定性和包容性，缺点是需要足够开放稳定的平台。

有国外研究机构的报告认为，“到 2019 年，全球 2000 强企业 50%的对外服务和解决方案花费，将通过不到十家组织生态系统的战略供应商提供。”采用生态系统供应商有诸多优点。首先，每类安全产品或服务都会有多家供应商在生态系统内，彼此良性竞争，可以为用户提供更多样化的选择。其次，由于安全产品和服务的种类在不断增加，彼此的联动也越来越复杂，生态供应商负责组织彼此间的协同，可以大幅提高管理效率。最后，对于不断涌现的新兴厂商提供的先进技术，企业客户自身去尝试会面临较大的风险和代价，由生态供应商逐步尝试，就可以减少这种风险。

安全技术的复杂性给客户带来了诸多怀疑，而生态供应商想要赢得

企业客户，就必须提供一个开放、公正的平台。只有这样才可能形成良性循环，就像消费者市场中的苹果生态系统，最终为消费者提供了高质量的服务，同时使应用开发商和平台方提供方获利。

360 企业安全正在与合作伙伴共同建设一个开放透明的“安全生态体系”，提供给客户动态可扩展的安全能力，提供给供应商统一平台和开发的接口。这个“安全生态体系”兼容不同厂商提供的产品和服务；由大数据技术支撑的安全平台统一进行管理，平台可以部署在用户本地，也可以部署在云端，甚至支持混合部署；用户可以从“安全应用市场”中下载各种应用；安全厂商和增值服务厂商在平台上发布应用，可以对本地数据和云端威胁情报进行关联分析，或是将本地功能和云端服务进行协同联动，从而提供更强大的安全功能。

三、智能协同：机器和人类的智能提升

前面说的数据和产业协同都是实际操作层面的，而智能协同则是一种更高层面的协同。在 2016 年的 DEFCON 上，美国国防部组织了一次“机器黑客”大赛，比赛中，“机器黑客”代替人类来挖掘对手系统的漏洞并发动攻击，同时还要确保自身的安全，随时补上自己的漏洞。这个比赛表面上看是机器算法的攻防比拼，背后其实需要高性能运算系统、人工智能专家、漏洞挖掘专家、安全防护专家的高度协同。从世界范围内发生的多起安全事件看，还需要更多领域的专家参与到协同里来，不同的领域、设备、行业之间都需要进行不同维度的协同。这个协同，是超过

企业层面、行业层面、领域层面、区域层面的协同，甚至超越国家层面的协同。

信息安全是一场战争，面对纷繁复杂的信息情报，如何正确决策与响应，是每个安全团队面临的难题之一。智能协同，将机器和人类的智能联系起来，获得能力提升，将是人工智能时代新的安全解决之道。

具体来说，智能协同也可以分为以下三个方面。

第一个方面是“机器 + 机器”。面对越来越复杂的网络和安全场景，往往需要多个产品或设备的协同，才能完成响应活动。这些协同包括了本地设备之间的协同，包括本地设备和云端服务之间的协同，也包括检测设备和响应设备之间的协同。提升安全自动化的途径之一，是建立“机器 + 机器”的智能协同，大量基础的响应工作由机器之间自动协同完成。就如同人类的自主神经系统，无须有意识地下达指令，就可以自动控制脏器运作、血液循环和腺体分泌等活动。

第二个方面是“机器 + 人”，以强化安全事件的分析能力。当前安全业界的一个共识是，单纯依靠自动化识别或人工智能，无法有效识别复杂入侵者的行为。无论是 FireEye 还是 Palantir 这样的公司，都采用了“机器辅助 + 人工分析”的方式，其实是一种“机器 + 人”的智能协同。例如，在 APT 发现和溯源过程中，需要对现场线索和海量数据进行自动化关联分析，同时由多位安全研究员进行人工协同分析。把机器的运算和效率，与人类的经验与智慧相结合，将分析能力推至极致。

第三个方面是“人 + 人”。机器智能在特定场景中的确存在优势，但人类智能的潜力更是无穷的，能够挖掘出这种潜力，就可以获得强大的

“人 + 人”的智能协同。例如，应用漏洞是企业面对的重要安全问题之一，而一般的安全团队由于缺乏攻击者的视角，很难发现这些漏洞。到目前为止，解决这个问题最有效的方式是利用社区力量，采用众测模式公开悬赏来进行发现。由于大量白帽子熟悉攻击者的技巧和方式，所以更适合这种持续的漏洞发现工作，不同个体之间的技术和思路存在的差别，也让这种测试更全面。2016 年 3 月，美国五角大楼花费 15 万美元，与 HackerOne 平台合作进行众测项目“攻陷五角大楼计划”。众位白帽子也不负众望，发现了 100 多个漏洞。而国内的补天、乌云等平台，也对漏洞的发现和修复做出了大量贡献。

结　　语

除了上述三个具体层面的协同外，协同联动的概念可能还包含着更多，更广阔的含义，这里未能尽述。例如，我们可能还需要全球互联网政策层面的协同：全球范围的网络诈骗泛滥，很重要的原因是网站真假难辨。数字签名技术在欧美等发达国家已经普及，但在包括中国在内的发展中国家普及率不及 10%；再比如对漏洞的管理、扫描器的管理、对僵尸网络的治理等，也都需要全国各地，甚至全球各国政策的协同。

协同联动是一个含义丰富，但同时又充满挑战的新型安全理念。其真正的挑战或许并不在于对这个概念本身的理解和技术实现的方法，而在于整个安全产业界如何才能下定决心消除彼此之间的商业壁垒，共建一个开放透明的合作平台。

大数据技术的发展已经为安全行业注入了新的活力，这为解决无穷无尽的安全问题带来了一丝光明的希望。然而，比起对面的攻击者，自身的怀疑才是我们最大的敌人。利用安全协同的力量共创春天，还是在孤独中的面对寒冬，是或不是，这是一个问题。