网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

微软安全机制演进的启示

安天研究院

威胁框架：认知与实践

寒夜远征

操作系统软件代码数量巨大，复杂程度高，存在缺陷的可能性非常大。微软公司以其强大的综合能力维系了一个稳定而功能强大的产品，为国产操作系统的成长提供了重要的参考。

寒夜速记

CONTENTS

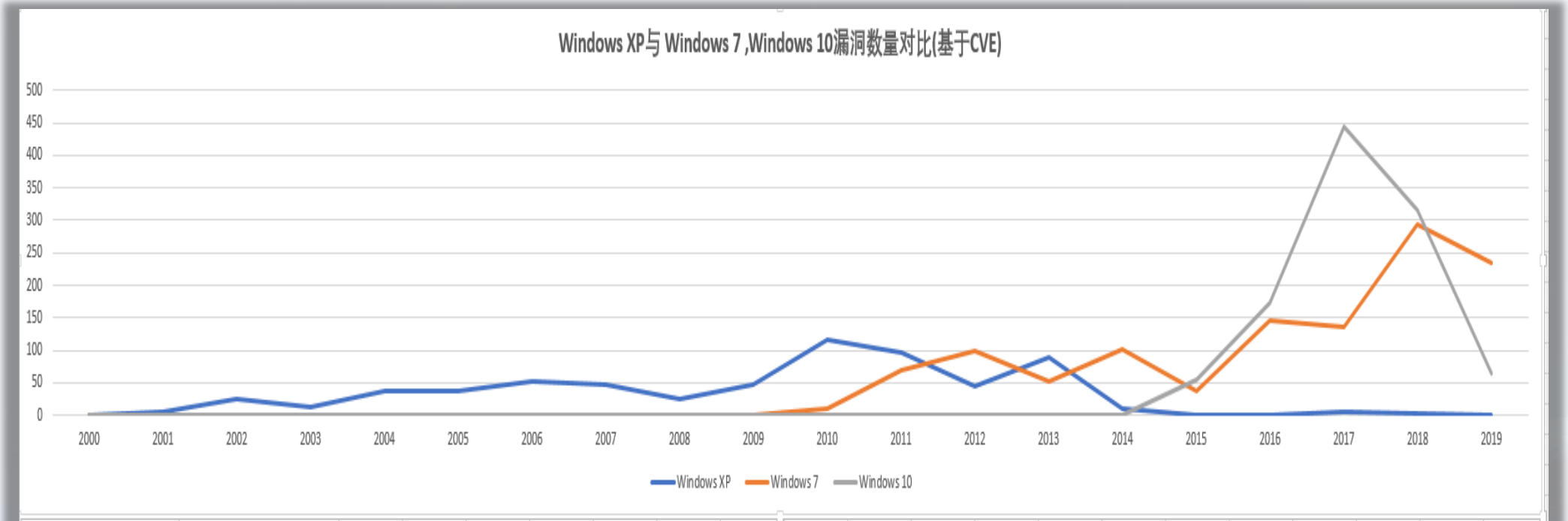
目 录

寒夜速记

威胁框架：认知与实践

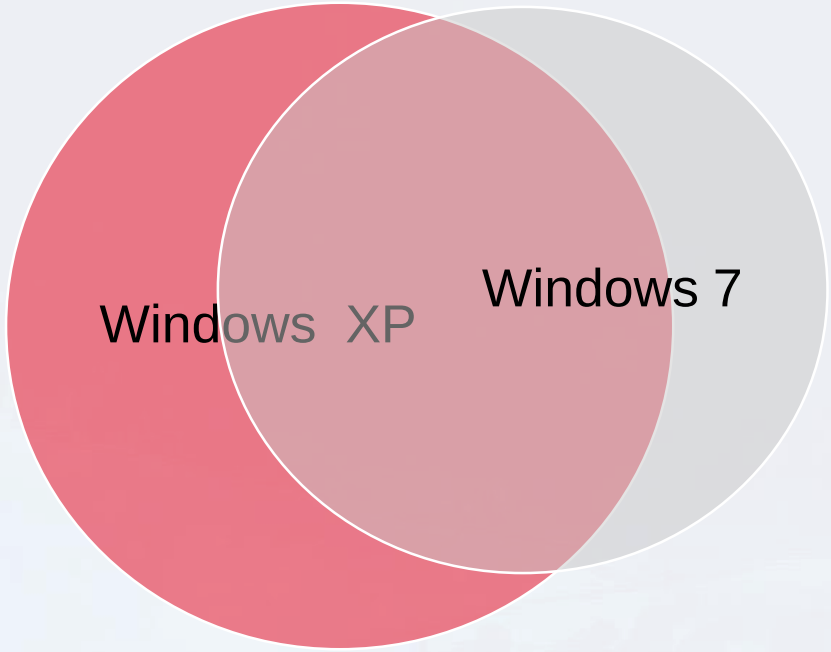
01 从Windows的漏洞曲线说起

从Windows的漏洞曲线说起



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Windows XP	0	4	26	12	37	36	52	46	25	48	117	97	44	88	9	0	0	6	2	0
Windows 7	0	0	0	0	0	0	0	0	1	0	11	69	99	53	102	37	145	136	295	234
Windows 10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	54	174	444	317	65

从Windows的漏洞曲线说起



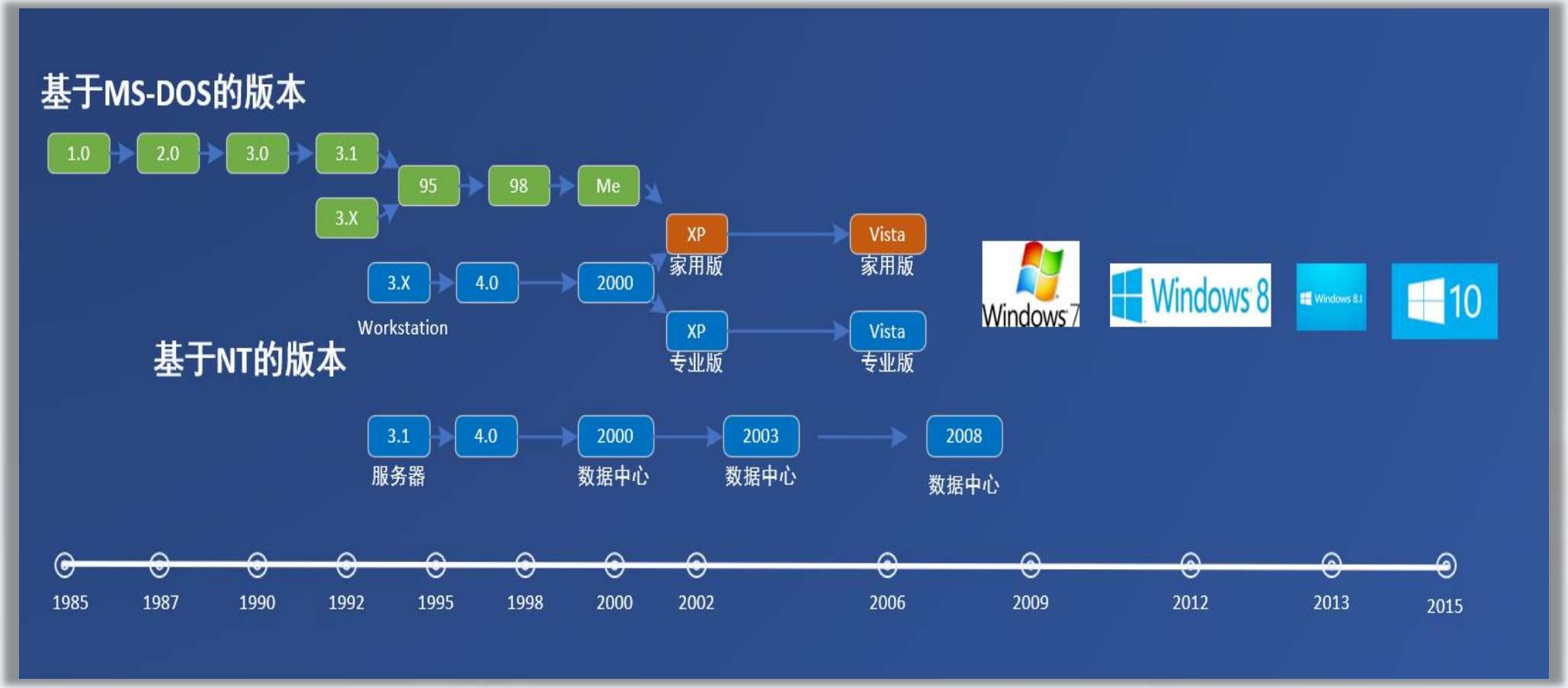
2009-2013

Windows XP 系统漏洞 422

Windows 7系统漏洞 331

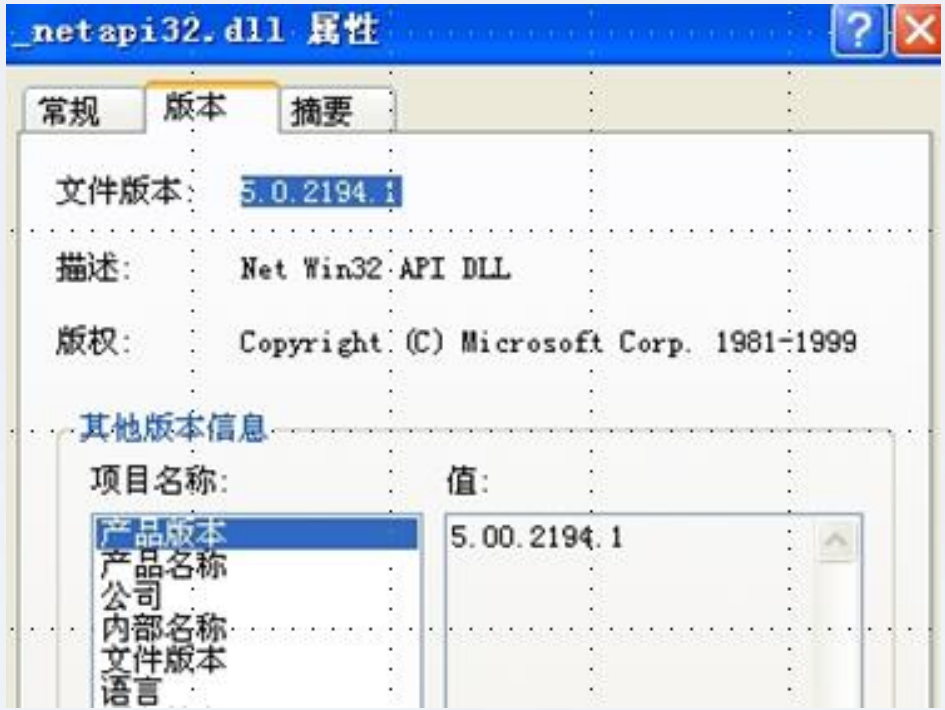
其中重叠漏洞 257

自WinXP开始的Windows桌面操作系统都是NT架构系统



补丁比对是最常见漏洞定位的方法

- 以在XP系统根据补丁寻找MS08-067的溢出点为例
- Microsoft 安全公告 MS08-067 ((CVE-2008-4250)

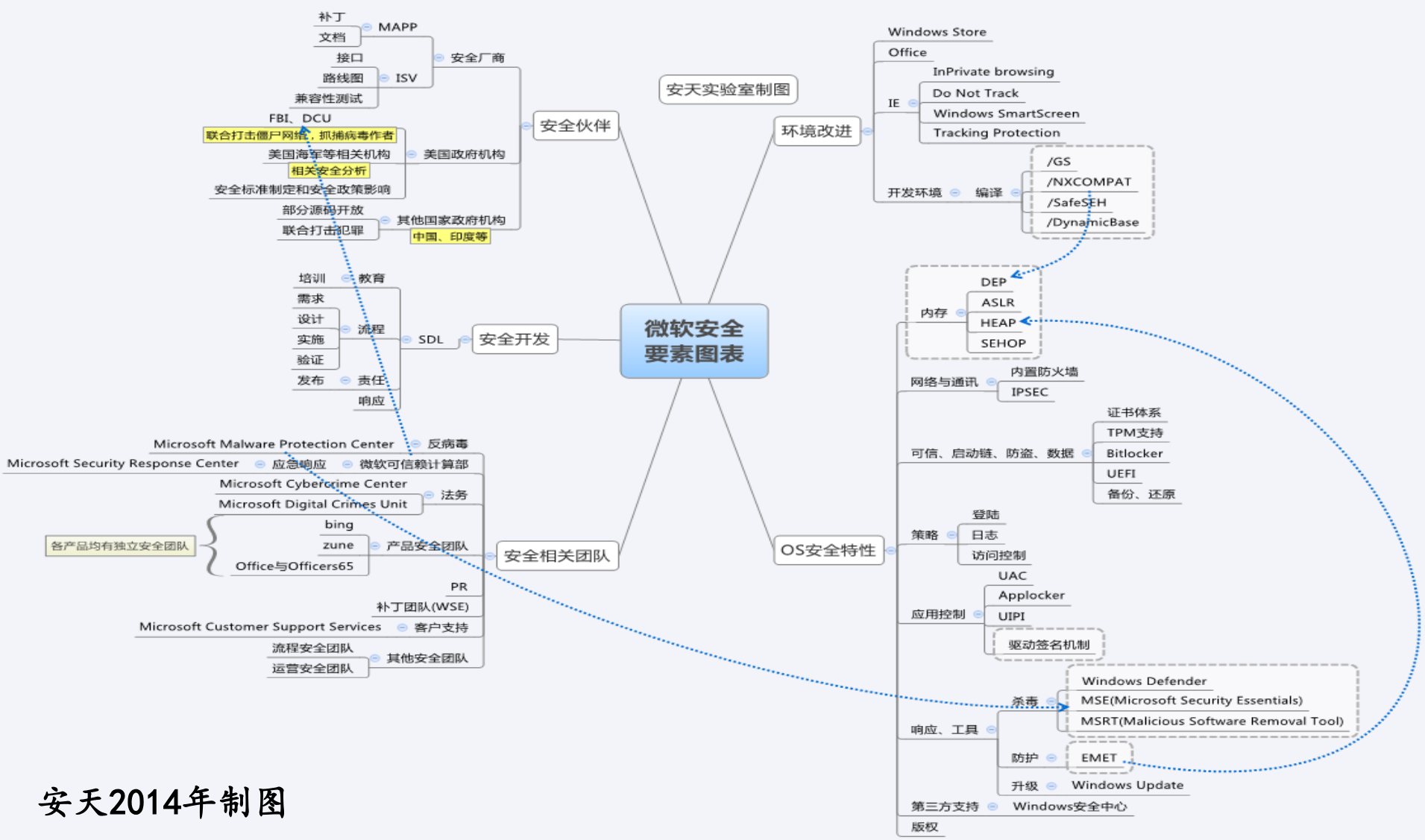


寒夜速记

威胁框架：认知与实践

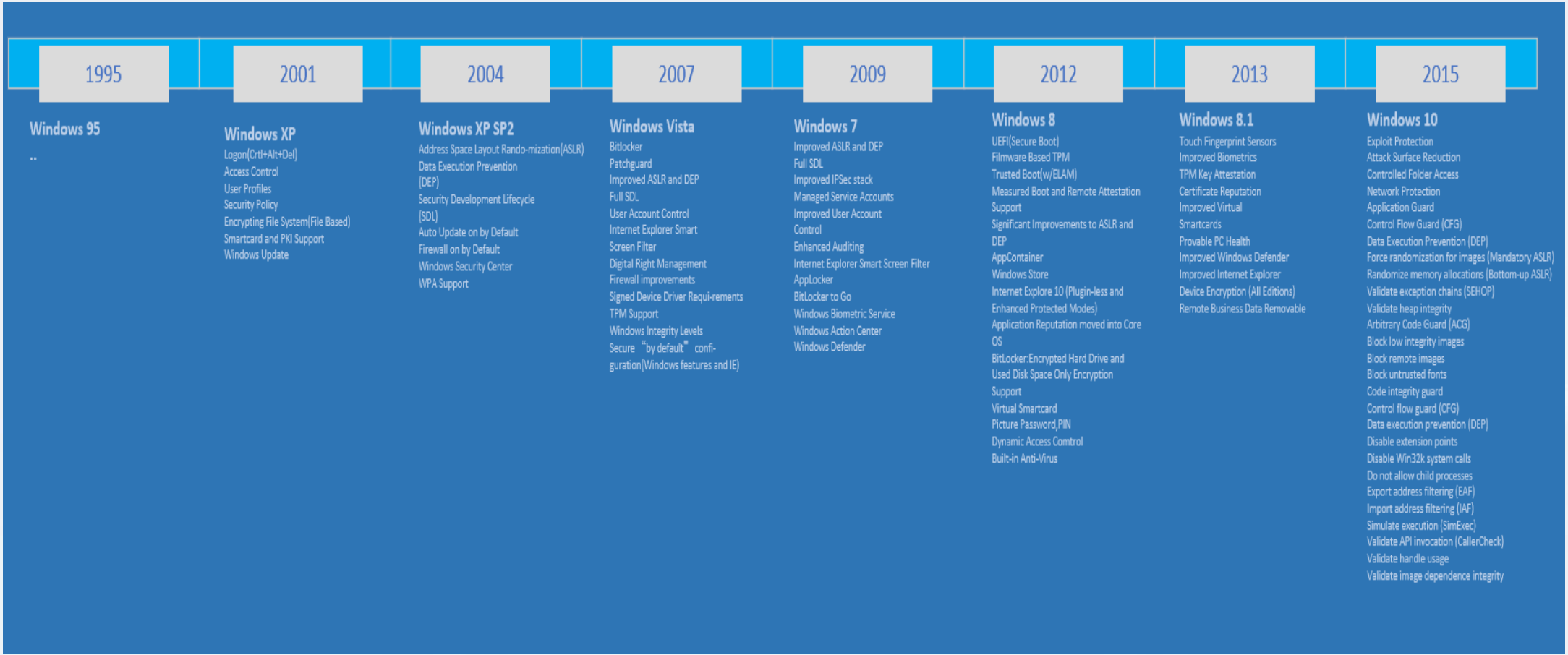
02 微软安全机制的现状与演进

微软安全机制的现状与演进

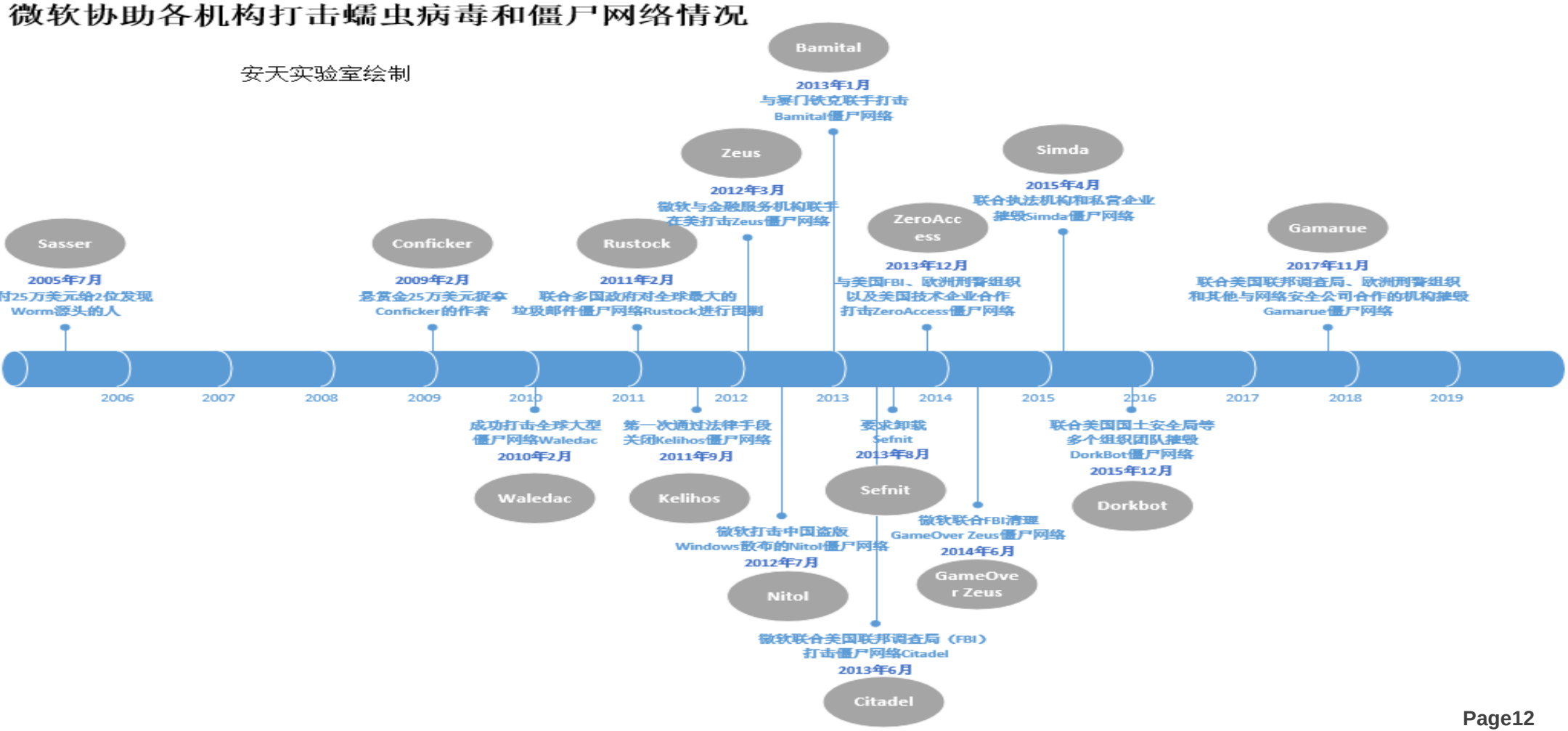


安天2014年制图

操作系统安全特性的演进



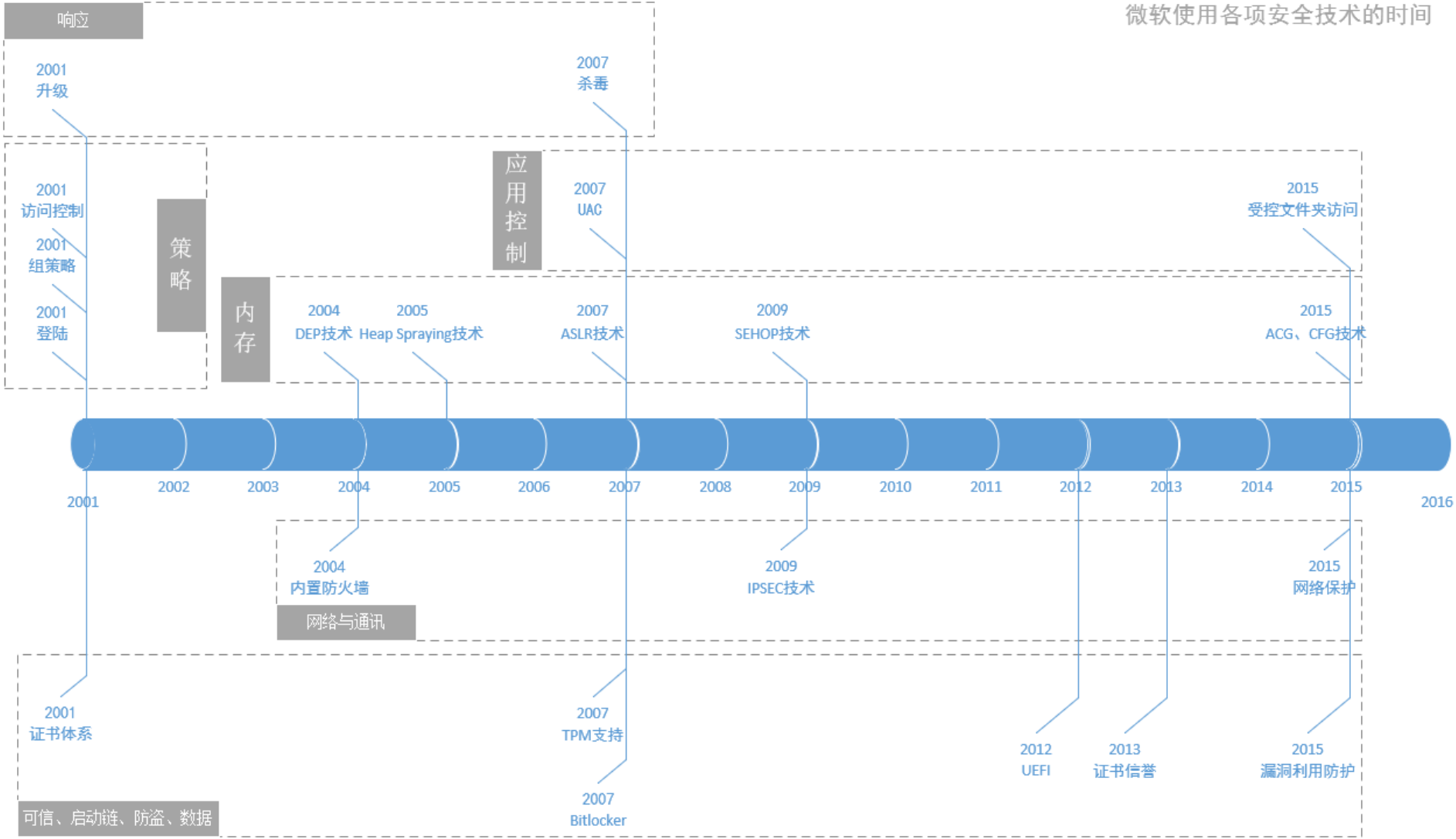
政府协作：持续的犯罪打击



微软SDL(Security Development Lifecycle）流程

- 微软SDL(Security Development Lifecycle)流程，是一种专注于软件开发安全保障的流程，为了实现保证最终的用户安全，在软件开发各阶段中引入安全和隐私保护。

微软各项安全技术使用时间轴

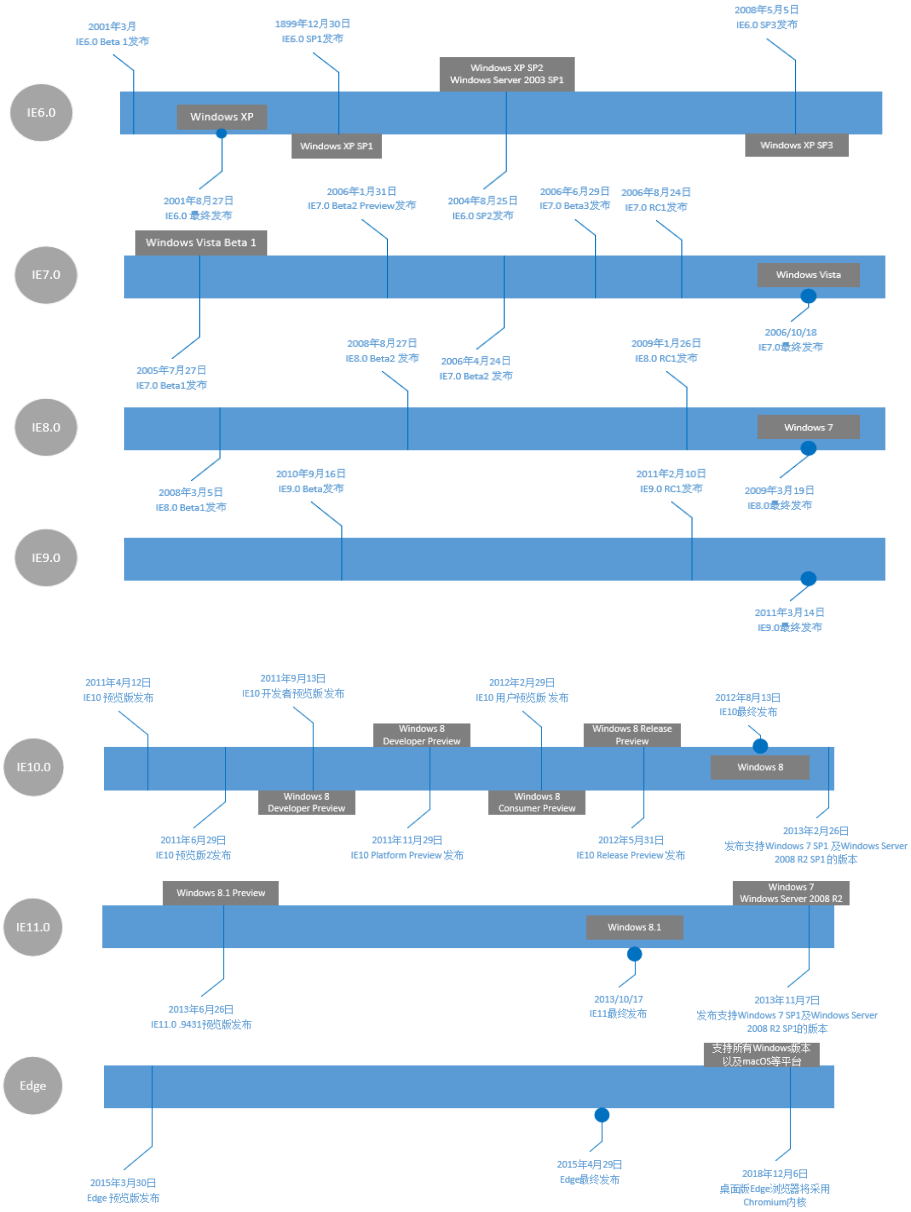


微软安全机制的现状与演进

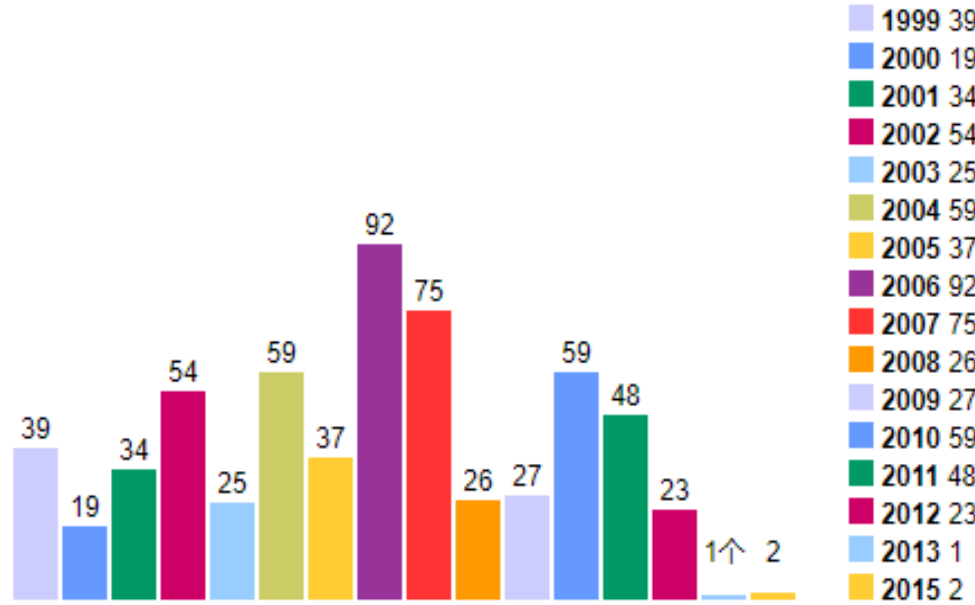
版本	发布日期	重要变更／事项	一同发布的产品
1	1995年8月	首发布版本	Plus! for Windows 95
1.5	1996年1月	兼容于Windows NT 3.5	
2.0 Beta	1995年10月	支持HTML表格、框架和其他组件	
2	1995年11月	新增SSL、Cookies、VRML及互联网新闻组	Windows NT 4.0 Windows 95 OSR1 Internet Starter Kit
2.01	*没有数据*	错误修正发布版	
3.0 Alpha 1	1996年3月	改进对HTML表格、框架、MIDI音乐、GIF动画和其他组件的支持	
3.0 Alpha 2	1996年5月	支持VBScript和JScript	
3.0 Beta 2	1996年7月	支持CSS和Java	
3	1996年8月	最终发布	Windows 95 OSR2
3.01	1996年10月	错误修正发布版	
3.02	1997年3月	错误修正发布版	
3.03	*没有数据*	错误修正发布版	
4.0 Beta 1	1997年4月	改进对CSS和Microsoft DOM的支持	
4.0 Beta 2	1997年7月	改进对HTML和CSS的支持	
4	1997年9月	改进对HTML和CSS的支持	Windows 95 OSR 2.5
4.01	1997年11月	错误修正发布版	Windows 98
5.0 Beta 1	1998年6月	支持更多CSS2的功能	
5.0 Beta 2	1998年11月	支持双向文字、旁注标记、XML／XSL及更多CSS的属性	
5	1999年3月	最终发布，支持Windows 3.x和Windows NT 3.x的最终版本	Windows 98 SE
5.01	1999年11月	错误修正发布版	Windows 2000
5.5 Beta 1	1999年12月	支持更多CSS的属性、框架支持的小改进	
5.5	2000年7月	最终发布，支持Windows 95的最终版本	Windows Me
5.6	2000年8月	针对Windows Whistler build 2257（Windows XP）的发布	Windows Whistler（现Windows XP）

在浏览器演进史中，进一步呈现了XP2的安全转折点效应

微软安全机制的现状与演进



2001，引入漏洞修补
2004，弹窗、ActivX封锁、组件管理
2006，版权强化
2008，连接诊断，隐私浏览，黑名单过滤，跨站和其他XSS攻击对抗。
2010，追踪防护
2011，HTML5沙箱，追踪保护
2015，Microsoft Edge取代IE浏览器



cvedetails网站提供的IE漏洞数量统计

微软的应急体制


Watch
The MSRC and its partners are always on the alert for threats.
Alert and Mobilize Resources
When a threat is identified, engineers and communications professionals are paged and mobilized.
Assess
The engineering team investigates the issue and works with the communications team to develop guidance for customers nd
Stablize and Recover
The communication team provides guidance to customers, while the engineering team develops the solution.
Resolve
The MSRC provides tools and solutions, and the Watch phase resumes.

微软对安全团队&安全公司的并购史

公司&团队名称	Logo	公司&团队简介	并购时间
安全软件开发公司 XDgrees			2002年9月
罗马尼亚反病毒企业 GECAD公司	gecad .mind for innovation	该公司成立于1992年，主要专注于安全相关的软件开发，尤其是反病毒软件。	2003年6月
反间谍软件开发商 Giant		该公司是生产反间谍软件以及互联网安全产品的企业。	2004年12月
以色列VPN安全公司 Whale Communications	Whale Communications	该公司位于以色列的罗斯艾因城，专营安全专用设备，这类设备的特点是当员工处于公司防火墙之外时，可通过这类安全专用设备实现对应用程序的访问。公司成立于1998年，分别在美国、英国和法国设有办事处。	2006年5月
反病毒软件开发商 Sybari	Sybari	该公司位于美国纽约，为多家安全厂商提供反垃圾邮件及反病毒解决方案。	2005年6月
信息安全公司Komoku	KOMOKU	Komoku是一家新兴安全公司，成立于2004年，主要开发进行rootkits、malicious探测的安全软件产品。Komoku的客户多为高级别要求用户，其中包括美国国土安全部、国防部以及美国的国防先进技术研究计划署。	2008年3月
FrontBridge Technologies	FRONTBRIDGE Email Security for Enterprises	该公司管理提供的外包服务帮助企业过滤进入企业的电子邮件和即时通信中的病毒，并保证他们的内容不违反相关的法律规定。	2005年7月

微软对安全团队&安全公司的并购史

公司&团队名称	Logo	公司&团队简介	并购时间
以色列安全公司 Aorato	AORATO	该公司是由以色列国防军技术部门的老兵于2012年创立，总部位于赫兹利亚(Herzliya)，拥有约10名员工。其所开发和销售的软件可监控企业IT系统中央通讯组件的访问情况，并以此判断是否出现了未授权访问。	2014年11月
以色列安全公司 Adallom	ADALLOM	该公司创建于2012年，总部位于美国加州帕洛阿尔托市(Palo Alto)，但研发和运营中心位于以色列特拉维夫市。	2015年9月
以色列安全初创公司 Secure Islands	secure islands	该公司的技术可以增强 Azure 版权管理服务的数据保护能力，以提供灵活的体系结构，满足最严格的保护。	2015年11月
以色列网络安全公司 Team8	TEAM8 Rethinking Cyber	该公司是以色列一家网络安全初创企业，专注于为网络安全提供解决方案，英特尔作为Team8的战略合作伙伴，基于欺骗性的网络安全从软件扩展到硬件，致力于解决网络安全问题。	2017年1月
网络安全公司 Hexadite	HEXADITE Intelligent Security Orchestration and Automation	该公司总部位于波士顿。公司的主要技术是自动识别网络攻击并迅速做出正确的反应。该系统能够连接到多个来源的警报信息，并帮助公司内部的网络安全人员管理和优先处理潜在威胁。	2017年6月
软件安全公司 BlueTalon	BlueTalon	该公司成立于2013年，公司位于加州 Redwood City。BlueTalon是一家为现代数据平台提供统一数据访问控制解决方案的领先供应商。BlueTalon与全球财富100强企业合作，消除数据安全盲点，获得数据的可见性和控制权。	2019年7月

寒夜速纪

威胁框架：认知与实践

03 微软和其他阵营的对比思考

微软各OS版本年度漏洞情况

时间 数量	Windows 2000	Windows NT	Windows XP	Windows server 2003	Windows vista	Windows Server 2008	Windows 7	Windows RT 8	Windows 8	Windows Server 2012	Windows Server 2016	Windows 10
2000	24	17	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2001	39	24	4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2002	35	19	26	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2003	21	19	12	5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2004	26	19	37	21	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2005	43	7	36	18	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2006	52	5	52	7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2007	47	4	46	10	35	1	1	N/A	N/A	N/A	N/A	N/A
2008	34	3	25	6	17	1	N/A	N/A	N/A	N/A	N/A	N/A
2009	60	N/A	48	22	17	14	11	N/A	N/A	N/A	N/A	N/A
2010	42	1	117	50	65	68	69	N/A	N/A	N/A	N/A	N/A
2011	1	1	97	82	88	95	99	N/A	N/A	N/A	N/A	N/A
2012	N/A	N/A	44	42	47	51	53	N/A	18	6	N/A	N/A
2013	N/A	N/A	88	81	94	103	102	N/A	69	60	N/A	N/A
2014	N/A	N/A	9	25	34	38	37	N/A	37	36	N/A	N/A
2015	N/A	N/A	N/A	62	135	148	145	4	153	153	N/A	54
2016	N/A	N/A	N/A	N/A	130	132	136	135	155	155	39	174
2017	N/A	N/A	6	5	70	297	295	254	293	296	386	444
2018	N/A	N/A	2	1	3	171	234	128	178	179	261	317
2019	N/A	N/A	N/A	N/A	N/A	17	114	19	20	19	24	65

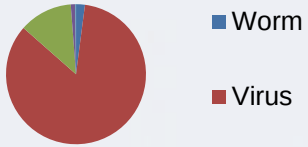
Linux的漏洞情况

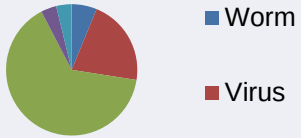
时间 数量	Linux Kernel	Redhat Linux	Gentoo	Ubuntu	Debian	Suse	FreeBSD
2000	7	48	0	0	16	18	27
2001	22	49	0	0	33	21	35
2002	16	23	0	0	8	9	29
2003	19	37	4	0	10	4	13
2004	58	48	46	5	21	33	15
2005	109	99	79	44	52	83	16
2006	94	11	3	9	12	9	27
2007	76	38	8	5	12	10	6
2008	76	36	7	3	26	4	14
2009	112	17	0	8	10	1	11
2010	153	40	0	1	6	1	8
2011	145	35	6	3	5	1	10
2012	71	44	4	0	11	0	6
2013	172	191	4	1	17	2	12
2014	35	71	0	3	12	5	2

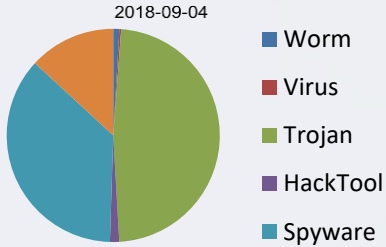
格式文档溢出的统计

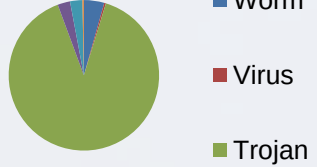
时间 数量	Excel	Word	PowerPoint	Visio	SWF格式相关	PDF格式相关	Adobe Flash(flash相关)
2000	3	1	1	N/A	N/A	3	N/A
2001	1	3	2	N/A	N/A	N/A	N/A
2002	5	3	1	N/A	1	3	N/A
2003	1	3	1	N/A	N/A	3	N/A
2004	2	5	N/A	N/A	1	7	N/A
2005	3	6	N/A	N/A	N/A	15	N/A
2006	21	14	18	N/A	3	13	4
2007	21	7	2	2	4	30	15
2008	28	14	17	2	5	35	21
2009	27	12	33	3	6	78	25
2010	40	19	26	4	5	34	66
2011	35	1	18	4	5	44	66
2012	13	4	2	7	10	32	70
2013	5	13	N/A	2	21	31	58
2014	4	13	1	N/A	9	37	77
2015	25	17	6	1	4	41	339
2016	33	21	5	2	9	86	256
2017	18	10	6	N/A	29	148	70
2018	38	34	8	N/A	19	184	26
2019	22	10	4	N/A	5	122	7

2000～2018数据分析





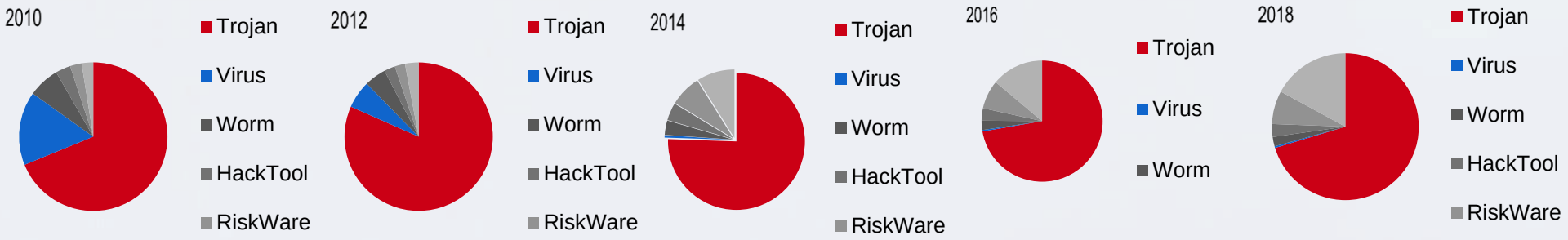




日期/分类	2000/10/24	2006/11/10	2012/11/27	2013/11/04	2015/06/25	2018/09/04
Worm	512	8109	354049	435247	149137	101674
Virus	21006	27760	29940	30060	29397	29980
Trojan	3066	84811	7262094	8423751	3283882	5289006
HackTool	260	4968	217502	301076	153493	154800
Spyware	37	4899	214570	340751	622344	4013384
RiskWare	0	88	25800	201401	458035	1451458

来源：Kapersky对应日期病毒名变种列表

2010～2020数据分析



日期/分类	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Trojan	105856	191344	351168	2781524	4654026	6679871	7473987	8508125	9260840	9508162	10338715
Virus	24688	25090	25927	30496	34915	37658	39567	40623	48065	41348	49430
Worm	10473	14914	20335	172832	208851	240974	255247	261843	271410	270359	276946
HackTool	5043	7690	10323	207639	257627	328041	342796	356414	372576	375374	385361
RiskWare	3887	6868	9705	38226	457698	641942	795007	902246	965398	995355	1055493
GrawWare	3874	5739	12736	105309	548852	1102948	1436328	1898963	2249846	2432708	2640863

来源：安天自主样本捕获体系统计

微软和其他阵营的对比思考

- 没有Linux无病毒神话
- 开源并不导致安全
- 不要把安全性押宝于开源
- 更不要把安全性押宝于对开源的闭源化处理
- 安全有其基本基本规律

寒夜速记

威胁框架：认知与实践

04 操作系统安全问题的思考

操作系统安全问题的思考

- 2013年：进入国产化开发领域
- 2015年：与国产化操作系统厂商进行**代码级**合作
- 2016年：国家保密局发起的ZYJ**万套示范项目**，安天是当时**唯一**的防病毒软件提供商
- 2018年5月：入围涉密专用信息设备适配软硬件产品名录**（一期名录）**
- 2018年11月：入围涉密专用信息设备适配软硬件产品名录**（二期名录）**

- **投入最早**

安天于**2013年**进入国产化配套软件和防病毒领域。2015年，在国家相关部门的统一规划下，安天分别与中标麒麟、中科方德、银河麒麟等国产化操作系统厂商进行了**深入的代码级合作，实现了安天智甲的预装试点**。

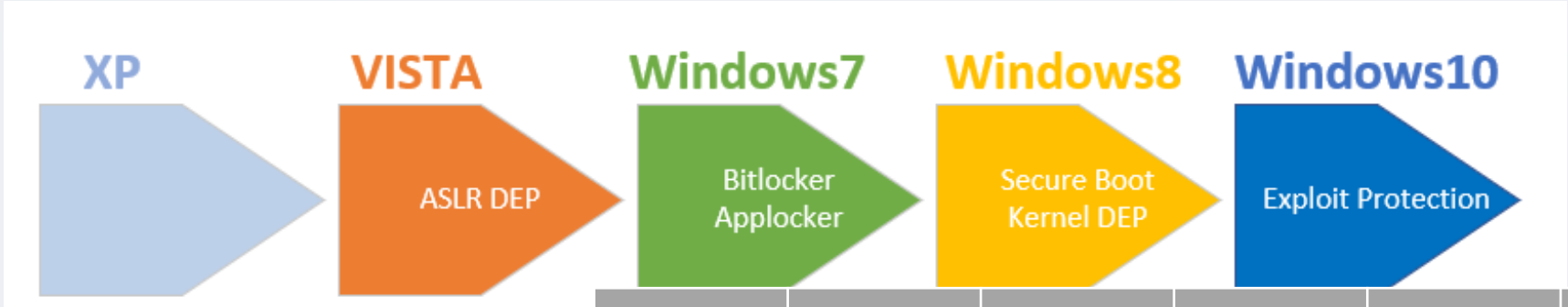
- **运行稳定**

2016年，安天智甲成功支撑了**“型号首批万套部署”**，产品运行稳定、效果良好，获得了**主管部门的高度认可**。

- **适配全**

按照“国产化硬件+国产化操作系统”的双国产组合计算，智甲已实现**对近百种版本的环境良好适配**，并且与**中标麒麟、银河麒麟、中科方德、达梦数据库**等厂商的产品具有兼容互认证明。

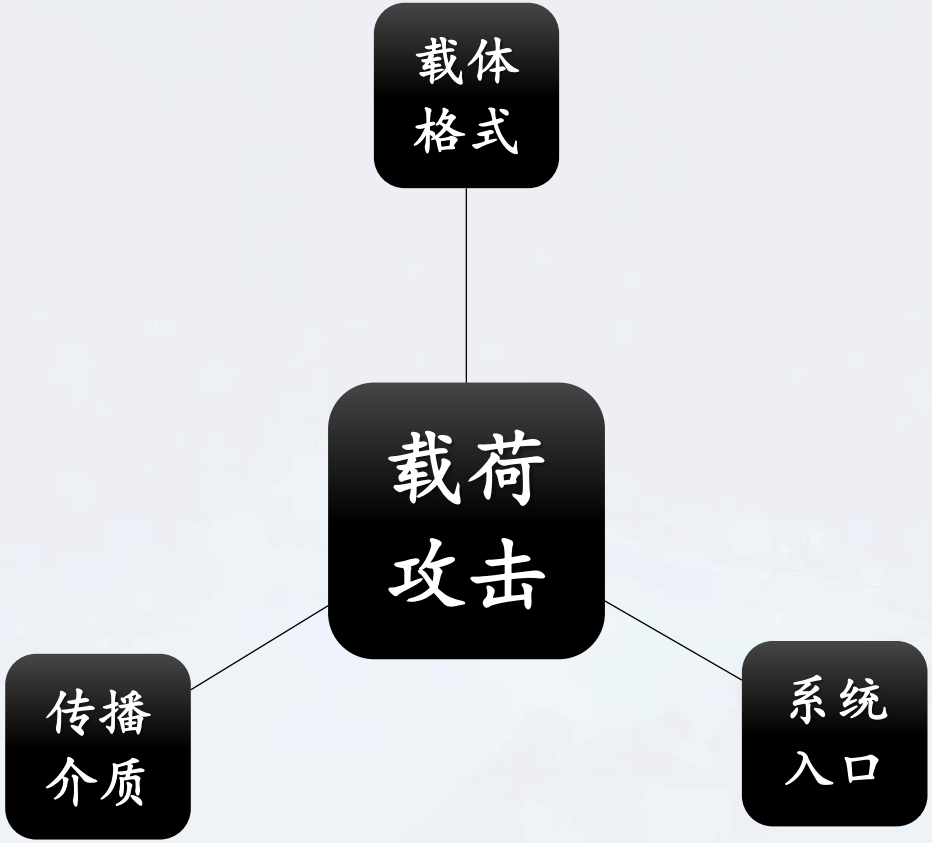
操作系统安全问题的多层次性



	XP	XP SP2	Vista	Win7	win8	win10
ASLR		支持	增强	增强	重大提升	增强
DEP		支持	增强	增强	重大提升	增强
SDL		支持	完整	完整版	完整版	完整版
Firewall		支持	升级	升级	升级	升级
Bitlocker			支持全部 磁盘加密	支持全部 磁盘加密	支持可选 磁盘空间加密	支持全部 磁盘加密
UAC			只有开/关	4个档位 可调节	4个档位 可调节	4个档位 可调节
AppLocker				支持	支持	支持
UEFI (Secure Boot)					支持	支持

仅就单点攻防特性来看，个人操作系统的安全增强与改善是事实，尽管其中的一部分也被攻击手段和能力的丰富与提升对冲掉了。

从载荷攻击看安全的规律



- 应用可以运行，攻击载荷即可运行
- 应用可以签名，攻击载荷即可签名
- 用户可以登录，攻击者即可尝试

……

- 恶意代码与正常程序的区别，没有数学级形式化方法，攻击者和正常用户间，就更不可能有这种形式化方法
- 不要寻觅永动机

陷阱-忽略安全基本规律

- 国产化降低了产品本身的带有主观恶意的可能性，但并不必然增加（甚至短时间可能降低）国产信息系统常态攻防层面的安全性，必须进行改进。
- 安全不可能一劳永逸。
- 信息产品安全性取决于大量相关因素

安全规范的开发组织过程	开发者的安全素质意识和代码质量	安全层次和权限模型的设计	上层整体的防护机制
配套的安全产品和工具聚	代码审查	持续的修补、长期维护	

- 产品安全性对比更多的是上述能力的博弈。

陷阱-忽略安全基本规律


微软安全层次
2014.5.21 安天实验室绘制
对外支撑能力
补丁体系
应急响应
开发环境
应用平台
操作系统核心
安全特性
浏览器
产业伙伴
资深安全团队
体系和建设
并购扩张
政府协作

强化开源社区互动能力

问题

- 既必须依赖于开源OS，同时又对开源社区本身的运行规律缺少了解，更缺少有效的输入和互动能力。
- 追求每行代码都自己编写的小农式安全观依然有较大市场，导致假原创，真抄袭的局面比比皆是，事实上增加了不透明性和相关的连带风险。
- 对可能由开源引入风险的情况恐慌，但又没有足够扎实持续性的工作去降低相关的风险。

建议

- 建立与国产OS相关的内核代码同步与保护机制；
- 建立中国的开源社区，在与国际开源代码融合的基础上，保持自身特有的独立性，防止“断供”；
- 提升与开源社区的互动，国产OS采用的代码必须经过安全验证，并加以保护，同时增加对开源社区的贡献度，提高话语权；
- 形成对开源代码的持续性审计分析能力和漏洞挖掘发现能力。通过全生命周期的安全理念，对冲可能由开源引入的风险。

版本管理：控制碎片化

问题

- 目前龙芯、飞腾、申威、兆芯等多种不同体系架构的CPU与中标麒麟、银河麒麟、深度等国产系统形成非常复杂的交叉组合关系；
- 同时各OS存在着大量定制版，碎片化极为严重，导致难以形成高效的补丁分发机制，在面对出现严重漏洞和其他脆弱性问题的时候，运维成本极大；同时也极大提升了相关安全防护软件的适配成本。

建议

- 对国产化CPU进行不同方向的针对性引导，如：针对嵌入式应用、桌面应用、云和虚拟化应用，形成有侧重点的差异化局面。避免多个小生态劣质竞争。
- 对OS进行相应的战略整合，鼓励定制，但应避免无节制地大量的定制分支。
- 强化版本管理，逐步收敛已有版本，降低基础软件生态中的成本。

借鉴SE Linux经验，打造高安全性OS

问题

- 虽然国产OS做了部分的安全性验证和工作，但是从目前来看，依然缺少可用于高等级防护场景的版本。相关所谓的安全版本或本身稳定性可靠性极差，或只是应用了某种单点的安全手段。
- 从整体上来看，缺少类似美国情报部门为自身高安全应用打造的SE linux级别的OS版本。

建议

- 借鉴SE Linux经验，为通用化OS建立一整套安全加固机制和安全中间层，形成完整系统的安全控制和防御策略，在保证底层内核能修补更新的同时，建设一个相对独立的安全层次，以此版本服务更高场景等级的安全系统。

支持、建设完善的安全响应能力

问题

- 当前国产OS中，从补丁升级、风险阻断等方面，基于大规模政企级应用的考量极弱，几乎全部成了孤岛型的系统。
- 安全的OS不应打补丁等错误观念依然存在。
- 从既有的部署情况来看，国产OS都没有做好应对高级别的网络攻击准备。

建议

- **补丁机制：**必须建立起完善的补丁升级机制，安全策略分发机制，快速处理响应机制，作为OS内嵌的安全能力。
- **安全运维平台：**建立起对于内网大规模补丁分发的系列支持，以弹性的安全配置策略和不同场景下的安全策略模板来保证在不同安全场景下的基础安全性。

倡导供应链透明化

问题

- 大量软件产品以开源代码为基础汉化或改进编写，或在部分功能上借鉴引用开源代码，或者使用第三方模块，但从客户到相关部门完全不了解相关情况。
- 在开源软件、第三方模块或中间件出现安全问题时，能否及时修补用户侧漏洞，完全看厂商自身敏感性、能力和责任心，导致安全风险持续传递、扩散。

建议

- 建立鼓励供应链透明化的机制，并对高安全需求场景建立强制化的供应链透明机制，要求软件产品厂商报备披露其应用开源代码、模块、应用第三方中间件等情况。对其中重要的第三方中间件要进行穿透披露。
- 国家相关机构建立更完善的开源软件和中间件安全分析机制，绘制完整的利用和继承关系图谱。建立起更完善的供应链威胁情报共享机制，强化强制性改进要求，在出现风险隐患时可能快速传递修改。

建立可靠可信的软件供应链

问题

- 目前对国产化软件生态链的强化型安全要求不足，包括WPS Office、国产浏览器等安全能力需要提升。
- 目前国产系统软件和应用软件都缺少一致且可靠的证书验证机制，和配套实现。

对策

- 对桌面应用，在办公Office软件、输入法、浏览器等配套环节上，必须进行安全要求强化，增强安全测试，提升安全响应速度。
- 建立起完整的国产软件的证书签名机制。
- 建立起企业/机构应用商店机制。

研发生产和环境安全考虑

问题

- 对外方通过网络、人力和其他物理手段入侵我研发生产环境，弱化代码质量，设置缺陷的敌情想定准备不足。
- 从整个系统研发过程缺少全生命周期的安全机制。

建议

- 综合考虑基础软硬件安全的现实风险，加强人员、环境、技术多方面的安全能力保障，将基础软硬件研发环境作为高安全需求场景，建设动态综合的安全防御机制。
- 推动全生命周期的安全规划、研发、测试、响应机制，建立SRC机制，应对相关安全风险。

网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

敬请批评指正

寒夜远征

威胁框架：认知与实践