



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

智者安天下

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

安天科技集团 肖新光

威胁框架：细粒度对抗

長纓縛展

長纓待展

CONTENTS

目 录

01

从安天自己的“产品矩阵”说起

02

从安全产品演进看“赛道”是怎样形成的

03

从威胁框架改善产品能力的视角看对传统赛道的突破

04

从现有网络安全框架看对安全产品的能力需求

05

从关键安全能力视角重新梳理能力性产品框架

智者安天下

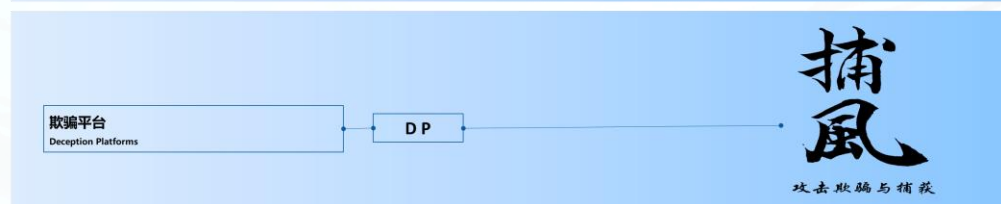
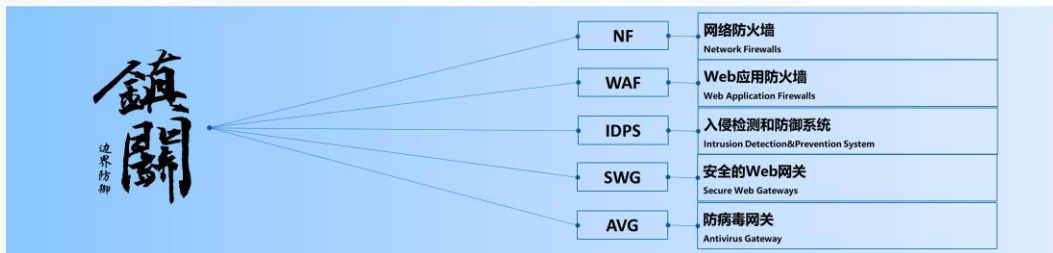
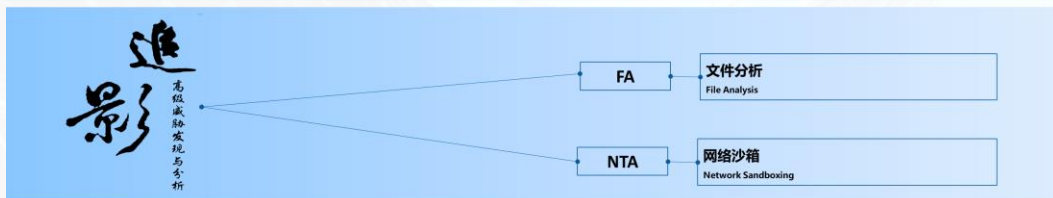
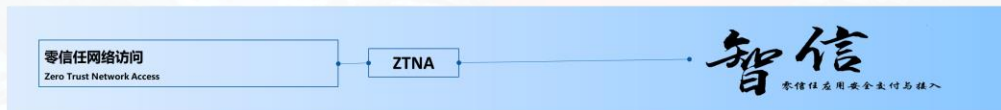
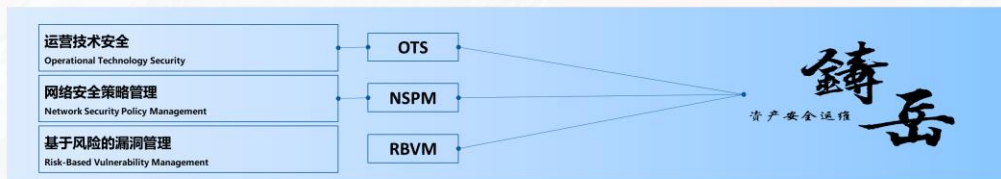
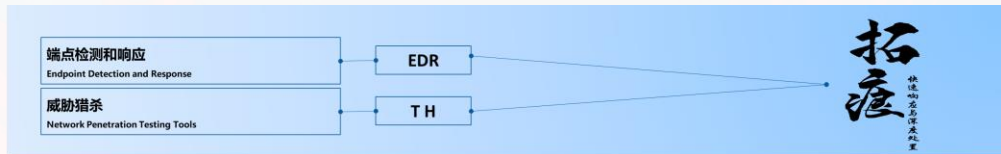
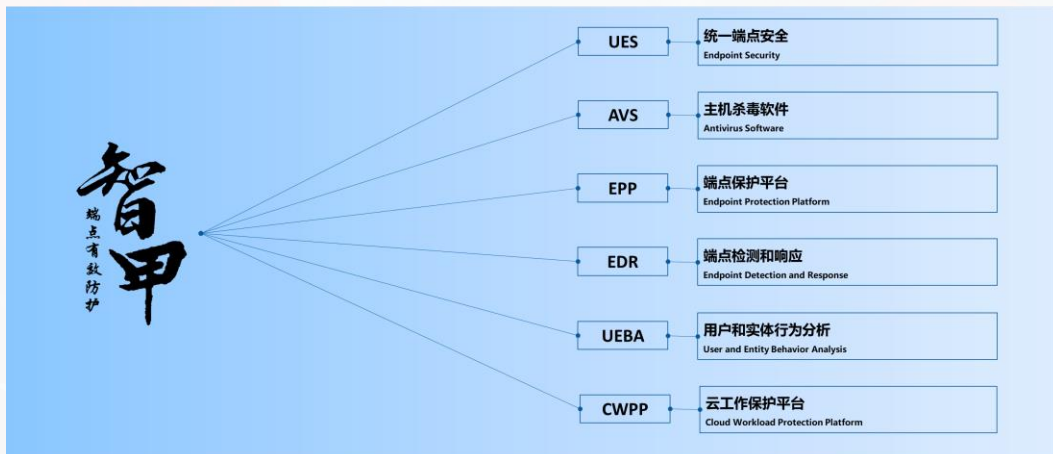


长缨待展

威胁框架：细粒度对抗

01 从安天自己的“标品矩阵”说起

从安天标品品牌矩阵和产品品类 “赛道” 的映射说起



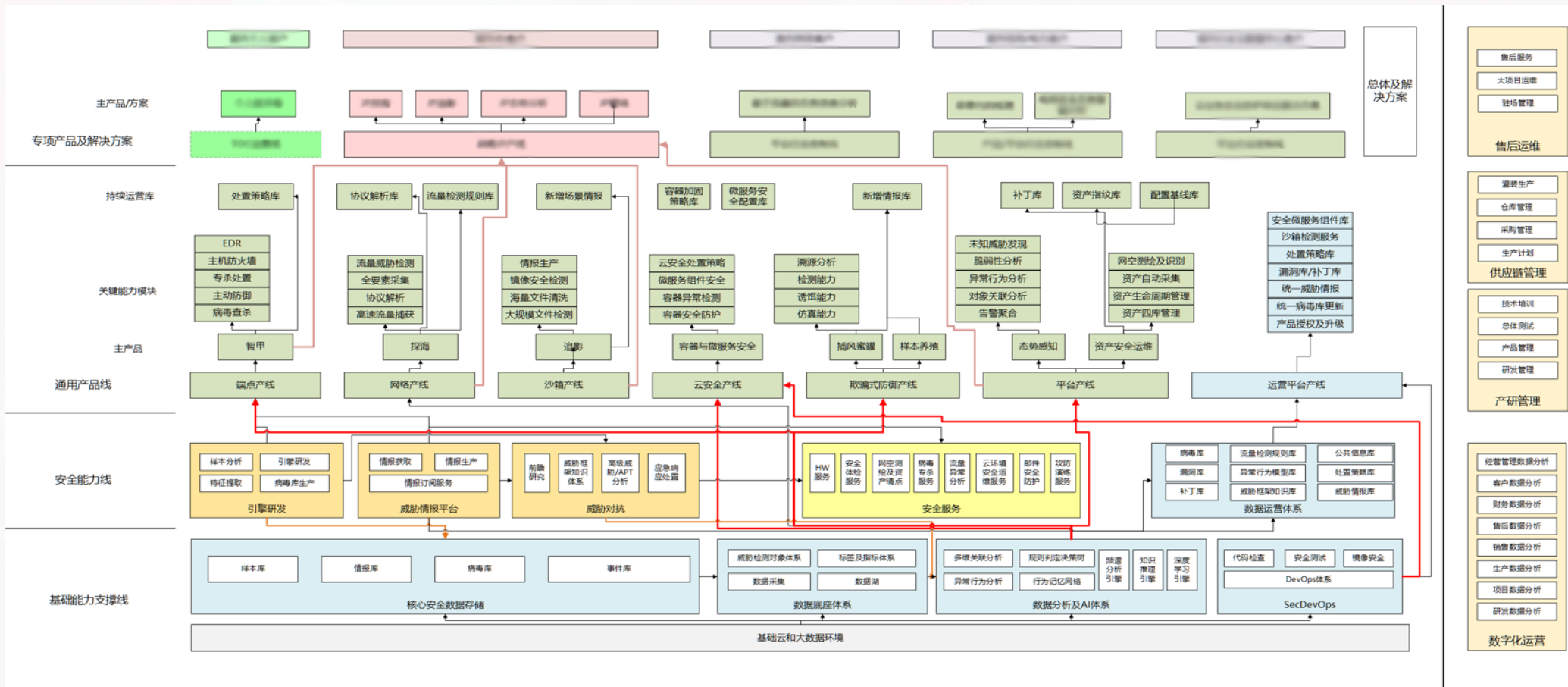
通过现有赛道定义产品能有效支撑高级威胁对抗么？



初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用.bash_profile和... 启动代理 利用服务器软件组件	操纵访问令牌 利用服务注册表权限...	操纵访问令牌 绕过Gatekeeper Process Doppelg�ng...	操纵账户 发现账户	利用AppleScript	捕获音频	利用常用端口	自动导出数据	删除账户权限
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能 启动守护进程 利用服务注册表权限...	借助辅助功能 利用Setuid和Setgid位	填充二进制文件 修改组策略 替换进程内存	查看bash历史 发现应用程序窗口	利用应用程序部署软件	自动收集	通过可移动介质通信	压缩数据	损毁数据
利用外部远程服务	利用命令行	加入空格隐藏扩展名	操纵账户 利用Launchctl 利用Setuid和Setgid位	利用AppCert DLL(注... SID历史注入	利用BITS服务 隐藏文件目录 进程注入	暴力破解 发现浏览器书签	利用组件对象模型(C...	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据...
添加硬件	利用HTML编译文件	利用系统中的第三...	利用AppCert DLL(注... 添加LC_LOAD_DYLIB 修改快捷方式	利用Applnit DLL(注... 利用启动项	绕过用户账户控制(UAC) 隐藏用户 冗余访问	凭证转储 发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容置换攻击
通过可移动介质复制	利用组件对象模型(C...	利用Trap命令	利用Applnit DLL(注... 利用linux本地任务调度	利用Windows应用程... 会话发起协议(SIP)和...	利用Sudo命令 清除命令历史 隐藏窗口	获取Web浏览器凭证 发现文件和目录	执行内部鱼叉式钓鱼...	收集本地系统数据	使用自定义加密协议	通过备选协议回传	擦除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用受信的开发工具	利用Windows应用程... 利用登录项 利用启动项	绕过用户账户控制(U... 利用Sudo缓存凭证	利用CMSTP HISTCONTROL 利用Regsvr32	获取文件中的凭证 扫描网络服务	利用登录脚本	收集网络共享驱动数据	编写数据	通过C2信道回传	擦除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协...	诱导用户执行	利用认证包 利用登录脚本 利用系统组件	DLL搜索顺序劫持 利用有效账户	代码签名 映像劫持 使用Rootkit	获取注册表中的凭证 发现网络共享	利用密码哈希认证	收集可移动介质数据	混淆数据	通过其他网络介质回传	端点拒绝服务(DoS)
通过服务执行鱼叉式...	通过API执行	利用Windows管理规...	利用BITS服务 利用LSASS驱动程序 利用Systemd服务	Dylib劫持 使用Web Shell	投送后编译 阻止信标捕获 利用Rundll32	利用凭证访问漏洞 网络嗅探	利用Ticket认证	回传数据准备	前置域名	通过物理介质回传	损坏硬件
入侵供应链	通过模块加载执行	利用Windows远程管...	使用Bootkit 修改现有服务 利用Windows时间服务	提示用户输入合法凭...	利用HTML编译文件 删除工具中的信标 使用脚本	强制认证 发现密码策略	利用远程桌面协议	收集电子邮件	使用域名生成算法(DGA)	定时传输	禁止系统恢复
利用受信关系	利用主机软件漏洞	利用XSL文件执行脚本	添加浏览器扩展插件 Netsh Helper DLL 利用Trap命令	利用事件监控守护进程	利用组件组件 删除主机中的信标 执行签名的二进制文...	利用Hook 发现主机插入设备	拷贝远程文件	输入捕捉	使用备用信道		网络侧拒绝服务(DoS)
利用有效账户	利用图形用户界面(GUI)		更改默认文件关联 新建服务 利用有效账户	利用漏洞提权	组件对象模型(COM)劫持 间接执行命令 执行签名的脚本代理	输入捕捉 发现权限组	利用远程服务	浏览器中间人攻击(MitB)	利用多跳代理		资源劫持
	利用InstallUtil		利用组件组件 启动Office应用程序 使用Web Shell	额外窗口内存注入(E...	利用连接代理 安装根证书 会话发起协议(SIP)和...	发现进程 通过可移动介质复制	通过可移动介质复制	获取屏幕截图	创建多级信道		操纵运行时数据
	利用Launchctl		组件对象模型(COM)... 路径拦截 利用Windows事件订...	利用文件系统权限漏洞	利用控制面板项 利用InstallUtil 软件加壳 使用Kerberoasting技术	查询注册表 共享Webroot目录	共享Webroot目录	捕获视频	使用多协议通信		禁用服务
	利用linux本地任务调度		创建账户 修改属性列表 Winlogon Helper D...	利用Hook	使用DCShadow技术 利用Launchctl 加入空格隐藏扩展名	发现远程系统 SSH劫持	SSH劫持	使用多层加密			操纵本地存储数据
	利用LSASS驱动程序		DLL搜索顺序劫持 端口敲门	映像劫持	反混淆/解密文件或信息 LC_MAIN劫持 模板注入	发现安全软件 污染共享内容	污染共享内容	端口敲门			系统关机/重启
	利用Mshhta		Dylib劫持 端口监控	启动守护进程	禁用安全工具 仿冒 修改文件时间戳	网络嗅探 发现软件	利用系统中的第三...	利用远程访问工具			操纵传输中的数据
	利用PowerShell		利用事件监控守护进程 利用PowerShell配置...	新建服务	DLL搜索顺序劫持 修改注册表 利用受信的开发者工具	发现系统信息 利用Password Filter...	利用Windows管理员...	拷贝远程文件			
	利用Regsvcs/Regasm		利用外部远程服务 利用Rc.common文件	伪造父进程	DLL旁路加载 利用Mshhta 利用有效账户	收集私钥 发现系统网络配置	利用Windows远程管...	使用标准应用层协议			
	利用Regsvr32		利用文件系统权限漏洞 重启应用程序	路径拦截	按条件执行 删除网络共享连接 虚拟化/沙箱逃逸	利用Securityd内存 发现系统网络连接		使用标准加密协议			
	利用Rundll32		隐藏文件和目录 冗余访问	修改属性列表	利用漏洞规避防御 利用NTFS交换数据流... 利用Web服务	窃取Web会话Cookie 发现系统所有者/用户		使用标准非应用层协议			
	利用计划任务		利用Hook 添加注册表运行/启...	端口监控	额外窗口内存注入(EW... 混淆文件身份信息 利用XSL文件执行脚本	双因子认证拦截 发现系统服务		利用不常用端口			
	使用脚本		利用Hypervisor 利用计划任务	利用PowerShell配置...	修改文件和目录权限 伪造父进程	发现系统时间		利用Web服务			
	利用Windows服务		映像劫持 利用屏幕保护程序	进程注入	删除文件 修改属性列表	虚拟化/沙箱逃逸					
	利用签名的二进制文...		利用内核模块和扩展 利用SSP DLL(注册表...	利用计划任务	文件系统逻辑偏移 端口敲门						

可扩展进行攻击的战术
恶意代码已有的攻击战术

复杂的内部能力供应链只是为了支撑 “赛道” 标品吗？



能力内核和情报的高度复用说明赛道被打通了吗？



安天核心能力单元	能力分支	安天产品嵌入核心能力的产品单元					
		智甲	探海	追影	捕风	拓痕	镇关
AVL SDK检测引擎	威胁监测	有	有	有	有	有	有
	向量拆解	有	有	有	有	有	
流量监测引擎		有	有	有	有	有	
场景化引擎	主机侧	有	有	有	有	有	
	网络侧	有	有	有	有	有	
威胁框架分析引擎		有	有	有	有	有	
高精度网络协议栈			有				
动态分析内核			有	有	有	有	
主动防御驱动		有					
深度提取和处置模块		有				有	
通用界面/可视化组件	资产拓扑	有 (管理中心侧)	有		有		
	威胁框架	有 (管理中心侧)	有	有	有		
规则更新和情报	病毒库升级	有	有	有	有	有	有
	IOC情报	有	有	有	有	有	有
	向量情报	有	有	有	有	有	
	威胁框架TTPs	有	有	有	有	有	

我们将在冬训营讨论的话题



- **产品需要与场景深度融合**

- 云安全、容器安全不是传统主机安全的移植，而要从其场景特点展开。参见报告《容器与微服务安全的对抗实践》
- 面对系统安全威胁，从管理中心到端点防护，需要支持更细粒度的处置能力。参见报告《智甲系统如何在端点实现细粒度防御》
- 邮件作为常见的攻击入口，需要在多个环节进行对抗，参见报告《邮件安全的威胁认知与防御关口设置》

- **产品需要强有力的共性内核和运营支持**

- 引擎+情报正在成为一种共性能力，参见报告《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》和《威胁情报和检测引擎结合,有效提升安全防护能力》

- **产品需要深入的联动融合**

- 沙箱作为威胁情报的生产设施，如何与其他安全环节无缝对接如何融合，参见报告《流量威胁检测与文件深度分析的最佳实践》

- **产品赛道正在变的模糊**

- 欺骗防御不在是蜜罐产品的专利，而正在成为一种普遍性的产品特性，参见报告《从蜜罐捕获到无所不在的欺骗防御》。

问题来了



- 在场景价值沉浸细分，基础能力贯通融合，系统全局运营的时代？
- 我们还应该用“赛道”衡量安全产品么？

智者安天下

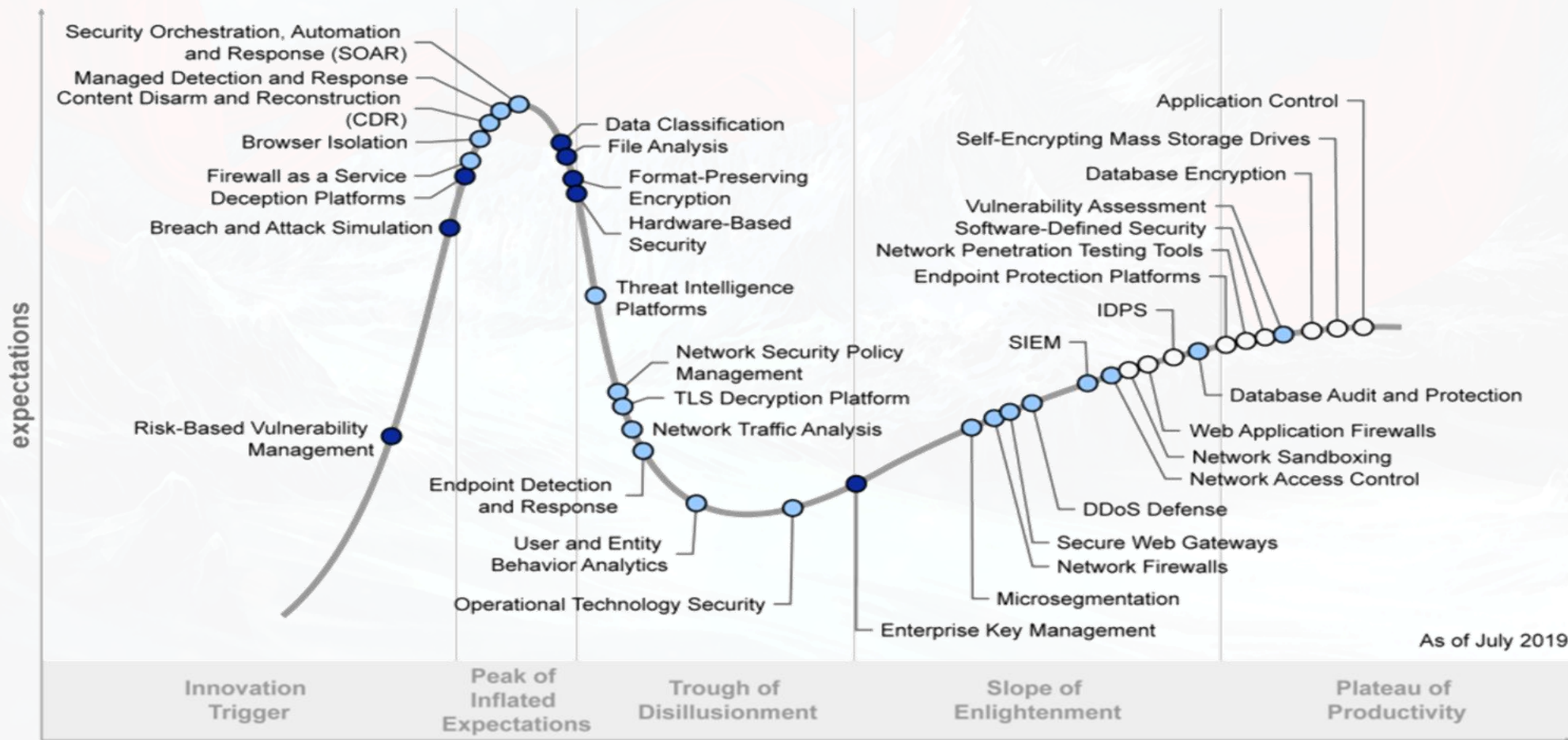


长缨待展

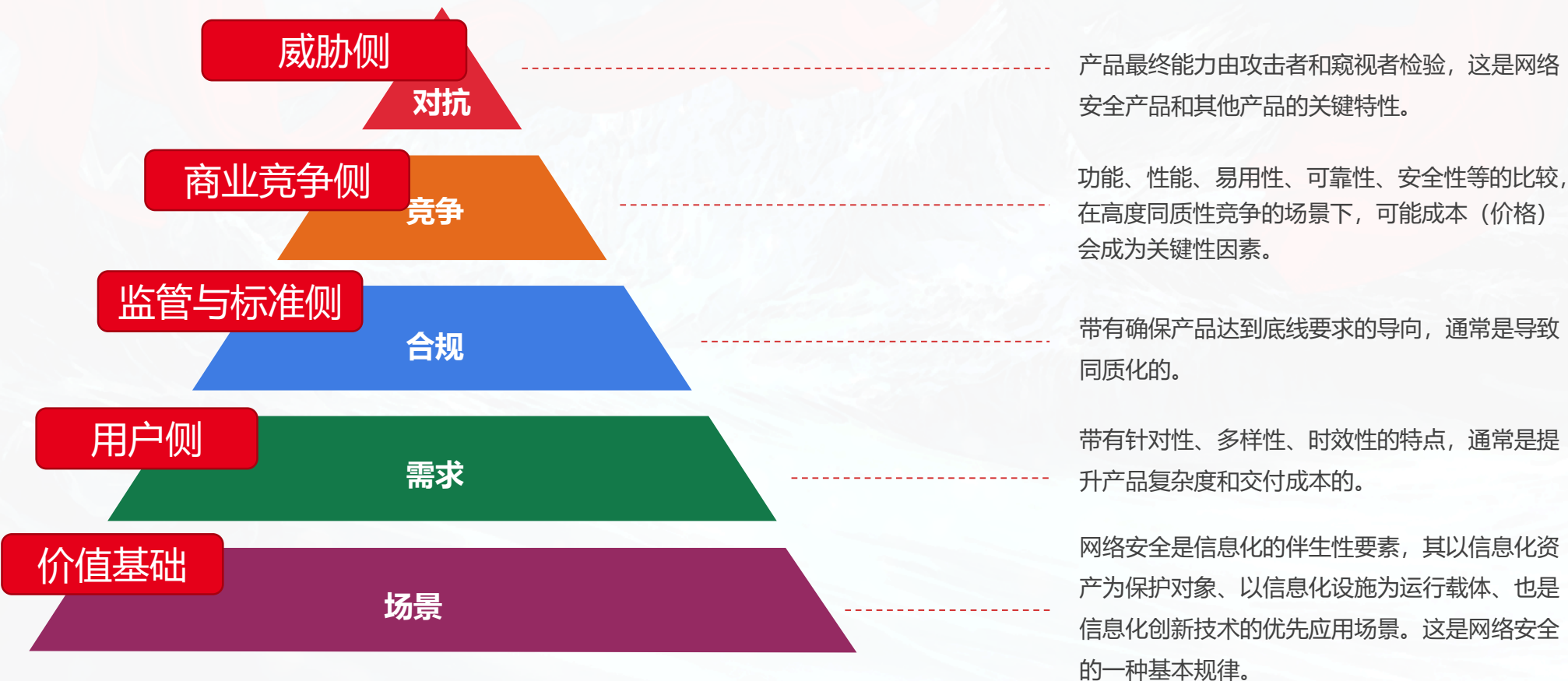
威胁框架：细粒度对抗

02 从安全产品演进看“赛道”是怎样形成的

从Gartner技术成熟度曲线看安全产品赛道现状



产品赛道形成中有哪些外力要素



计算机恶意代码史与IT产业发展关系图

1981-2013 | 2013年11月20日 首次发布
2013年12月4日 第1次修订版本

按语

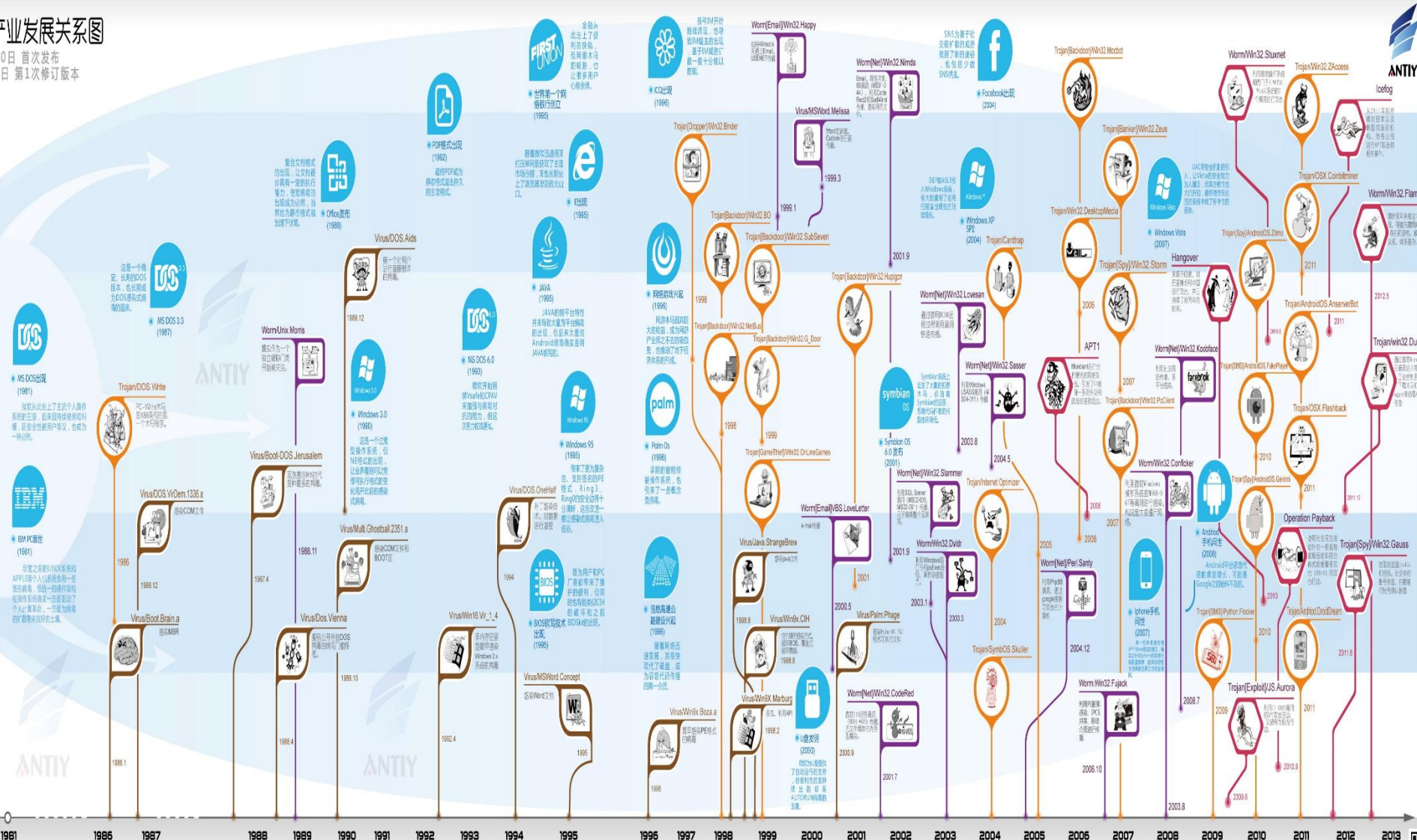
1981年，IBM PC 诞生，奠定了统治IT多年的三驾马车架构。五年后，第一个针对X86 PC架构系统的病毒巴基斯病毒面世。从此恶意代码像瘟疫般的席卷IT，伴随着信息技术的发展壮大同步蔓延膨胀。

所有新的操作系统和版本在服务器用户的同时，同样被病毒编写者分析，所有新的应用趋势，无一不同样带来安全风险。凡属服务器用户或便利的接口和方案，无一不成为病毒扩散的渠道。

因此恶意代码的进化不是一部孤立的历史，而是IT技术发展史上一种挥之不去的蓝色创痕。为此，安天实验室病毒科编研小组将产业史与恶意代码相关的一些关键节点与典型有影响力的恶意代码，按照时间进行了梳理，仓促形成此图。

由于时间仓促，难免出现各种错误，敬请读者指正，我们将在Viewview网站修正更新。
安天实验室 病毒科编研小组

图例



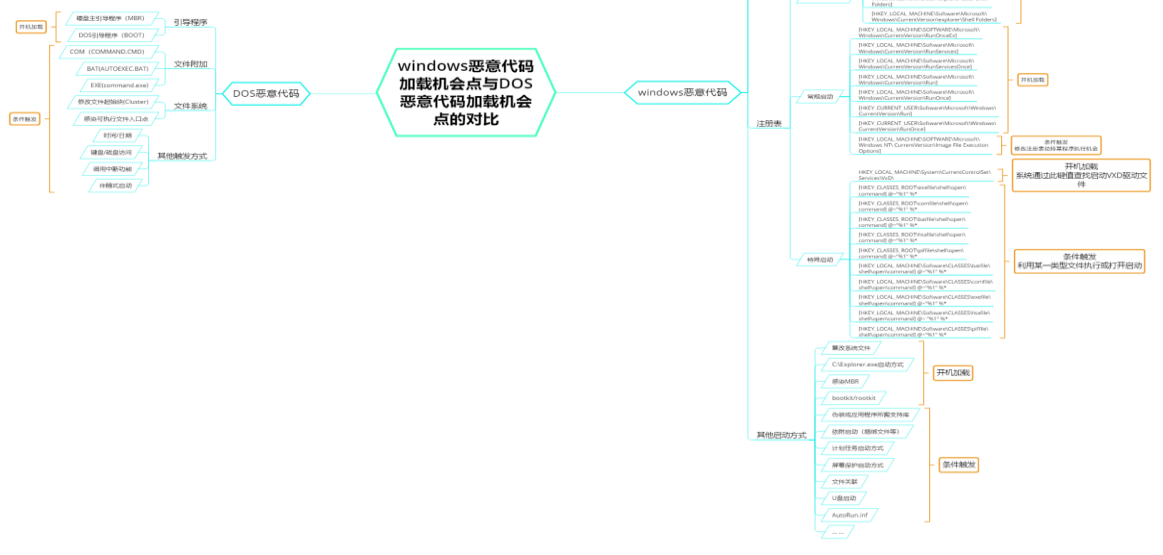
IT场景变化驱动：算力、带宽和复杂度同步增长



年代	CPU						内存					操作系统		
	具体年份	型号	CPU主频	CPU位数	晶体管数量	制造工艺	具体年份	型号	针脚	单条容量	运行频率	具体年份	型号	代码行数
1970-1980	1978	8086	5MHz-10MHZ	16位	2.9万	3微米								
	1979	8088	4.77MHz-8MHZ	内部16位, 外部8位	2.9万	3微米								
1980-1990	1982	80286	6MHz-25MHz	16位	13.4万	1.5微米						1981	DOS 1.0	数千行 (猜测)
							1982	SIMM内存	30pin	256k	N/A	1984	DOS 3.0	N/A
	1985	80386	12MHz-40MHz	32位	27.5万	1微米-1.5微米	1988	SIMM内存	72pin	512KB-2MB	N/A	1985	Win1.0	N/A
	1989	80486	16MHz-100MHz	32位	90万/118.5万	0.6微米-1微米						1987	Win2.0	N/A
1990-2000	1993	Intel Pentium	50MHz-200MHz	32位	320万	0.6微米	1991	EDO DRAM	72pin	6M-16M	N/A	1990	Win3.0	N/A
	1995	Pentium Pro	150MHz-200MHz	32位	220万	0.355微米-0.5微米						1992	Win4.0	N/A
	1997	Intel Pentium MMX	166MHz-300MHz	32位	450万	0.35微米						1993	DOS 6.0	N/A
	1997	Intel PentiumII	233MHz-450MHz	32位	750万	0.18微米-0.35微米						1995	Win95	N/A
	1999	Intel PentiumIII	450MHz-1.4GMHz	32位	950万	0.13微米-0.25微米						1998	Win98	1500万
2000-2010	2000	Intel Pentium4	3.06GHz	32位/64位	5500万	0.18微米、0.13微米、0.09微米、65纳米	2000	DDR1	180pin	128M-1G	400MHz	2000	Win2000	N/A
	2002	Intel Pentium 4 HT	3.2GHz-3.5GHz	32位/64位	N/A	90纳米						2002	WinXP	4000万
	2003	Intel Pentium M	1.3GHz-1.6GHz	32位	7700万	90纳米	2003	DDR2	240pin	256M-4G	1066MHz			
	2005	Intel Pentium D	2.8GHz-3.2GHz	32位/64位	2.3亿	90纳米								
	2006	Intel Core 2 Duo	2.2GHz	32位/64位	2.91亿	65纳米、45纳米						2006	Vista	5000万
	2008	Intel Core i3/i5/i7	2.8GHz/3.46GHz	32位/64位	5.82亿	32纳米、45纳米	2007	DDR3	240Pin	512M-8G、16G	1066MHz	2009	Win7	5000万
2010-2018	2010	第二代处理器 (Sandy Bridge架构)	2.4GHz-3.8GHz	32位/64位	11.6亿	32纳米								
	2012	第三代处理器 (Ivy Bridge架构)	2.6GHz-3.9GHz	32位/64位	18.6亿	22纳米						2012	Win8	>5000万
	2014	第四代处理器 (Haswell架构)	2.8GHz-4.0GHz	32位/64位	14亿+	22纳米	2014	DDR4	284Pin	4G、8G、16	2133MHz-4200MHz			
	2015	第五代处理器 (Broadwell架构)	3.1GHz-3.6GHz	32位/64位	19亿	14纳米						2015	Win10	>1亿
	2016	第六代处理器 (Skylake架构)	2.8GHz-4.0GHz	32位/64位	N/A	14纳米								
	2017	第七代处理器 (Kaby Lake、Skylake-X架构)	3.5GHz-4.2GHz	32位/64位	80亿+	14纳米								
	2018	第八代处理器 (CoffeeLake架构)	2.8GHz-4.0GHz	32位/64位	N/A	14纳米								

算力、带宽等资源提升同时提升了攻防双方的资源能力，复杂度对攻防双方提供了挑战

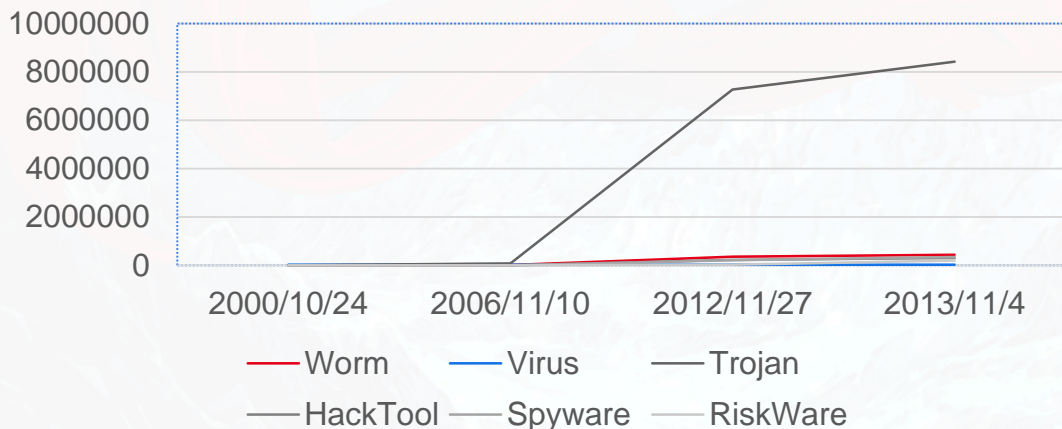
系统复杂为攻击带来更多的窗口和机会



- 安天的工程师在这里只列举了恶意代码的加载机会，尚不包括主机系统的完整的可攻击点。
- 端点系统的复杂为攻击者带来了更多的机会，操作系统的代码不只必然带来更多的漏洞攻击点，由于系统一方面需要提供更多便利性，同时需要兼容原有的应用、协议等，因此同样带来了大量可以被非法利用的“合法”入口。而安全需要在达成安全效果的同时，确保资产的可用性和可靠性。
- 信息化建设是由大量的充满了“不确定性”和“隐形质量”的复杂端点系统和连接关系组成的。对于规模化的信息系统来说，确保每个节点都绝对不失陷，显然是不可能的。

威胁驱动：威胁数量膨胀带来的影响

2000-2013 恶意代码的变种总量统计

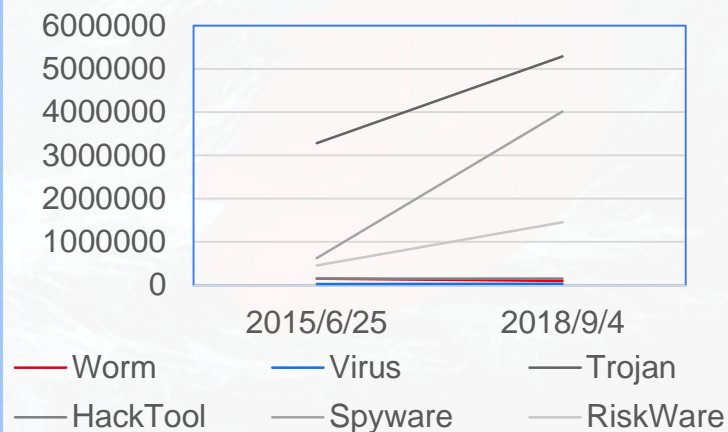


分类/日期	2000/10/24	2006/11/10	2012/11/27	2013/11/04
Worm	512	8109	354049	435247
Virus	21006	27760	29940	30060
Trojan	3066	84811	7262094	8423751
HackTool	260	4968	217502	301076
Spyware	37	4899	214570	340751
RiskWare	0	88	25800	201401

来源：Kaspersky（卡巴斯基）对应日期病毒名列表

从观测来看，2014年开始，由于卡斯基后台分析与同源合并能力的增强，一些病毒家族和变种发生变化，因此出现了部分数量减少，但总体种类膨胀超过**400**倍。

2015-2018 恶意代码的变种总量统计



分类/日期	2015/06/25	2018/09/04
Worm	149137	101674
Virus	29397	29980
Trojan	3283882	5289006
HackTool	153493	154800
Spyware	622344	4013384
RiskWare	458035	1451458

威胁驱动：载荷的复杂度带来的影响

	DOS样本	早期木马 (以Back Orifice)	APT样本 (以方程式攻击组织的DS为例)
运行平台	DOS平台	Windows平台	全平台
样本数量	单一样本	单一样本 (少数带有插件)	高级恶意代码工程、样本集合 (集成化、模块化)
代码规模	几十到几百行	数千~数万行	数十万行
函数调用			
网络通信	无	多数为无加密通信	多种方式加密通信
开发者	个人	个人或民间小规模组织	有充足成本支持的规模型组织
命令与控制	无	简单	复杂
操作界面	无		
回连地址	无	需要感染节点能够被控制端访问到	大量地址
生命周期	短	几周	隐匿, 长期控制
控制方式	无	正向连接	正向、反向、激活、近场控制等
使用漏洞	无	几乎没有	0day
抗分析能力	无	相对比较简单, 易于分析	高强度的本地加密, 复杂的调用机制

威胁驱动：威胁的高级化带来的影响



初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响						
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用.bash_profile和...	启动代理	利用服务器注册表权限...	操纵访问令牌	绕过Gatekeeper	Process Doppelg�ng...	操纵账户	发现账户	利用AppleScript	捕获音频	利用常用端口	自动导出数据	删除账户权限		
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能	启动守护进程	利用服务器注册表权限...	借助辅助功能	利用Setuid和Setgid位	填充二进制文件	修改组策略	替换进程内存	查看bash历史	发现应用程序窗口	利用应用程序部署软件	自动收集	通过可移动介质通信	压缩数据	篡改数据
利用外部远程服务	利用命令行	加入空格隐藏扩展名	操纵账户	利用Launchctl	利用Setuid和Setgid位	利用AppCert DLL(注...	SID历史注入	利用BITS服务	隐藏文件目录	进程注入	暴力破解	发现浏览器书签	利用组件对象模型(C...	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据...
添加硬件	利用HTML编译文件	利用系统中的第三...	利用AppCert DLL(注...	添加LC_LOAD_DYLIB	修改快捷方式	利用Applnit DLL(注...	利用启动项	绕过用户账户控制(UAC)	隐藏用户	冗余访问	凭证转储	发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容置换攻击
通过可移动介质复制	利用组件对象模型(C...	利用Trap命令	利用Applnit DLL(注...	利用linux本地任务调度	会话发起协议(SIP)和...	利用Windows应用程...	利用Sudo命令	清除命令历史	隐藏窗口	利用Regsvcs/Regasm	获取Web浏览器凭证	发现文件和目录	执行内部鱼叉式钓鱼...	收集本地系统数据	使用自定义加密协议	通过备选协议回传	擦除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用受信的开发工具	利用Windows应用程...	利用登录项	利用启动项	绕过用户账户控制(U...	利用Sudo缓存凭证	利用CMSTP	HISTCONTROL	利用Regsvr32	获取文件中的凭证	扫描网络服务	利用登录脚本	收集网络共享驱动数据	编码数据	通过C2信道回传	擦除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协...	诱导用户执行	利用认证包	利用登录脚本	利用系统组件	DLL搜索顺序劫持	利用有效账户	代码签名	映像劫持	使用Rootkit	获取注册表中的凭证	发现网络共享	利用密码哈希认证	收集可移动介质数据	混淆数据	通过其他网络媒介回传	端点拒绝服务(DoS)
通过服务执行鱼叉式...	通过API执行	利用Windows管理规...	利用BITS服务	利用LSASS驱动程序	利用Systemd服务	Dylib劫持	使用Web Shell	投送后编译	阻止信标捕获	利用Rundll32	利用凭证访问漏洞	网络嗅探	利用Ticket认证	回传数据准备	前置域名	通过物理介质回传	损坏硬件
入侵供应链	通过模块加载执行	利用Windows远程管...	使用Bootkit	修改现有服务	利用Windows时间服务	提示用户输入合法凭...		利用HTML编译文件	删除工具中的信标	使用脚本	强制认证	发现密码策略	利用远程桌面协议	收集电子邮件	使用域名生成算法(DGA)	定时传输	禁止系统恢复
利用受信关系	利用主机软件漏洞	利用XSL文件执行脚本	添加浏览器扩展插件	Netsh Helper DLL	利用Trap命令	利用事件监控守护进程		利用组件劫持	删除主机中的信标	执行签名的二进制文...	利用Hook	发现主机插入设备	拷贝远程文件	输入捕捉	使用备用信道		网络侧拒绝服务(DoS)
利用有效账户	利用图形用户界面(GUI)		更改默认文件关联	新建服务	利用有效账户	利用漏洞提权		组件对象模型(COM)劫持	间接执行命令	执行签名的脚本代理	输入捕捉	发现权限组	利用远程服务	浏览器中间人攻击(MitB)	利用多跳代理		资源劫持
	利用InstallUtil		利用组件劫持	启动Office应用程序	使用Web Shell	额外窗口内存注入(E...		利用连接代理	安装根证书	会话发起协议(SIP)和...	欺骗用户输入凭证	发现进程	通过可移动介质复制	获取屏幕截图	创建多级信道		操纵运行时数据
	利用Launchctl		组件对象模型(COM)...	路径拦截	利用Windows事件订...	利用文件系统权限漏洞		利用控制面板项	利用InstallUtil	软件加壳	使用Kerberoasting技术	查询注册表	共享Webroot目录	捕获视频	使用多协议通信		禁用服务
	利用linux本地任务调度		创建账户	修改属性列表	Winlogon Helper D...	利用Hook		使用DCShadow技术	利用Launchctl	加入空格隐藏扩展名	利用Keychain	发现远程系统	SSH劫持		使用多层加密		操纵本地存储数据
	利用LSASS驱动程序		DLL搜索顺序劫持	端口敲门		映像劫持		反混淆/解密文件或信息	LC_MAIN劫持	模板注入	LLMNR/NBT-NS接...	发现安全软件	污染共享内容		端口敲门		系统关机/重启
	利用Mshhta		Dylib劫持	端口监控		启动守护进程		禁用安全工具	仿冒	修改文件时间戳	网络嗅探	发现软件	利用系统中的第三...		利用远程访问工具		操纵传输中的数据
	利用PowerShell		利用事件监控守护进程	利用PowerShell配置...		新建服务		DLL搜索顺序劫持	修改注册表	利用受信的开发者工具	利用Password Filter...	发现系统信息	利用Windows管理员...		拷贝远程文件		
	利用Regsvcs/Regasm		利用外部远程服务	利用Rc.common文件		伪造父进程		DLL旁路加载	利用Mshhta	利用有效账户	收集私钥	发现系统网络配置	利用Windows远程管...		使用标准应用层协议		
	利用Regsvr32		利用文件系统权限漏洞	重启应用程序		路径拦截		按条件执行	删除网络共享连接	虚拟化/沙箱逃逸	利用Securityd内存	发现系统网络连接			使用标准加密协议		
	利用Rundll32		隐藏文件和目录	冗余访问		修改属性列表		利用漏洞规避防御	利用NTFS交换数据流...	利用Web服务	窃取Web会话Cookie	发现系统所有者/用户			使用标准非应用层协议		
	利用计划任务		利用Hook	添加注册表运行项/启...		端口监控		额外窗口内存注入(EW...	混淆文件身份信息	利用XSL文件执行脚本	双因子认证拦截	发现系统服务			利用不常用端口		
	使用脚本		利用Hypervisor	利用计划任务		利用PowerShell配置...		修改文件和目录权限	伪造父进程			发现系统时间			利用Web服务		
	利用Windows服务		映像劫持	利用屏幕保护程序		进程注入		删除文件	修改属性列表			虚拟化/沙箱逃逸					
	利用签名的二进制文...		利用内核模块和扩展	利用SSP DLL(注册表...		利用计划任务		文件系统逻辑偏移	端口敲门								

可扩展进行攻击的战术
 恶意代码已有的攻击战术

在SolarWinds事件中，仅分析管理软件转化为RAT的风险影响，就涉及大量的技战术动作

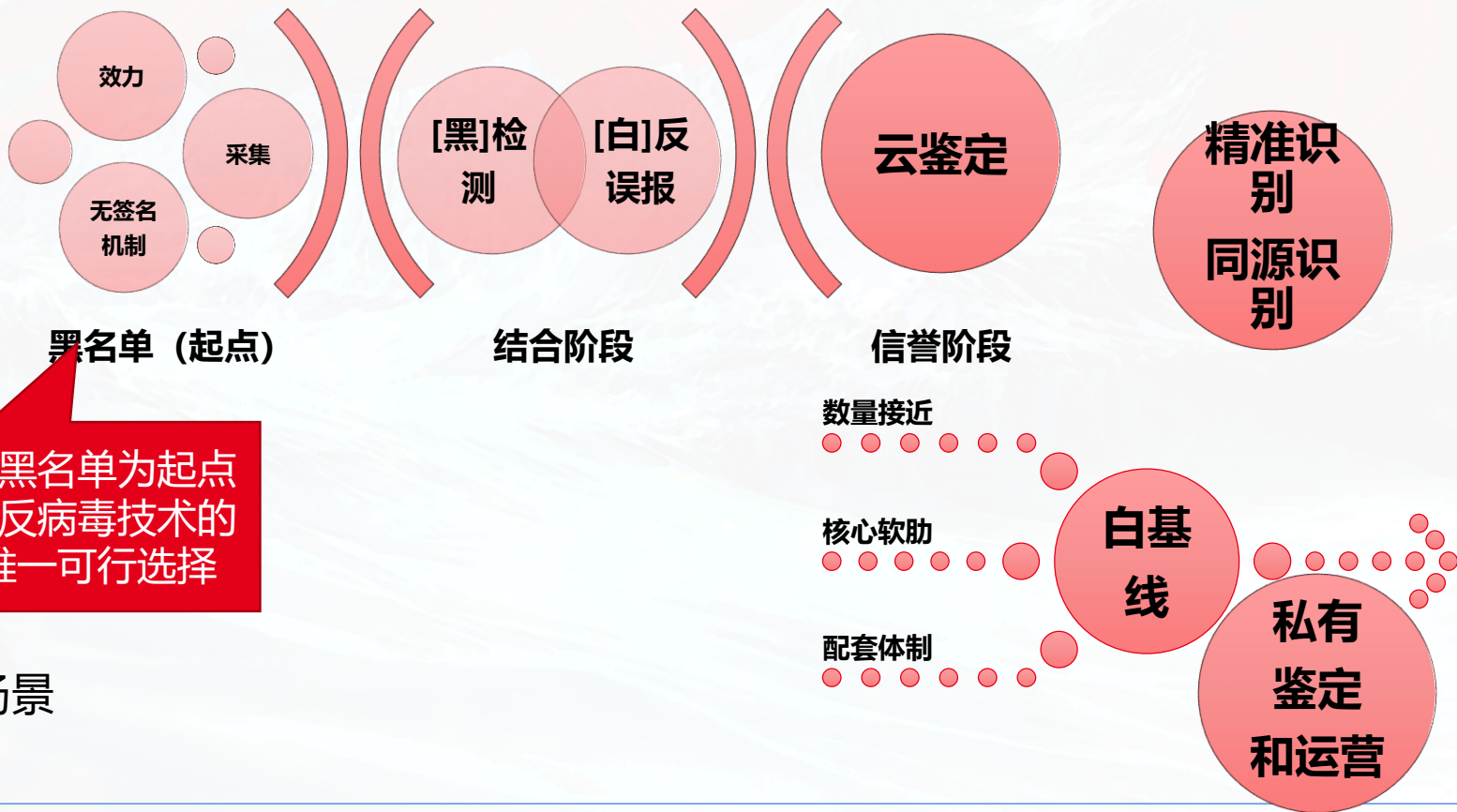
安全产品的演进：差异化、重定义带来的驱动



厂商	Netscreen	Fortinet	Paloalto Network	Fireeye
创建时间	1997.12	2000.12	2005	2004.1.1
上市时间	2001.12.12	2009.11.19	2012.7.27	2013.9.22
核心概念	硬件防火墙	UTM (统一威胁管理)	NG-FW (下一代防火墙)	Advanced Persistent Threat (APT) Attack & Zero-Day Protection
核心概念提出时间	1999.9	2004.2	2007.6.24	2011
主要产业背景	信息高速公路建设, 网络带宽迅速增长	网络应用蓬勃发展	网络客户端、社交网络等新形态, 带宽进一步增长	国家和政经集团间的相互攻击入侵
主要应对威胁	新的流量压力	邮件病毒、垃圾邮件	SNS 威胁、小众协议、僵尸网络	APT 0Day 漏洞
核心技术方法	ASIC 专用芯片	流还原检测、与传统文件病毒检测技术结合	精细协议解析 身份 ID 识别 可视化 基于多核体制和专有实现的高性能	沙箱前置 场景组合遍历 多向量检测 云端能力 异步检测与实时防护联动

场景环境约束与变化对技术路径的影响

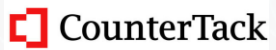
个人用户场景



以黑名单为起点
是反病毒技术的
唯一可行选择

企业侧和专有场景

赛道分支的形成：技术积累差异驱动(以EDRvsEPP为例)



雨伞专利对技术路线选择的影响



2005 新聞稿

美國國際貿易委員會 ITC 針對趨勢科技與 Fortinet 專利侵權訴訟案做出最後裁決

ITC 發布禁令 禁止 Fortinet 在美國進口和銷售 FortiGate? 系列產品

Cupertino, 美國加州 - 2005 年 8 月 9 日 - 致力於網路防毒和網路內容安全軟體及服務的領導廠商趨勢科技 (東京證交所: 4704, 美國 NASDAQ: TMIC) 宣佈, 美國國際貿易委員會 ITC 已經針對趨勢科技控告 Fortinet 侵犯其專利權一案於昨天做出最後裁決並發佈禁令, 禁止總部設於美國加州 Sunnyvale 的 Fortinet 公司在美國宣傳廣告、發行、進口和銷售 FortiGate? 系列產品。

這項最後裁決同時也是依據 ITC 於稍早在今年 5 月經過 6 天的審訊做出的初步判決的結果。Fortinet 的 FortiGate 防毒防火牆系列產品侵犯到趨勢科技登記於美國編號 5,623,600 之專利, 這項專利主要是指在資料傳輸到終端用戶的電腦之前, 就可以在伺服器端 (例如網路閘道或硬體設備) 進行病毒掃描的發明。

美國國際貿易委員會 ITC 所頒佈的禁令將在未來的 60 天內, 需先經由美國總統審核。在這段審核期間內, Fortinet 就必須提供擔保金。在 60 天審核期間結束並將被禁止在美國銷售所有 FortiGate 系列產品。美國國際貿易委員會 ITC 網站 <http://www.usitc.gov>

2000 公司新闻

Network Associates 侵犯趨勢科技專利案, 雙方達成協議簽署相互授權協定, Network Associates 另需支付趨勢科技高額賠償金

這項長達 3 年的 Network Associates 專利訴訟案, 近日有了新進展, 雙方同意對專利防毒技術採取賠償金, 引人矚目。

1997 年, 趨勢科技與 Network Associates 和 Trend Micro 遭到台灣軟體廠商控訴, 案情喧騰一時。根據雙方協議, 雙方同意對專利防毒技術採取賠償金, 引人矚目。

這項引起全球前三大軟體公司 (Microsoft, IBM, Oracle) 的專利訴訟案, 於 1997 年 4 月 22 日申請通過。趨勢科技 (groupware) 資料技術已運用在趨勢科技防毒軟體等以 Server 為

2000 新聞稿

Symantec 侵犯趨勢科技專利權訴訟案達成和解, 雙方簽訂雙授權協定, 同意彼此分享防毒專利技術

去年 5 月喧騰一時的 Network Associates (NETA, 前 McAfee Associates) 和 Symantec 兩家防毒軟體公司因侵犯趨勢科技研發的「On The Fly」(空中抓毒) 技術專利權, 而於 1997 年 4 月 22 日申請通過。趨勢科技與趨勢科技的防毒專利技術, 在雙方簽訂雙授權協定的前提下, 獲得彼此分享防毒專利技術。這項引起全球前三大軟體公司 (Microsoft, IBM, Oracle) 的專利訴訟案, 於 1997 年 4 月 22 日申請通過。趨勢科技 (groupware) 資料技術已運用在趨勢科技防毒軟體等以 Server 為

Barracuda 求助開源碼社群對抗趨勢科技

2008 年 01 月 31 日 | 2 則留言 |



Barracuda Networks 是一家專門開發電子郵件與 Web 安全硬體設備的網路安全供應商, 前陣子向開放原始碼社群發出求救訊號, 希望社群成員能夠幫助 Barracuda Networks 在與趨勢科技 (Trend Micro) 的閘道器防毒掃描技術專利權訴訟中, 有任何人能夠提供足以使 Trend Micro 在閘道器防毒掃描專利失效的資料。

思科败诉：因专利侵权被判赔付32亿美元，成为迄今为止美国专利案中最大一笔赔偿

2020-10-09 17:58 · 稿源：雷锋网

思科又一次因专利侵权而败诉。

10 月 6 日, 美国弗吉尼亚州地方法院作出了最终裁决, 思科系统公司 (Cisco) 因侵犯网络安全专利须向 Centripetal Networks 公司赔付 32 亿美元。这是迄今为止美国专利案件中最大的一笔赔偿金。

本章小结



- 关于安全产品的要素规律特点，还有很多没有总结。
- 现有的产品赛道产生是场景变迁演化、威胁演进驱动、商业竞争等要素的综合结果，有其起点的合理性，但并不代表其可以成为禁锢创新和业务价值达成的“藩篱”。
- 网络安全产品需要更要在客户场景下对抗威胁而，创造有效安全价值，这是一个“初心”。
- 那么，我们又能从威胁对抗上带来哪些启示？

智者安天下



长缨待展

威胁框架：细粒度对抗

03 从威胁框架改善产品能力的 视角看对传统赛道的突破

将威胁框架映射到产品能力环节



初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
本地攻击	利用AppleScript 利用安全脚本... 利用Source命令	利用bash_profile和... 启动代理 利用服务组件	通过访问令牌 利用注册表数据...	通过访问令牌 通过Gatekeeper Process Doppelganger...	通过用户输入... 通过Gatekeeper Process Doppelganger...	发现用户 通过Gatekeeper Process Doppelganger...	利用AppleScript	捕获音频 利用麦克风	利用麦克风	自动导出数据	删除用户权限
利用面向公众的应用...	利用CMSTP 利用Source命令	利用辅助功能 启动守护进程	利用注册表数据... 辅助功能 利用Setuid和Setgid位	通过二进制文件 修改注册表 删除进程内存	查看bash历史	发现应用程序窗口 利用应用程序编辑器	自动收集	通过可移动介质传输	压缩数据	窃取数据	
利用外部远程服务	利用命令执行 加入空档隐藏扩展名	捕获用户 利用Launchctl 利用Setuid和Setgid位	利用AppCert DLL注入... SID历史注入	利用BITS服务 隐藏文件目录 进程注入	暴力破解	发现浏览器书签 利用组件对象模型(COM)	收集系统数据	利用代理传输	加密数据	造成恶劣影响的数据...	
添加硬件	利用HTML编译文件 利用系统中的第三方...	利用AppCert DLL注入... 添加LOAD_DYLIB 修改使用方式	利用AppInitt DLL注入... 利用启动项	绕过用户账户控制(UAC) 隐藏用户 冗余访问	凭证传播	发现域信任 利用远程服务漏洞	收集系统数据	使用自定义协议	限制传输数据大小	网页内容直接攻击	
通过可移动介质攻击	利用组件对象模型(COM) 利用Trap命令	利用AppInitt DLL注入... 利用linux本地任务调度 会话发起协议(SIP)和...	利用Windows应用程序... 利用Sudo命令	清除命令历史 隐藏窗口 利用Regsvcs/Regasm	获取Web浏览器凭证	发现文件和目录 执行内部自定义协议	收集本地系统数据	使用自定义加密协议	通过设备协议回传	清除磁盘内容	
使用自定义的鱼饵	利用控制面服务 利用受信任的开发工具	利用Windows应用程序... 利用登录项 利用启动项	通过用户账户控制(UAC) 利用Sudo缓存凭证	利用CMSTP HISTCONTROL 利用Regsvr32	获取文件中的凭证 扫描网络服务	利用注册表 收集网络共享数据	编码数据	通过C信道回传	清除磁盘结构		
使用自定义的鱼饵链接	使用动态数据交换协议... 诱导用户执行	利用认证包 利用登录脚本 利用系统组件	DLL搜索顺序劫持 利用有效用户	代码签名 隐藏劫持 使用Rootkit	获取注册表中的凭证 发现网络共享	利用票据哈希认证 收集可移动介质数据	混淆数据	通过其他网络介质回传	端点解组服务(DoS)		
通过服务执行自定义...	通过API执行 利用Windows管理...	利用BITS服务 利用SASS驱动程序 利用Systemd服务	Dylib劫持 使用Web Shell	投送后编译 阻止劫持捕获 利用RunDll32	利用凭证访问漏洞 网络嗅探	利用Ticket认证 回传数据准备	前置域名	通过物理介质回传	损坏固件		
入侵供应链	通过模块加载执行 利用Windows进程...	使用Bootkit 修改现有服务 利用Windows网络服务	提示用户输入合法注...	利用HTML编译文件 删除工具中的标识 使用脚本	强制认证	发现密码策略 利用远程桌面协议	收集电子邮件	使用域名生成算法(DGA)	定时传输	禁止系统恢复	
利用受信任关系	利用主机软件漏洞 利用XSL文件执行脚本	添加浏览器扩展插件 Netsh Helper DLL 利用Trap命令	利用事件监听守护进程	利用组件组件 删除主机中的标识 执行签名的二进制文...	利用Hook	发现主机输入设备 拷贝远程文件	输入验证	使用备用信道	网络解组服务(DoS)		
利用有效账户	利用图形用户界面(GUI) 利用InstallUtil	更改默认文件关联 新建服务 利用有效用户	利用漏洞提权	组件对象模型(COM)劫持 网络执行命令 执行签名的二进制代...	输入验证	发现权限组 利用远程服务	浏览器中间人攻击(MIBS)	利用多代理	资源劫持		
	利用Launchctl	利用组件组件 启动Office应用程序 使用Web Shell	额外窗口内存注入(E...	利用连接代理 安装证书 会话发起协议(SIP)和...	欺骗用户输入凭证	发现进程 通过可移动介质复制	获取屏幕截图	创建多端通信	协议运行数据		
	利用Linux本地任务调度	创建用户 修改属性列表 Winlogon Helper D...	利用Hook	利用控制面服务 利用InstallUtil 软件壳 使用Kerberoasting技术	查询注册表	共享Webroot目录	捕获视频	使用多协议通信	禁用服务		
	利用SASS驱动程序	DLL搜索顺序劫持 窗口输入 Winlogon Helper D...	隐藏劫持	使用OSShadow技术 利用Launchctl 加入空档隐藏扩展名	利用Keychain	发现远程系统	SSH劫持	使用多倍加密	捕获本地存储数据		
	利用Msihta	Dylib劫持 端点监控	启动守护进程	禁用安全工具 仿冒 修改文件权限 网络嗅探	发现数据	利用系统中的第三方...	利用远程访问工具	拷贝远程文件	捕获传输中的数据		
	利用PowerShell	利用事件监听守护进程 利用PowerShell配置...	新建服务	DLL搜索顺序劫持 修改注册表 利用受信任的开发工具 利用Password Filter...	发现系统信息	利用Windows管理...	使用标准自举协议	使用标准加密协议			
	利用Regsvcs/Regasm	利用外部远程服务 利用RC.common文件	伪造父进程	DLL旁路加载 利用Msihta 利用有效用户	收集私钥	发现系统网络配置	利用Windows远程管...	使用标准自举协议			
	利用Regsvr32	利用文件系统权限漏洞 重启应用程序	信任拦截	按条件执行 删除网络共享连接 虚拟化/沙箱逃逸	利用Security的内存	发现系统网络连接	使用标准加密协议				
	利用RunDll32	隐藏文件和目录 冗余访问	修改属性列表	利用漏洞规避防御 利用NTFS交换数据流...	利用Web服务	窃取Web会话Cookie	发现系统所有者/用户	使用标准自举协议			
	利用计划任务	利用Hook 添加注册表运行值...	端口监控	额外窗口内存注入(EW... 混淆文件信息 利用XSL文件执行脚本	双因子认证拦截	发现系统服务	发现系统时间	利用web服务			
	使用脚本	利用Hypervisor 利用计划任务	利用PowerShell配置...	修改文件和目录数据 伪造父进程							
	利用windows服务	隐藏劫持 利用屏幕保护程序	进程注入	删除文件 修改属性列表							
	利用签名的二进制文...	利用内核数据块扩展 利用SSP DLL注册...	利用计划任务	文件系统逻辑劫持 端口输入							

- 相关/无关
- 降低动作成功率 (降低机会)
- 记录/告警
- 拦截
- 能力揭示

■ 不相关
■ 无效 (未覆盖)
■ 有效
● 可防御/可拦截
● 可检测/可记录
● 可降低机会
● 可输出知识

请输入子任务名称

侦察 (10)	资源开发 (6)	初始访问 (9)	执行 (10)	持久化 (18)	提权 (12)	防御规避 (37)	凭证访问 (14)	发现 (25)	横向移动 (9)	收集 (17)	命令与控制 (16)	数据渗出 (9)	影响 (13)
主动扫描	获取基础设施	水坑攻击	利用命令和本地脚本转移	操纵账户	滥用提升控制权限机制	滥用提升控制权限机制	暴力破解	发现账户	利用远程服务漏洞	后门/加密收集数据	使用应用程序协议	自动导出数据	删除账户权限
搜集受害者主机信息	入侵账户	利用面向公众的应用程序	利用主机软件漏洞执行	利用BITS服务	操纵访问令牌	操纵访问令牌	窃取密钥存储中的凭证	发现应用程序窗口	执行内部鱼叉式钓鱼攻击	捕获音频	通过可移动介质通信	限制传输数据大小	操纵数据
搜集受害者身份信息	入侵基础设施	利用外部远程服务	利用进程间通信	利用自动启动执行引导或登录	利用自动启动执行引导或登录	混淆文件和信息	利用凭证访问漏洞	发现浏览器书签	横向传输文件或工具	自动收集	编码数据	使用非C2协议回传	造成受影响的数据加密
搜集受害者网络信息	能力开发	添加硬件	利用API	利用初始化管理引导或登录	利用初始化管理引导或登录	从操作系统的启动	强制认证	发现基础设施结构	远程服务会话劫持	收集原始板数据	混淆数据	使用C2信道回传	操纵数据
搜集受害者组织信息	建立账户	网络钓鱼	利用计划任务/工作	添加驱动程序扩展件	创建或更改系统进程	直接访问卷	输入捕捉	云服务仪表盘	利用远程服务	收集云存储对象的数据	使用动态参数	使用其他网络介绍回传	篡改内容
通过网络钓鱼搜集信息	能力获取	通过可移动介质复制	利用共享模块执行	篡改客户端软件	事件触发执行	注意敏感域控制器	利用中间人攻击 (MITM)	云服务发现	通过可移动介质复制	收集配置库的数据	使用加密信道	使用物理介质回传	删除磁盘
从非公开来源搜集信息	入侵供应链	入侵供应链	利用第三方软件部署工具	创建账户	利用漏洞提权	使用Rootkit	修改身份验证过程	发现域信任	利用第三方软件部署工具	收集信息库数据	使用备用信道	使用Web服务回传	攻击物理基础设施 (DoS)
从公开技术数据库搜集信息	利用受信关系	利用受信关系	利用系统服务	创建系统进程	利用组策略修改	修改文件和目录权限	网络嗅探	发现文件和目录	污染共享内容	收集本地系统数据	使用入口工具传输	定时传输	损坏硬件
搜集公开网站/站	利用有效账户	利用有效账户	诱导用户执行	事件触发执行	执行流程劫持	修改组策略	操作系统凭证传输	扫描网络服务	使用鱼叉身份验证材料	收集网络共享驱动数据	创建多级信道	将数据转移到云账户	阻止系统恢复
搜集受害者自有网站	利用Windows管理工具 (WMI)	利用Windows管理工具 (WMI)	利用外部远程服务	执行流程劫持	进程注入	隐藏行为	窃取应用程序启动令牌	发现网络共享	使用鱼叉身份验证材料	收集可移动介质数据	使用标准非应用层协议	使用标准非应用层协议	网络嗅探服务 (DoS)
			启动Office应用程序	插入容器映像	利用计划任务/工作	利用计划任务/工作	窃取Web会话Cookie	网络嗅探	使用鱼叉身份验证材料	数据缓存	使用非标准端口	资源劫持	系统关机/重启
			在操作系统前启动	启动Office应用程序	利用有效账户	利用有效账户	窃取Web会话Cookie	发现密码策略	发现主机插入设备	收集电子邮件	使用协议隧道	禁用服务	
			利用计划任务/工作	利用流媒体	删除主机中的指标	删除主机中的指标	双因子认证拦截	发现权限组	发现主机插入设备	输入捕捉	使用代理		
			利用服务器软件组件	在操作系统前启动	网络防御机制	网络防御机制	未使用/不受支持的云资源	发现进程组	发现权限组	训练中间人攻击 (MITM)	利用流量窃听软件		
			使用流量指令	利用计划任务/工作	移除防御机制	移除防御机制	使用有效用户	发现进程组	发现进程组	利用中间人攻击 (MITM)	使用流量指令		
			利用有效账户	执行流程劫持	删除主机中的指标	删除主机中的指标	修改身份验证过程	查询注册表	发现远程系统	获取屏幕截图	利用合法Web服务		
				利用外部远程服务	网络执行命令	网络执行命令	修改云计算基础设施	发现远程系统	发现远程系统	捕获视频			
				插入容器映像	伪装	伪装	修改注册表	发现软件	发现软件				
				启动Office应用程序	使用流量指令	使用流量指令	修改注册表	发现系统信息	发现系统信息				
				在操作系统前启动	利用有效账户	利用有效账户	利用XSL文件执行脚本	发现系统网络配置	发现系统网络配置				
				利用计划任务/工作	删除防御机制	删除防御机制		发现系统网络连接	发现系统网络连接				
				利用服务器软件组件	移除防御机制	移除防御机制		发现系统所有者/用户	发现系统所有者/用户				
				使用流量指令	移除防御机制	移除防御机制		发现系统服务	发现系统服务				
				利用有效账户	移除防御机制	移除防御机制		发现系统时间	发现系统时间				
					移除防御机制	移除防御机制		虚拟化/沙箱逃逸	虚拟化/沙箱逃逸				

通过铸岳资产安全运维平台可以削弱那些攻击



初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用.bash_profile和... 启动代理	利用服务器软件组件 接管访问令牌	利用Setuid和Setgid位 接管访问令牌	发现账户	利用AppleScript	捕获音频	利用常用端口	自动渗出数据	删除账户权限
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能 启动守护进程	借助辅助功能 利用Setuid和Setgid位	填充二进制文件 修改组策略	利用应用程序窗口	利用应用程序部署软件	自动收集	通过可移动介质通信	压缩数据	浏览数据
利用外部远程服务	利用命令行	加入空格隐藏扩展名	接管账户 利用Launchctl	利用AppCert DLL(注... 利用AppInit DLL(注...)	SID历史注入 绕过用户账户控制(UAC)	发现浏览器书签	利用组件对象模型(C...	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据...
添加硬件	利用HTML编译文件	利用系统中的第三...	添加LC_LOAD_DYLIB 修改快捷方式	利用启动项 利用启动项	绕过用户账户控制(UAC) 清除命令历史	发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容替换攻击
通过可移动介质复制	利用组件对象模型(C...	利用Trap命令	利用AppInit DLL(注... 利用linux本地任务调度	利用Windows应用程... 绕过用户账户控制(U...	利用Sudo命令 利用Sudo缓存凭证	获取Web浏览器凭证	执行内部鱼叉式钓鱼...	收集本地系统数据	使用自定义加密协议	通过设备协议回传	删除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用受信的开发者工具	利用Windows应用程... 利用登录项	绕过用户账户控制(U... DLL搜索顺序劫持	利用CMSTP 代码签名	扫描网络服务	利用登录脚本	收集网络共享驱动数据	扫描网络服务	通过C2信道回传	删除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协议...	诱导用户执行	利用安装包 利用登录脚本	利用有效账户 利用有效账户	映像劫持 使用Web Shell	发现网络共享	利用密码哈希认证	收集可移动介质数据	发现网络共享	混淆数据	端点拒绝服务(DoS)
通过服务器执行鱼叉式...	通过API执行	利用Windows管理规...	利用BITS服务 利用LSASS驱动程序	Dylib劫持 使用Web Shell	投递后编译 阻止信标捕获	网络嗅探	利用Ticket认证	回传数据准备	网络嗅探	前置域名	破坏固件
入侵供应链	通过模块加载执行	利用Windows远程管...	使用Bootkit 修改现有服务	提示用户输入合法凭... 利用HTML编译文件	使用脚本 删除工具中的信标	发现文件和目录	利用远程桌面协议	收集电子邮件	发现密码策略	使用域名生成算法(DGA)	禁止系统恢复
利用受信关系	利用主机软件漏洞	利用XSL文件执行脚本	添加浏览器扩展插件 Netsh Helper DLL	利用事件监控守护进程 利用事件监控守护进程	利用HTML编译文件 删除主机中的信标	强制认证	浏览远程文件	输入捕捉	发现主机输入设备	使用备用信道	网络拒绝服务(DoS)
利用有效账户	利用图形用户界面(GUI)	利用XSL文件执行脚本	更改默认文件关联 新建服务	利用漏洞提权 利用漏洞提权	利用组件对象模型(COM)劫持 间接执行命令	输入捕捉	利用远程服务	浏览器中间人攻击(MitB)	发现权限组	利用多跳代理	资源劫持
	利用InstallUtil	利用XSL文件执行脚本	利用组件对象模型(COM)...	利用Hook 利用Hook	利用连接代理 安装根证书	输入捕捉	通过可移动介质复制	获取屏幕截图	发现进程	创建多级信道	操纵运行时数据
	利用Launchctl	利用XSL文件执行脚本	创建账户 修改属性列表	利用Hook 利用Hook	利用控制面板项 利用InstallUtil	输入捕捉	共享Webroot目录	捕获视频	查询注册表	使用多协议通信	禁用服务
	利用linux本地任务调度	利用XSL文件执行脚本	DLL搜索顺序劫持 端口敲门	映像劫持 启动守护进程	使用DCshadow技术 利用Launchctl	使用Kerberoasting技术	SSH劫持	发现远程系统	发现远程系统	使用多层加密	操纵本地存储数据
	利用LSASS驱动程序	利用XSL文件执行脚本	Dylib劫持 端口监控	新建服务 启动守护进程	反混淆/解密文件或信息 LC_MAIN劫持	利用Keychain	污染共享内容	发现安全软件	发现安全软件	端口敲门	系统关机/重启
	利用Mshta	利用XSL文件执行脚本	利用事件监控守护进程 利用PowerShell配置...	新建服务 伪造父进程	禁用安全工具 仿冒	网络嗅探	利用系统中的第三...	发现软件	发现软件	利用远程访问工具	操纵传输中的数据
	利用PowerShell	利用XSL文件执行脚本	利用外部远程服务 利用Rc.common文件	伪造父进程 路径拦截	DLL搜索顺序劫持 修改注册表	收集私钥	浏览远程文件	发现系统信息	发现系统信息	浏览远程文件	
	利用Regsvcs/Regasm	利用XSL文件执行脚本	利用文件权限漏洞 重启应用程序	路径拦截 修改属性列表	DLL旁路加载 利用Mshta	利用Securityd内存	使用标准应用层协议	发现系统网络配置	发现系统网络配置	使用标准应用层协议	
	利用Regsvr32	利用XSL文件执行脚本	隐藏文件和目录 冗余访问	修改属性列表 端口监控	按条件执行 删除网络共享连接	窃取Web会话Cookie	使用标准非应用层协议	发现系统所有者/用户	发现系统所有者/用户	利用不常用端口	
	利用Rundll32	利用XSL文件执行脚本	利用Hook 添加注册表运行键/启...	端口监控 利用PowerShell配置...	利用漏洞规避防御 利用NTFS交换数据流...	双因子认证拦截	利用Web服务	发现系统服务	发现系统服务	利用Web服务	
	利用计划任务	利用XSL文件执行脚本	利用Hypervisor 利用计划任务	进程注入 利用计划任务	额外窗口内存注入(EW... 混淆文件或信息			发现系统时间	发现系统时间		
	使用脚本	利用XSL文件执行脚本	映像劫持 利用屏幕保护程序		修改文件和目录权限 伪造父进程			虚拟化/沙箱逃逸	虚拟化/沙箱逃逸		
	利用windows服务	利用XSL文件执行脚本	利用内核模块和扩展 利用SSP DLL(注册表...		删除文件 修改属性列表						
	利用签名的二进制文...	利用XSL文件执行脚本			文件系统逻辑偏移 端口敲门						

- 不相关
- 无效 (未覆盖)
- 有效
- 可防御/可拦截
- 可检测/可记录
- 可降低机会
- 可输出知识

安天资产安全运维平台可以削弱的攻击



对比智甲和探海端点流量来看防御布防点的差异



初始访问	执行	持久化	提权	防御躲避	凭证访问	横向移动	收集	命令与控制	渗出	影响
本地攻击	利用AppletScript	利用Java的脚本引擎... 利用Java的脚本引擎... 利用Java的脚本引擎...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...

- 通过两者的对比，可见大部分攻击动作是基于系统实施和完成的。
- 同时各种安全能力环节有不同的价值和互补作用。

基于端点侧部署的安天智甲终端防御系统的检测和拦截点

初始访问	执行	持久化	提权	防御躲避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
本地攻击	利用AppletScript	利用Java的脚本引擎... 利用Java的脚本引擎... 利用Java的脚本引擎...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...	利用Windows的注册表... 利用Windows的注册表... 利用Windows的注册表...

基于流量侧部署的安天探海威胁监测系统的可输出的攻击动作标签

通过下一代威胁检测引擎+知识库输出载荷的TTPs



初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响						
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用bash_profile和...	启动代理	利用服务器软件组件	挂接访问令牌	绕过Gatekeeper	Process Doppelgänger...	挂接账户	发现账户	利用AppleScript	捕获音频	利用常用端口	自动渗出数据	删除账户权限		
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能	启动守护进程	利用服务器注册表权限...	挂接辅助功能	利用Setuid和Setgid	填充二进制文件	修改组策略	替换进程内存	查看Bash历史	发现应用程序窗口	利用应用程序部署软件	自动收集	通过移动介质通信	压缩数据	浏览数据
利用外部远程服务	利用命令行	加入空格隐藏扩展名	挂接账户	利用Launchctl	利用Setuid和Setgid	利用AppCert DLL(注...	SID历史注入	利用BITS服务	隐藏文件目录	进程注入	暴力破解	发现浏览器书签	利用组件对象模型(C...	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据...
添加硬件	利用HTML编译文件	利用系统中的第三万...	利用AppCert DLL(注...	添加LC_LOAD_DYLIB	修改快捷方式	利用AppInit DLL(注...	利用启动项	绕过用户账户控制(UAC)	隐藏用户	冗余访问	凭证转储	发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容置换攻击
通过移动介质复制	利用组件对象模型(C...	利用Trap命令	利用AppInit DLL(注...	利用linux本地任务调度	会话发起协议(SIP)和...	利用Windows应用程...	利用Sudo命令	清除命令历史	隐藏窗口	利用Regsvcs/Regasm	获取Web浏览器凭证	发现文件和目录	执行内部鱼叉式钓鱼...	收集本地系统数据	使用自定义加密协议	通过备份协议回传	清除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用受信的开发工具	利用Windows应用程...	利用登录项	利用启动项	绕过用户账户控制(U...	利用Sudo缓存凭证	利用CMSTP	HISTCONTROL	利用Regsvr32	获取文件中的凭证	扫描网络服务	利用登录脚本	收集网络共享驱动数据	编码数据	通过C2信道回传	清除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协...	诱导用户执行	利用认证包	利用登录脚本	利用系统固件	DLL搜索顺序劫持	利用有效账户	代码签名	映像劫持	使用Rootkit	获取注册表中的凭证	发现网络共享	利用密码哈希认证	收集可移动介质数据	混淆数据	通过其他网络介质回传	端点侧拒绝服务(DoS)
通过服务执行鱼叉式...	通过API执行	利用Windows管理理...	利用BITS服务	利用LSASS驱动程序	利用Systemd服务	Dylib劫持	使用Web Shell	投递后编译	阻止信标捕获	利用Rundll32	利用凭证访问漏洞	网络嗅探	利用Ticket认证	回传数据准备	前置域名	通过物理介质回传	损坏固件
入侵供应链	通过模块加载执行	利用Windows远程管...	使用Bootkit	修改现有服务	利用Windows时间服务	提示用户输入合法凭...		利用HTML编译文件	删除工具中的信标	使用脚本	强制认证	发现密码策略	利用远程桌面协议	收集电子邮件	使用域名生成算法(DGA)	定时传输	禁止系统恢复
利用受信关系	利用主机软件漏洞	利用XSL文件执行脚本	添加浏览器扩展插件	Netsh Helper DLL	利用Trap命令	利用系统监控守护进程		利用组件固件	删除主机中的信标	执行签名的二进制文...	利用Hook	发现主机接入设备	拷贝远程文件	输入捕捉	使用备用信道	网络侧拒绝服务(DoS)	
利用有效账户	利用图形用户界面(GUI)		更改默认文件关联	新建服务	利用有效账户	利用漏洞授权		组件对象模型(COM)劫持	间接执行命令	执行签名的脚本代理	输入捕捉	发现权限组	利用远程服务	浏览器中间人攻击(MitB)	利用多跳代理	资源劫持	
	利用InstallUtil		利用组件固件	启动Office应用程序	使用Web Shell	额外窗口内存注入(E...		利用连接代理	安装根证书	会话发起协议(SIP)和...	欺骗用户输入凭证	发现进程	通过可移动介质复制	获取屏幕截图	创建多级信道	挂接运行时数据	
	利用Launchctl		组件对象模型(COM)...	路径拦截	利用Windows事件订...	利用文件系统权限漏洞		利用控制面板项	利用InstallUtil	软件加壳	使用Kerberoasting技术	查询注册表	共享Webroot目录	捕获视频	使用多协议通信	禁用服务	
	利用linux本地任务调度		创建账户	修改属性列表	Winlogon Helper D...			使用DShadow技术	利用Launchctl	加入空格隐藏扩展名	利用Keychain	发现远程系统	SSH劫持	使用多层加密	挂接本地存储数据		
	利用LSASS驱动程序		DLL搜索顺序劫持	端口敲门		映像劫持		反弹URL/解密文件或信...	LC_MAIN劫持	模板注入	LLMNR/NBT-NS投毒...	发现安全软件	污染共享内容	端口敲门	系统关机/重启		
	利用Mshta		Dylib劫持	端口监控		启动守护进程		禁用安全工具	仿冒	修改文件时间戳	网络嗅探	发现软件	利用系统中的第三万...	利用远程访问工具	挂接传输中的数据		
	利用PowerShell		利用事件监控守护进程	利用PowerShell配置...		新建服务		DLL搜索顺序劫持	修改注册表	利用受信的开发工具	利用Password Filter...	发现系统信息	利用Windows管理理...	拷贝远程文件			
	利用Regsvcs/Regasm		利用外部远程服务	利用Rc.common文件		伪造父进程		DLL旁路加载	利用Mshta	利用有效账户	收集私钥	发现系统网络配置	利用Windows远程管...	使用标准应用层协议			
	利用Regsvr32		利用文件系统权限漏洞	重启应用程序		路径拦截		按条件执行	删除网络共享连接	虚拟化/沙箱逃逸	利用Securityd内存	发现系统网络连接		使用标准非应用层协议			
	利用Rundll32		隐藏文件和目录	冗余访问		修改属性列表		利用漏洞规避防御	利用NTFS交换数据流...	利用Web服务	窃取Web会话Cookie	发现系统所有者/用户		利用不常用端口			
	利用计划任务		利用Hook	添加注册表运行项/启...		端口监控		额外窗口内存注入(EW...	混淆文件或信息	利用XSL文件执行脚本	双因子认证拦截	发现系统服务		利用Web服务			
	使用脚本		利用Hypervisor	利用计划任务		利用PowerShell配置...		修改文件和目录权限	伪造父进程			发现系统时间					
	利用Windows服务		映像劫持	利用屏幕保护程序		进程注入		删除文件	修改属性列表			虚拟化/沙箱逃逸					
	利用签名的二进制文...		利用内核模块和扩展	利用SSP DLL(注册表...		利用计划任务		文件系统逻辑偏移	端口敲门								

- 不相关
- 无效 (未覆盖)
- 有效
 - 可防御/可拦截
 - 可检测/可记录
 - 可降低机会
 - 可输出知识

安天AVL SDK支持的攻击载荷TTPs标签输出

继续的问题



- 威胁视角是产品的从对抗能力的评价要素？
- 其是关键的，但不是唯一的，而且其不是一种结构性定义。
- 如何构建产品的能力价值视角？

智者安天下



长缨待展

威胁框架：细粒度对抗

04

从现有网络安全框架看对安全产品的能力需求

MITRE公司提出的Shield积极防御框架



MITRE公司是美国一家非盈利性研究机构，成立于1958年，最早主要做美国国防部的威胁建模，后续延伸到网络空间安全领域，其使命是“解决问题，创造更安全的世界”。



ATT&CK[®]

MITRE公司于2013年开始开发ATT&CK威胁框架，2015年5月正式发布，之后ATT&CK知识库通常每季度更新一次，持续更新中。

MITRE | Shield

MITRE公司于2019年创建MITRE Shield知识库，其结构与ATT&CK威胁框架类似。

MITRE Shield知识库——Shield



这个项目源于MITRE团队记录了在与对手交互行动中可能有用的技术。MITRE公司称其在网络欺骗和对手交互方面有着丰富的经验，因此对于团队来说，创建这个知识库也成为自然而然的过程。

为什么叫Shield?

Shield既是动词，意思是防御危险或风险；也是名词，意思是保护或盾牌。MITRE公司希望用户能够依据实际需求以多种方式使用Shield知识库。

Shield中为什么没有主动攻击?

MITRE公司认为攻击技术超出典型组织的工作范围，因此也不在MITRE Shield的关注范围内。

为什么称为积极防御知识库?

MITRE公司希望提高用户防御意识，激发防御者更积极的思维方式与对手进行对抗。充分利用防御者的优势赢得与对手对抗的最终胜利。

基于积极防御的MITRE Shield知识库



- MITRE公司将Shield知识库暂时分为战术、技术两个层次，共包含8个战术阶段、33种技术、其中欺骗防御技术中占比接近一半。

MITRE Shield知识库 (安天中译版)

DTA0001 引导 (18)		DTA0002 收集 (18)		DTA0003 约束 (11)		DTA0004 检测 (20)		DTA0005 干扰 (16)		DTA0006 促进 (16)		DTA0007 合法化 (12)		DTA0008 测试 (19)	
技术		技术		技术		技术		技术		技术		技术		技术	
技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文
DTE0001 管理员权限	Admin Access	DTE0003 API监控	API Monitoring	DTE0001 管理员权限	Admin Access	DTE0003 API监控	API Monitoring	DTE0001 管理员权限	Admin Access	DTE0001 管理员权限	Admin Access	DTE0004 应用多样性	Application Diversity	DTE0001 管理员权限	Admin Access
DTE0003 API监控	API Monitoring	DTE0004 应用多样性	Application Diversity	DTE0006 基线建立	Baseline	DTE0004 应用多样性	Application Diversity	DTE0004 应用多样性	Application Diversity	DTE0004 应用多样性	Application Diversity	DTE0008 痕迹仿真	Burn-In	DTE0003 API监控	API Monitoring
DTE0004 应用多样性	Application Diversity	DTE0005 备份与恢复	Backup and Recovery	DTE0010 诱饵账户	Decoy Account	DTE0007 行为分析	Behavioral Analytics	DTE0005 备份与恢复	Backup and Recovery	DTE0007 行为分析	Behavioral Analytics	DTE0010 诱饵账户	Decoy Account	DTE0004 应用多样性	Application Diversity
DTE0010 诱饵账户	Decoy Account	DTE0010 诱饵账户	Decoy Account	DTE0014 诱饵网络	Decoy Network	DTE0010 诱饵账户	Decoy Account	DTE0006 基线建立	Baseline	DTE0008 痕迹仿真	Burn-In	DTE0011 诱饵内容	Decoy Content	DTE0005 备份与恢复	Backup and Recovery
DTE0011 诱饵内容	Decoy Content	DTE0011 诱饵内容	Decoy Content	DTE0018 受控环境执行	Detonate Malware	DTE0011 诱饵内容	Decoy Content	DTE0007 行为分析	Behavioral Analytics	DTE0010 诱饵账户	Decoy Account	DTE0012 诱饵凭证	Decoy Credentials	DTE0010 诱饵账户	Decoy Account
DTE0012 诱饵凭证	Decoy Credentials	DTE0012 诱饵凭证	Decoy Credentials	DTE0020 硬件操控	Hardware Manipulation	DTE0012 诱饵内容	Decoy Content	DTE0011 诱饵内容	Decoy Content	DTE0011 诱饵内容	Decoy Content	DTE0013 诱饵多样性	Decoy Diversity	DTE0011 诱饵内容	Decoy Content
DTE0014 诱饵网络	Decoy Network	DTE0014 诱饵网络	Decoy Network	DTE0022 隔离	Isolation	DTE0014 诱饵网络	Decoy Network	DTE0012 诱饵凭证	Decoy Credentials	DTE0012 诱饵凭证	Decoy Credentials	DTE0014 诱饵网络	Decoy Network	DTE0012 诱饵内容	Decoy Content
DTE0015 诱饵角色信息	Decoy Persona	DTE0017 诱饵系统	Decoy System	DTE0023 迁移攻击向量	Migrate Attack Vector	DTE0017 诱饵系统	Decoy System	DTE0014 诱饵网络	Decoy Network	DTE0013 诱饵多样性	Decoy Diversity	DTE0015 诱饵角色信息	Decoy Persona	DTE0013 诱饵多样性	Decoy Diversity
DTE0016 诱饵进程	Decoy Process	DTE0018 受控环境执行	Detonate Malware	DTE0026 网络操控	Network Manipulation	DTE0019 电子邮件操控	Email Manipulation	DTE0019 电子邮件操控	Email Manipulation	DTE0015 诱饵角色信息	Decoy Persona	DTE0016 诱饵进程	Decoy Process	DTE0014 诱饵网络	Decoy Network
DTE0017 诱饵系统	Decoy System	DTE0019 电子邮件操控	Email Manipulation	DTE0032 安全控制	Security Controls	DTE0021 狩猎	Hunting	DTE0020 硬件操控	Hardware Manipulation	DTE0017 诱饵系统	Decoy System	DTE0017 诱饵系统	Decoy System	DTE0015 诱饵角色信息	Decoy Persona
DTE0018 受控环境执行	Detonate Malware	DTE0025 网络多样性	Network Diversity	DTE0036 软件操控	Software Manipulation	DTE0022 隔离	Isolation	DTE0022 隔离	Isolation	DTE0025 网络多样性	Network Diversity	DTE0025 网络多样性	Network Diversity	DTE0017 诱饵系统	Decoy System
DTE0023 迁移攻击向量	Migrate Attack Vector	DTE0027 网络监控	Network Monitoring	DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation	DTE0030 仿真数据	Pocket Litter
DTE0025 网络多样性	Network Diversity	DTE0028 PCAP收集	PCAP Collection	DTE0027 网络监控	Network Monitoring	DTE0032 安全控制	Security Controls	DTE0029 外设管理	Peripheral Management	DTE0029 外设管理	Peripheral Management	DTE0029 外设管理	Peripheral Management	DTE0023 迁移攻击向量	Migrate Attack Vector
DTE0026 网络操控	Network Manipulation	DTE0029 外设管理	Peripheral Management	DTE0028 PCAP收集	PCAP Collection	DTE0033 标准操控流程	Standard Operating Procedure	DTE0030 仿真数据	Pocket Litter	DTE0030 仿真数据	Pocket Litter	DTE0025 网络多样性	Network Diversity	DTE0025 网络多样性	Network Diversity
DTE0029 外设管理	Peripheral Management	DTE0031 协议解码器	Protocol Decoder	DTE0030 仿真数据	Pocket Litter	DTE0035 培训用户	User Training	DTE0032 安全控制	Security Controls	DTE0032 安全控制	Security Controls	DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation
DTE0030 仿真数据	Pocket Litter	DTE0032 安全控制	Security Controls	DTE0031 协议解码器	Protocol Decoder	DTE0033 标准操控流程	Standard Operating Procedure	DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation	DTE0029 外设管理	Peripheral Management	DTE0029 外设管理	Peripheral Management
DTE0032 安全控制	Security Controls	DTE0034 系统活动监控	System Activity Monitoring	DTE0033 标准操控流程	Standard Operating Procedure	DTE0034 系统活动监控	System Activity Monitoring	DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation	DTE0030 仿真数据	Pocket Litter	DTE0030 仿真数据	Pocket Litter
DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation	DTE0034 系统活动监控	System Activity Monitoring	DTE0035 培训用户	User Training	DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation	DTE0032 安全控制	Security Controls	DTE0032 安全控制	Security Controls
				DTE0035 培训用户	User Training	DTE0036 软件操控	Software Manipulation					DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation

Active Defense Matrix

Copyright © 2020, The MITRE Corporation.
MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.
<https://shield.mitre.org/matrix/>
安天研究院2021年01月译制



安天微信公众号

MITRE Shield知识库分类聚合分析



MITRE Shield知识库 (安天中译版)

DTA0001 引导 (18)		DTA0002 收集 (18)		DTA0003 约束 (11)		DTA0004 检测 (20)		DTA0005 干扰 (16)		DTA0006 促进 (16)		DTA0007 合法化 (12)		DTA0008 测试 (19)	
技术		技术		技术		技术		技术		技术		技术		技术	
技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文
DTE0001 管理员权限	Admin Access	DTE0003 API监控	API Monitoring	DTE0001 管理员权限	Admin Access	DTE0003 API监控	API Monitoring	DTE0001 管理员权限	Admin Access	DTE0001 管理员权限	Admin Access	DTE0004 应用多样性	Application Diversity	DTE0001 管理员权限	Admin Access
DTE0003 API监控	API Monitoring	DTE0004 应用多样性	Application Diversity	DTE0006 基线建立	Baseline	DTE0004 应用多样性	Application Diversity	DTE0004 应用多样性	Application Diversity	DTE0004 应用多样性	Application Diversity	DTE0008 痕迹仿真	Burn-In	DTE0003 API监控	API Monitoring
DTE0004 应用多样性	Application Diversity	DTE0005 备份与恢复	Backup and Recovery	DTE0010 诱饵账户	Decoy Account	DTE0007 行为分析	Behavioral Analytics	DTE0005 备份与恢复	Backup and Recovery	DTE0007 行为分析	Behavioral Analytics	DTE0010 诱饵账户	Decoy Account	DTE0004 应用多样性	Application Diversity
DTE0010 诱饵账户	Decoy Account	DTE0010 诱饵账户	Decoy Account	DTE0014 诱饵网络	Decoy Network	DTE0010 诱饵账户	Decoy Account	DTE0006 基线建立	Baseline	DTE0008 痕迹仿真	Burn-In	DTE0011 诱饵内容	Decoy Content	DTE0005 备份与恢复	Backup and Recovery
DTE0011 诱饵内容	Decoy Content	DTE0011 诱饵内容	Decoy Content	DTE0018 受控环境执行	Detonate Malware	DTE0011 诱饵内容	Decoy Content	DTE0007 行为分析	Behavioral Analytics	DTE0010 诱饵账户	Decoy Account	DTE0012 诱饵凭证	Decoy Credentials	DTE0010 诱饵账户	Decoy Account
DTE0012 诱饵凭证	Decoy Credentials	DTE0012 诱饵凭证	Decoy Credentials	DTE0020 硬件操控	Hardware Manipulation	DTE0012 诱饵凭证	Decoy Credentials	DTE0011 诱饵内容	Decoy Content	DTE0011 诱饵内容	Decoy Content	DTE0013 诱饵多样性	Decoy Diversity	DTE0011 诱饵内容	Decoy Content
DTE0014 诱饵网络	Decoy Network	DTE0014 诱饵网络	Decoy Network	DTE0022 隔离	Isolation	DTE0014 诱饵网络	Decoy Network	DTE0012 诱饵凭证	Decoy Credentials	DTE0012 诱饵凭证	Decoy Credentials	DTE0014 诱饵网络	Decoy Network	DTE0012 诱饵凭证	Decoy Credentials
DTE0015 诱饵角色信息	Decoy Persona	DTE0017 诱饵系统	Decoy System	DTE0023 迁移攻击向量	Migrate Attack Vector	DTE0017 诱饵系统	Decoy System	DTE0014 诱饵网络	Decoy Network	DTE0013 诱饵多样性	Decoy Diversity	DTE0015 诱饵角色信息	Decoy Persona	DTE0013 诱饵多样性	Decoy Diversity
DTE0016 诱饵进程	Decoy Process	DTE0018 受控环境执行	Detonate Malware	DTE0026 网络操控	Network Manipulation	DTE0019 电子邮件操控	Email Manipulation	DTE0019 电子邮件操控	Email Manipulation	DTE0015 诱饵角色信息	Decoy Persona	DTE0016 诱饵进程	Decoy Process	DTE0014 诱饵网络	Decoy Network
DTE0017 诱饵系统	Decoy System	DTE0019 电子邮件操控	Email Manipulation	DTE0032 安全控制	Security Controls	DTE0021 狩猎	Hunting	DTE0020 硬件操控	Hardware Manipulation	DTE0017 诱饵系统	Decoy System	DTE0017 诱饵系统	Decoy System	DTE0015 诱饵角色信息	Decoy Persona
DTE0018 受控环境执行	Detonate Malware	DTE0025 网络多样性	Network Diversity	DTE0036 软件操控	Software Manipulation	DTE0022 隔离	Isolation	DTE0022 隔离	Isolation	DTE0016 诱饵进程	Decoy Process	DTE0016 诱饵进程	Decoy Process	DTE0017 诱饵系统	Decoy System
DTE0023 迁移攻击向量	Migrate Attack Vector	DTE0027 网络监控	Network Monitoring			DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation	DTE0023 迁移攻击向量	Decoy System	DTE0023 迁移攻击向量	Decoy System	DTE0018 受控环境执行	Detonate Malware
DTE0025 网络多样性	Network Diversity	DTE0028 PCAP收集	PCAP Collection			DTE0027 网络监控	Network Monitoring	DTE0032 安全控制	Security Controls	DTE0029 外设管理	Peripheral Management	DTE0029 外设管理	Peripheral Management	DTE0023 迁移攻击向量	Migrate Attack Vector
DTE0026 网络操控	Network Manipulation	DTE0029 外设管理	Peripheral Management			DTE0028 PCAP收集	PCAP Collection	DTE0033 标准操控流程	Standard Operating Procedure	DTE0030 仿真数据	Pocket Litter	DTE0030 仿真数据	Pocket Litter	DTE0025 网络多样性	Network Diversity
DTE0029 外设管理	Peripheral Management	DTE0031 协议解码器	Protocol Decoder			DTE0030 仿真数据	Pocket Litter	DTE0035 培训用户	User Training	DTE0032 安全控制	Security Controls	DTE0032 安全控制	Security Controls	DTE0026 网络操控	Network Manipulation
DTE0030 仿真数据	Pocket Litter	DTE0032 安全控制	Security Controls			DTE0031 协议解码器	Protocol Decoder	DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation	DTE0029 外设管理	Peripheral Management
DTE0032 安全控制	Security Controls	DTE0034 系统活动监控	System Activity Monitoring			DTE0033 标准操控流程	Standard Operating Procedure							DTE0030 仿真数据	Pocket Litter
DTE0036 软件操控	Software Manipulation	DTE0036 软件操控	Software Manipulation			DTE0034 系统活动监控	System Activity Monitoring							DTE0032 安全控制	Security Controls
						DTE0035 培训用户	User Training							DTE0036 软件操控	Software Manipulation
动作相关	布置相关	操控相关	与产品无关			DTE0036 软件操控	Software Manipulation								

Active Defense Matrix

Copyright © 2020, The MITRE Corporation.
MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.
<https://shield.mitre.org/matrix/>
安天研究院2021年01月译制



安天微信公众号

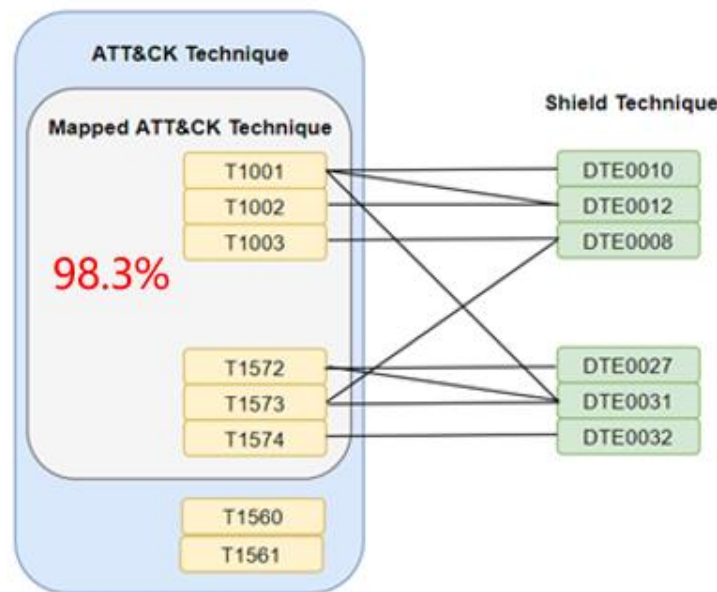
MITRE Shield知识库与ATT&CK威胁框架关系



MITRE Shield技术和ATT&CK威胁框架技术之间的映射关系

能对应上的ATT&CK技术总计有174个，占总数量（177）的98.3%，覆盖率已经较高

ATT&CK Technique	Opportunity Space	AD Technique	Use Case
T1078 - Valid Accounts	There is an opportunity to introduce user accounts that are used to make a system look more realistic.	DTE0010 - Decoy Account	A defender can create decoy user accounts which are used to make a decoy system or network look more realistic.
T1078 - Valid Accounts	There is an opportunity to deploy a tripwire that triggers an alert when an adversary touches a network resource or uses a specific technique.	DTE0012 - Decoy Credentials	A defender can seed systems with decoy credentials in a variety of locations and establish alerting that will trigger if an adversary harvests the credentials and attempts to use them.
T1078 - Valid Accounts	There is an opportunity to prepare user accounts so they look used and authentic.	DTE0008 - Burn-In	A defender can prepare a Decoy System by logging in to the Decoy Account and using it in ways consistent with the deception story, creating artifacts in the system that make it look legitimate.



MITRE Shield知识库与ATT&CK威胁框架相互映射

MITRE Shield知识库对ATT&CK威胁框架的覆盖率

MITRE Shield知识库的应用案例



Attivo Networks是一家位于加利福尼亚州弗里蒙特的网络安全服务公司，该公司宣称其提供的解决方案覆盖MITER Shield知识库中提出的33项主动防御技术中27项，覆盖范围达到82%，该公司还表示未覆盖领域主要是备份、硬件管理、培训以及其他与检测无关的行为活动。

Channel (18/18)	Collect (15/18)	Contain (9/11)	Detect (17/20)	Disrupt (11/16)	Facilitate (16/16)	Legitimize (12/12)	Test (18/19)
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Baseline	Application Diversity	Application Diversity	Application Diversity	Burn-In	API Monitoring
Application Diversity	Backup and Recovery	Decoy Account	Behavioral Analytics	Backup and Recovery	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Account	Decoy Network	Decoy Account	Baseline	Burn-In	Decoy Content	Backup and Recovery
Decoy Content	Decoy Content	Detonate Malware	Decoy Content	Behavioral Analytics	Decoy Account	Decoy Credentials	Decoy Account
Decoy Credentials	Decoy Credentials	Hardware Manipulation	Decoy Credentials	Decoy Content	Decoy Content	Decoy Diversity	Decoy Content
Decoy Network	Decoy Network	Isolation	Decoy Network	Decoy Credentials	Decoy Credentials	Decoy Network	Decoy Credentials
Decoy Persona	Decoy System	Migrate Attack Vector	Decoy System	Decoy Network	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Process	Detonate Malware	Network Manipulation	Email Manipulation	Email Manipulation	Decoy Persona	Decoy Process	Decoy Network
Decoy System	Email Manipulation	Security Controls	Hunting	Hardware Manipulation	Decoy System	Decoy System	Decoy Persona
Detonate Malware	Network Diversity	Software Manipulation	Isolation	Isolation	Network Diversity	Network Diversity	Decoy System
Migrate Attack Vector	Network Monitoring		Network Manipulation	Network Manipulation	Network Manipulation	Pocket Litter	Detonate Malware
Network Diversity	PCAP Collection		Network Monitoring	Security Controls	Peripheral Management		Migrate Attack Vector
Network Manipulation	Peripheral Management		PCAP Collection	Standard Operating Procedure	Pocket Litter		Network Diversity
Peripheral Management	Protocol Decoder		Pocket Litter	User Training	Security Controls		Network Manipulation
Pocket Litter	Security Controls		Protocol Decoder	Software Manipulation	Software Manipulation		Peripheral Management
Security Controls	System Activity Monitoring		Standard Operating Procedure				Pocket Litter
Software Manipulation	Software Manipulation		System Activity Monitoring				Security Controls
			User Training				Software Manipulation
			Software Manipulation				

Threat Defend平台与MITRE Shield知识库映射关系

MITRE Shield知识库的价值与不足



价值：

- Shield的表现形式有利于组织进行网络防御基础设施的部署决策过程；
- 防御者利用ATT&CK威胁框架分析已知对手战术、技术和信息等，同时利用MITRE Shield知识库部署网络防御措施计划以及捕获对下一步网络防御工作有用的信息，两者配合应用有利于加强组织防御能力。

不足：

- 尚处于初始阶段，分类、结构粒度较粗；
- 与ATT&CK威胁框架中攻击技术映射关系较粗；
- 其主要与ATT&CK威胁框架进行映射，但ATT&CK威胁框架尚无法枚举全部攻击方法，因此Shield存在先天不足；
- Shield中提及到的积极防御技术更多得在于通过诱骗捕获攻击行为，与积极防御的概念还存在一定差距。

MITRE | Shield



框架CORE（核心）

框架核心使用易于理解的通用语言提供一系列所需的网络安全活动和结果，指导企业以一种补充企业现有网络安全和风险管理流程的方式管理和降低其网络安全风险。

框架TIERS（实现层级）

通过提供有关机构如何看待网络安全风险管理的背景来帮助企业，指导企业为其网络安全计划考虑适当的严格程度，并经常作为沟通工具，以讨论风险偏好、任务优先级和预算。

框架PROFILE（轮廓/概况）

是企业的要求、目标、风险偏好、资源与框架核心预期结果的一致性评判。概述主要用于识别和优先考虑改善企业网络安全的机会。

NIST网络安全框架核心要素



框架功能	识别 ID	类别	子类别	参考性文献
保护 PR	类别	子类别	参考性文献	
检测 DE	类别	子类别	参考性文献	
响应 RS	类别	子类别	参考性文献	
恢复 RC	类别	子类别	参考性文献	

- 功能：基本的网络安全活动
- 类别：功能进一步细分
- 子类别：进一步将类别分为技术和/或管理活动的具体结果。
- 参考性文献：通用的标准、指南和实践的具体章节。

NIST网络安全框架核心要素



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Supply Chain Risk Management	ID.SC
	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
Respond	Detection Processes	DE.DP
	Response Planning	RS.RP
	Communications	RS.CO
Recover	Analysis	RS.AN
	Mitigation Improvements	RS.MI
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

- 5个功能
- 23个类别
- 108个子类别

功能唯一识别标识	功能	类别唯一识别标识	类别
ID	识别	ID.AM	资产管理
		ID.BE	业务环境
		ID.GV	治理
		ID.RA	风险评估
		ID.RM	风险管理策略
PR	保护	ID.SC	供应链风险管理
		PR.AC	身份管理和访问控制
		PR.AT	意识和培训
		PR.DS	数据安全
		PR.IP	信息保护流程与程序
		PR.MA	维护
		PR.PT	保护性技术
DE	检测	DE.AE	异常和事件
		DE.CM	安全持续监控
		DE.DP	检测流程
RS	响应	RS.RP	响应计划
		RS.CO	沟通
		RS.AN	分析
		RS.MI	缓解
		RS.IM	改进
RC	恢复	RC.RP	恢复计划
		RC.IM	改进
		RC.CO	沟通

NIST网络安全框架实践



- 框架轮廓是将功能、类别和子类别与组织业务需求、风险承受能力和资源相匹配的结果。
- 在与组织和部门目标高度一致的前提下，同时考虑法律法规要求和行业最佳实践，并反映风险管理的重点，建立出降低网络安全风险的路线图。

	Individual Functional Areas - Subject Matter Experts score their functional areas based on organization structure and for each function, category, and sub-category.			Scores - SME scores compared against independent core group.		Results - Combine scores and compare against targets set by organization. The resulting risk gap must be addressed.		
	Area 1 (i.e., Policy)	Area 2 (i.e., Network)	Area 3 (i.e., Applications)	SME Average	Core Group	Combined	Tier Target	Risk Gap
Identify								
Business	3	3	2	3	3	3	3	0
Asset	2	1	2	1	2	2	3	1
Governance	2	2	4	2	2	2	2	0
Risk Assess	2	2	2	2	2	2	2	0
Risk Management	2	2	2	2	2	2	3	1
Protect	2	1	1	1	1	1	3	2
Detect	2	2	2	2	2	2	3	1
Respond	1	1	2	1	2	1	3	2
Recover	2	4	3	3	3	3	4	1

一切正常
 需要工作
 需分析和校正

NIST CSF概要步骤



NIST和Shield的共性启示



- NIST虽然是一个风险管理、成熟度和覆盖力评价视角的框架，但其从“功能”逻辑上看构成了沿袭传统事前、事中、事后的认知痕迹，试图一个完整的安全行为闭环，而Shield更像针对APT型攻击更有针对性的猎杀闭环。
- 如果说杀伤链模型是攻击活动OODA循环的铺平展开，威胁框架则是对杀伤链模型的矩阵化并进一步多维化的细化展开。而NIST和Shield展示了共性特点是，防御同样存在着类似攻击杀伤链到威胁框架的战术阶段和技术动作。能有效应对确定性威胁动作和技术利用的关键防御动作是安全产品和能力环节的核心价值要素。
- 通过NIST和Shield也能看到部分的资产、环境、对象、位置等相关要素，但缺少有效的聚合。
- NIST和Shield的思路，为我们进一步梳理一套使用与指引安全能力和产品研发提供了非常重要的基础和参考。

智者安天下



长缨待展

威胁框架：细粒度对抗

05

从关键安全能力视角重新梳理能力性产品框架

编辑副标题

框架组成



核心要素——关键防御动作战术环节



塑造是建立防御主动性的前提。对关键系统要素制定标准、定义系统控制原则或利用资产、拓扑、场景以及环境等的识别进行模拟的过程，旨在更好的与对手进行威胁对抗活动。

检测是发现、定位和定性网络安全威胁的方法统称。制定并执行适当的行动对边界、端点、流量等进行检测，发现系统存在或潜在的漏洞、风险等，旨在避免网络安全事件的发生。



识别 (Identify)



塑造 (Shape)



防护 (Protect)



检测 (Detect)



响应 (Respond)

识别是网络安全管理的基础。通过培养并提升组织对网络安全风险的认识能力，加以对系统、人员、资产、数据以及功能等进行网络安全管理，旨在提升组织对自身的认知。

防护是系统对威胁做出的行为反制。通过制定并执行具有针对性的保障措施，使组织具备限制或控制潜在网络安全事件产生影响的能力，旨在确保关键服务的网络安全性。

响应是处理、管理风险和威胁事件的过程。通过制定并执行适当的行动，利用组织所具备的控制潜在网络安全事件影响的能力，对检测到的网络安全事件采取处置措施，旨在清除网络安全事件影响。

核心要素——作用对象集合



网络类对象

- 地址、端口、通联、协议、拓扑

用户类对象

- 用户、帐户、身份、权限

应用类对象

- 基础类：DNS、TLS、VPN、RDP……
- 业务类：邮件、WEB、FTP、网盘、视频会议……

信息类对象

- 配置、脆弱点、补丁、……

作用承载类对象

- 文件、载荷、进程、内存、服务……

作用位置属性类对象

- 主机、边界、流量、应用系统、供应链……

安天认为：安全的可运营基础来自持续的对象数据采集和元数据化！

核心要素——防御动作集合

身份认证、权限控制、配置基线建立、网络域划分、数据资产分级分类、网络通联约束、仿真资产构造、主机行为管控……

主机环境检测（载荷检测、进程检测、内存检测、异常行为检测）、流量环境检测（全流量解析还原、全要素记录、入侵检测、C2检测、恶意代码检测、DNS检测、加密流量检测、异常通联检测、邮件还原检测、自定义场景检测）、应用环境检测（SQL注入检测、跨站脚本攻击检测、DDOS攻击检测……）、威胁情报检测……



资产识别、业务识别、网络空间识别、用户识别、配置识别、漏洞识别、补丁识别、供应链识别、行为识别……

主机安全防护、外设安全防护、边界安全防护、数据安全防护、应用安全防护、运维安全防护……

缓解、固证、提取、分析、清除、恢复、策略调整……

安天能力型安全产品框架 V0.1



关键防御动作矩阵

识别	塑造	防护	检测	响应
资产识别	身份认证	主机防护	系统环境检测	缓解
业务识别	权限控制	外设防护	流量环境检测	固证
网络空间识别	配置基线建立	通信网络防护	应用环境检测	提取
用户识别	网络通联约束	数据安全防护	数据体检测	分析
配置识别	数据资产分级分类	应用安全防护		清除
暴露面/脆弱性识别	仿真资产构造	运维安全防护		恢复
活动识别	主机行为管控			策略调整

作用对象

网络类	用户类	应用类	信息类	执行体类	作用位置
内容 地址 协议 端口	用户 帐户 身份 权限	DNS TLS VPN 邮件 WEB	配置 补丁 脆弱点	载荷 进程 内存 服务	主机 边界 流量 应用 流程

部署方式

与被保护对象原生融合or安装 | 基于载体设备部署 | 基于虚拟化资源部署

管理模式

单点管控/集中管控 | 无管控

认知威胁	攻击者	意图	装备	载荷	行为	被攻击者	脆弱性	检测结果	后果	保护目标	硬件资产	软件资产	外设资产	数据资产	仿真资产
------	-----	----	----	----	----	------	-----	------	----	------	------	------	------	------	------

- 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

智者安天下

海阔凭鱼跃 天高任鸟飞

长缨缚展

威胁框架：细粒度对抗