智甲如何实现端点侧细粒度防御与处置

安天产品事业部

威胁框架：细粒度对抗

長纓待展

CONTENTS

目 录

智者安天下

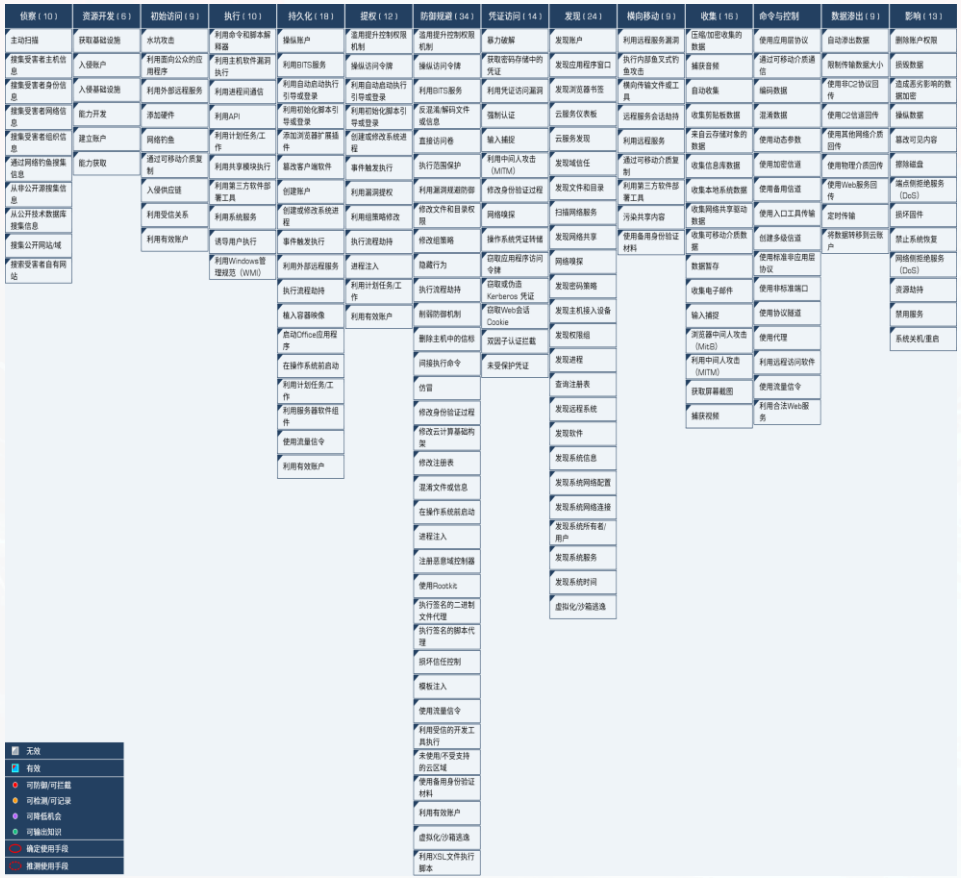
01 细粒度防御的价值与要素

端点是网络威胁对抗的主战场以及最后一道防线

- 端点中存储着用户最重要的核心资产，也是业务系统稳定运行的关键支撑
- 大部分的攻击技战术动作都是在端点环境中完成
- 传统物理隔离和网络边界的威胁拒止成功率在持续降低
  - 可移动介质复制
  - 入侵供应链技术
  - 流量加密技术的广泛使用

端点是网络威胁对抗中的主战场 → **我们退无可退** → 需要在端点建立更加有效的防御和处置能力，以应对新的威胁挑战

针对端点的攻击技术在威胁框架中占有最高比重



对ATT&CK威胁框架中攻击技术统计分析可以发现：

攻击技术大类：**200**项
端点相关技术：**117**项，占比**58.5**%

子技术总数：**560**项
端点相关技术：**440**项，占比**78.5**%

细粒度的攻击技战术，需要细粒度的应对

端点安全防护产品现状、问题以及应对

现状

目前市场上已经具有多种类型的端点安全防护产品

- 杀毒软件
- 桌管系统
- 主机审计系统
- 入侵检测系统
- 数据防外泄系
- EDR类产品
- ...

主流产品能力都相对成熟，每款产品的防御范围和能力都具有明确针对性

问题

- 端点资源有限，安装过多安全产品势必会对主机性能产生影响，并且存在兼容性风险
- 各品类产品都具有明显的防御短板，如EPP类产品具有较强主防能力，但数据采集能力弱，无法有效捕获未知威胁；而EDR类产品虽然数据采集能力强，但主防能力弱，导致无法及时遏制攻击行为，保护核心资产
- ……

应对

- 突破传统EPP、EDR等产品边界的局限，在整个威胁框架的基础上，将端点所有安全性整合，由统一平台运营管理，响应所有端点的威胁。为实现这一目的，需要提高安全产品在威胁框架中的能力覆盖度
- 针对威胁框架中的各个子技术手段建立有针对性的响应策略，例如拦截高危行为、提醒敏感行为、记录常规行为，即实现“细粒度防御与处置”
- ……

端点安全一体化防护，细粒度防御和处置是实现这一目标的关键基础

实现端点细粒度防御和处置的三要素

针对攻击技术足够全面的防御点覆盖度

威胁框架枚举出了攻击者所使用的攻击数据，而要想实现对各类威胁的防御或者感知，就要求安全产品具有足够的覆盖度，在主要环节、主要技术上不允许有空白，而且不仅仅是要对攻击手段粗粒度的防御，而是要对威胁框架中的子技术也全面覆盖

精细化的防御检测和处置点

威胁框架中的技术虽然可被攻击者利用，但这并不能说使用该种技术就一定是攻击行为，如果采用传统匹配及拦截模式，不仅会产生大量误报，还会影响业务系统，因此要对技术进行划分：针对高危行为（例如“凭证访问-暴力破解”）立刻进行拦截，对敏感行为（例如“执行-利用系统服务”）要参考用户环境、上下文等仅产生事件告警，对于常规行为（例如“数据渗出-使用Web服务回传”）则后台记录，未来如果有需要可进行攻击回溯

可运维的响应能力

针对不同环境、不同的防御需求，产品应能提供不同的防御能力，这需要安全产品可进行细粒度的运维，例如不同防御点是否启用，响应方式如何等，管理人员都可以针对具体场景按需配置，并且支持与SOAR等系统的联动。

02 智甲细粒度防御的技术说明

智甲产品能力指标

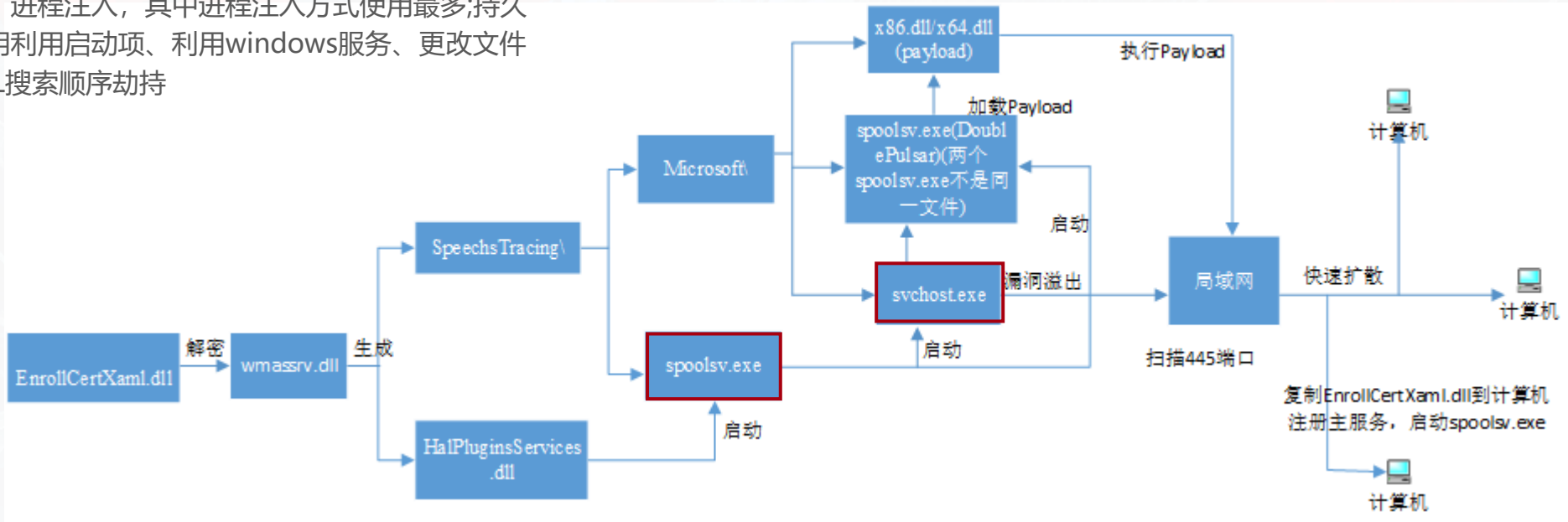
在**440**个端点相关的子技术中

广度：智甲目前可覆盖**256**项，其中默认策略为告警方式有**52**项，策略为仅记录的**204**项

深度：持久化（自启动）和提权（进程注入）

实战案例1——WannaMine案例分析（1）

挖矿病毒为了达到长时间在系统中运行，通常使用持久化和各种隐藏方式来达到目的。隐藏方式包括隐藏进程、捆绑进程、进程注入，其中进程注入方式使用最多;持久化较多使用利用启动项、利用windows服务、更改文件关联、DLL搜索顺序劫持



WannaMine病毒作业流程

实战案例1——WannaMine案例分析（2）

ATT&CK威胁框架中涉及到进程注入的子技术共11种，智甲针对这11种技术对应的防御点如下：

序号	攻击技术	默认防御策略	实现机理
1	动态链接库注入	通过Hook可以监控指令序列，当CreateRmoteThread函数调用后，判断被注入进程，是直接告警，反之记录。不调用此指令序列不进行任何防御动作。Hook放行后，Ring0层感知DLL加载，拦截DLL加载，投递AVL扫描，白放行并记录，黑阻止加载并输出标签	Ring0驱动/Ring3Hook
2	可执行文件注入	同动态链接库注入方式类似，Hook放行后，Ring0层感知进程启动，投递AVL扫描，白放行并记录，黑阻止运行并输出标签	Ring0驱动/Ring3Hook
3	线程执行劫持	通过Hook监控对应的指令序列，当ResumeThread函数调用后，判断被改写的线程是否属于系统进程或指定第三方应用程序，是直接告警，反之记录。不调用此指令序列不进行任何防御动作	Ring3Hook
4	异步过程调用（APC）	通过Hook监控对应的指令序列，当WriteProcessMemory函数调用后，判断被插入APC的进程是否属于系统进程或指定第三方应用程序，是直接告警，反之记录。不调用此指令序列不进行任何防御动作	Ring3Hook
5	线程本地存储（TLS）	通过Hook监控对应的指令序列，当ResumeThread函数调用后，判断被TLS回调修改的进程是否属于系统进程或指定第三方应用程序，是直接告警，反之记录。不调用此指令序列不进行任何防御动作	Ring3Hook
6	Process Hollowing（利用进程镂空注入）	通过Hook监控对应的指令序列，当ResumeThread函数调用后，判断被改写的线程是否属于系统进程或指定第三方应用程序，是直接告警，反之记录。不调用此指令序列不进行任何防御动作	Ring3Hook

实战案例1——WannaMine案例分析（3）

序号	攻击技术	默认防御策略	实现机理
7	Process Doppelgänging（仿冒合法进程）	通过Hook可以监控指令序列，当内存改写完成后，当RollbackTransaction函数调用后，判断被改写的进程是否为系统进程或指定第三方应用程序，是直接告警，反之记录。不调用此指令序列不进行任何防御动作	Ring3Hook
8	额外窗口内存注入（EWMI）	通过Hook可以监控指令序列，当内存改写完成后，当SendNotifyMessage函数调用后，判断被改写的进程是否为系统进程或指定第三方应用程序，是直接告警，反之记录。不调用此指令序列不进行任何防御动作	Ring3Hook
9	VDSO劫持（Linux&国产化）	通过Ring0层监控，判断被修改的进程是否属于系统进程或第三方应用程序，是直接告警，反之记录	Ring0驱动
10	利用ptrace系统调用注入（Linux&国产化）	通过Ring0层监控Ptrace系统调用，判断被附加的进程是否属于系统进程或第三方应用程序，是直接告警，反之记录	Ring0驱动
11	利用Proc内存注入（Linux&国产化）	通过Ring0层监控，判断被修改的进程是否属于系统进程或第三方应用程序，是直接告警，反之记录	Ring0驱动

实战案例1——WannaMine案例分析（4）

再以WannaMine利用的持久化技术为例，威胁框架中实现持久化的子技术主要包括84种，智甲目前已覆盖50种子技术。
针对常用6种技术对应的防御策略如下：

序号	攻击技术	默认防御策略	实现机理
1	利用启动项	可以实时感知注册表启动项的创建和启动目录的文件的创建，通过AVL引擎检测，查看启动项的内容是否为白，白只记录，否则告警	Ring0驱动
2	利用Windows服务	可以实时感知注册表服务项的创建和服务的启动，主要采取记录方式，并使用AVL引擎扫描启动的服务进程	Ring0驱动
3	更改文件关联	可以实时感知注册表文件关联项的更改，当修改的进程不是regedit.exe时，进行记录，并使用AVL检测修改后的关联进程	Ring0驱动
4	DLL搜索顺序劫持	可以实时感知DLL的加载，当发现DDL劫持时，主动告警，并阻止DLL加载	Ring0驱动
5	利用AppInit DLL	可以实时感知注册表项AppInit_DLLs的改写，当发现被改写时，主动告警，并阻止注册表修改	Ring0驱动
6	利用计划任务	可以实时感知Tasks目录下的文件创建，并解析对应内容，记录要启动的进程、启动时间等信息，并使用AVL检测要启动的进程	Ring0驱动

实战案例1——WannaMine案例分析（5）


安天

六小时处置挖矿蠕虫的内网大规模感染事件

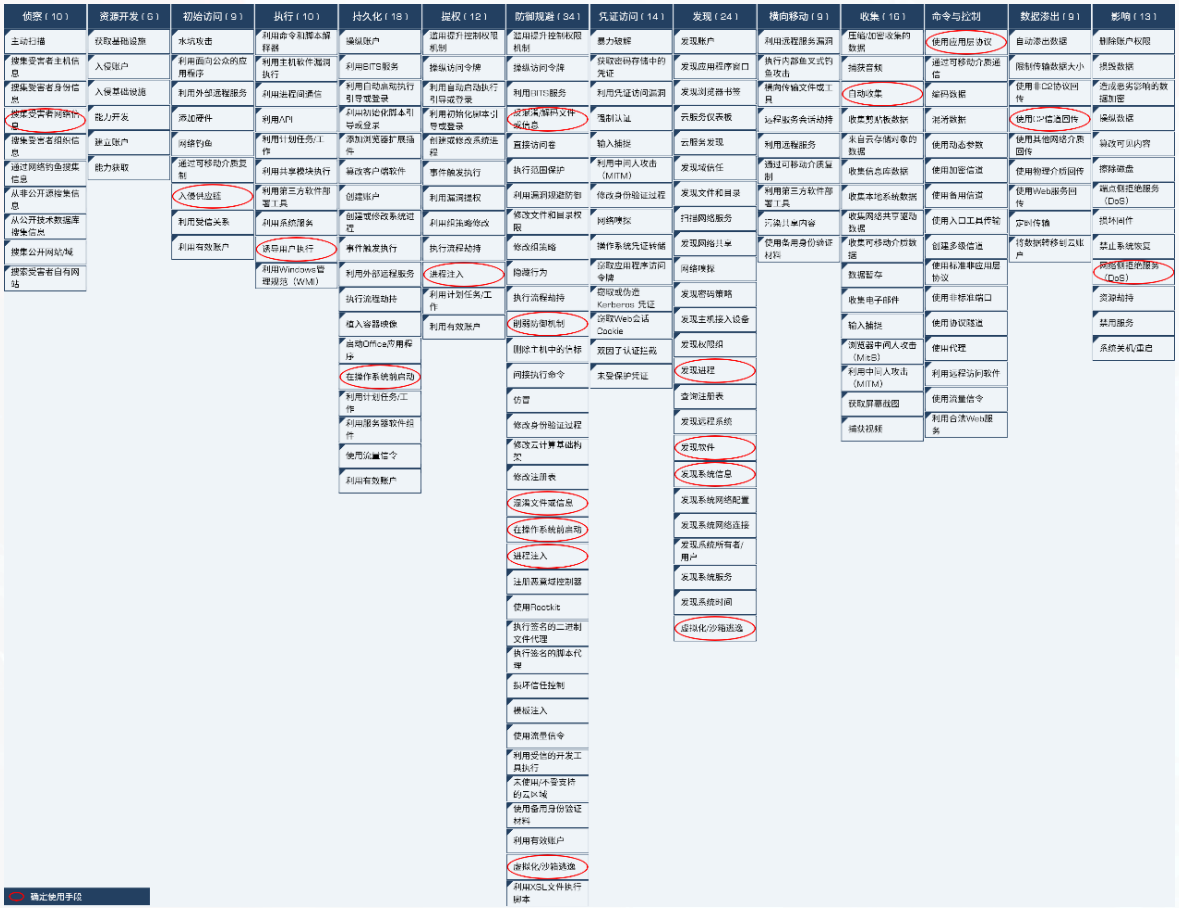
安天端点安全产品研发部

初稿完成时间：2019 年 9 月 24 日
本版更新时间：2019 年 9 月 25 日

扫二维码获取最新版报告

安天发布报告
《六小时处置挖矿蠕虫的内网大规模感染事件》

实战案例2——暗云Ⅲ（1）

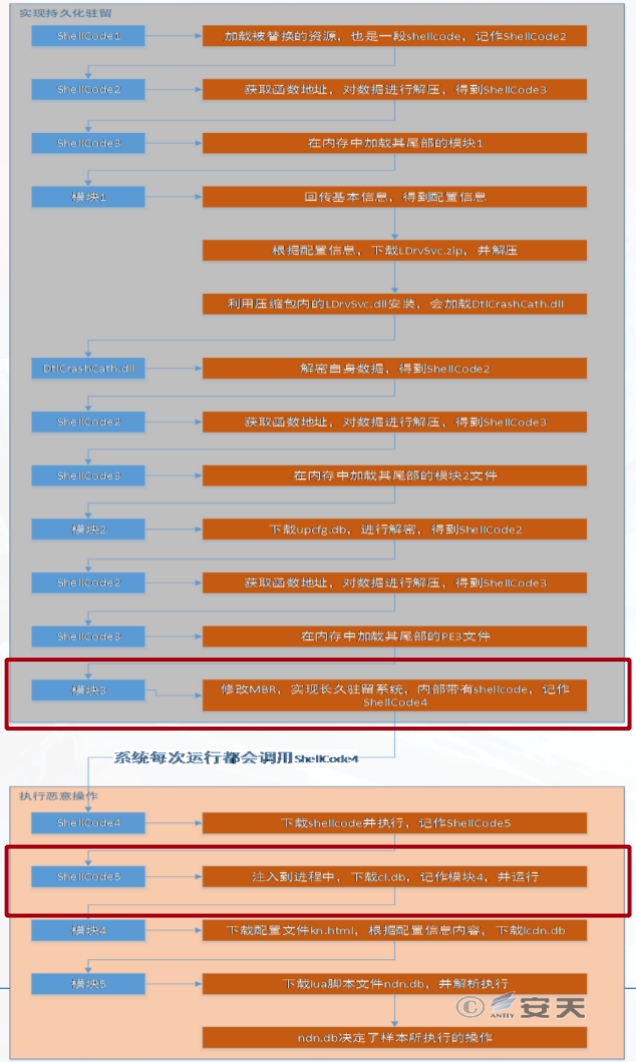


1. “入侵供应链“->”入侵软件供应链“子技术：捆绑下载器中的软件和一些正常游戏客户端；

2. “操作系统前启动”->“使用Bootkit MBR”子技术：系统引导时加载恶意程序；

3. “反混淆/解码文件或信息”：在内存中多次解密ShellCode，以躲避查杀。

实战案例2——暗云Ⅲ（2）



暗云三攻击流程为：通过捆绑游戏进程进行传播，当用户执行捆绑游戏进程后，以ShellCode方式进行加载，进行各种下载解密操作，利用解密后的恶意程序修改MBR，并且注入svchost中，进行下载配置文件和脚本文件。

对应ATT&CK框架中与终端有关的技术动作，只有进程注入被智甲拦截，但是在操作系统前启动只作为记录形式。

实战案例2——暗云Ⅲ（3）

安天针对“暗云Ⅲ”的样本分析及解决方案

安天ARR(Antiy Response Rule)开放式处置规则定义

ARR（Antiy Response Rule）的部分指令集		
一、注册表（可配自动处置规则）	1.创建注册表项/值	[Reg_Create]
	2.修改注册表项/值	[Reg_Modify]
	3.删除注册表项/值	[Reg_Delete]
	4.重命名注册表项/值	[Reg_Rename]
	5.删除注册表值	[Reg_Delete_Value]
二、计划任务（可配自动处置规则）	1.创建计划任务	[Task_Create]
	2.修改计划任务	[Task_Modify]
	3.删除计划任务	[Task_Delete]
三、文件（可配自动处置规则）	1.创建文件	[File_Create]
	2.修改文件	[File_Modify]
	3.删除文件	[File_Delete]
	4.重命名文件	[File_Rename]
	5.修改文件属性	[File_Attribute]
	6.删除文件指定内容	[File_DelText]
	7.MBR修复	[File_repairMbr]
四、进程（可配自动处置规则）	1.创建进程	[Proc_Create]
	2.挂起/恢复进程	[Proc_Modify]
	3.结束进程	[Proc_Terminate]
	4.挂起指定模块线程	[Proc_Module_Threads]
五、脚本	1.下发bat脚本并运行	[Script_Bat]
	2.下发shell脚本并运行	[Script_Shell]
	3.下发vbs脚本并运行	[Script_Vbs]
	4.下发powershell脚本并运行	[Script_PWL]
	5.下载文件并运行	[Script_File]
六、其他	1.外设弹出/规则	[Other_Device]
	2.断网处置	[Other_NetOff]
	3.禁用端口	[Other_Disabled_Port]
	3.禁用ip	[Other_Disabled_Ip]
	4.补丁修复	[Other_Fix_patch]
	5.创建互斥免疫	[Other_Create_Mutex]
	6.创建扫描并自动处置	[Other_QuickScan]

安天ARR开放式处置规则定义是安天为实现细粒度端点响应策略而定义的一组指令集合，包括了对扇区、注册表、文件、驱动、进程等进行相关操作的动作定义，并可以执行包括磁盘遍历，特征匹配搜索等逻辑动作。可以用于处理策略编排、专杀脚本生成，以执行细粒度的处置动作。

安天智甲可以执行SOAR下达的细粒度处置规则指令。

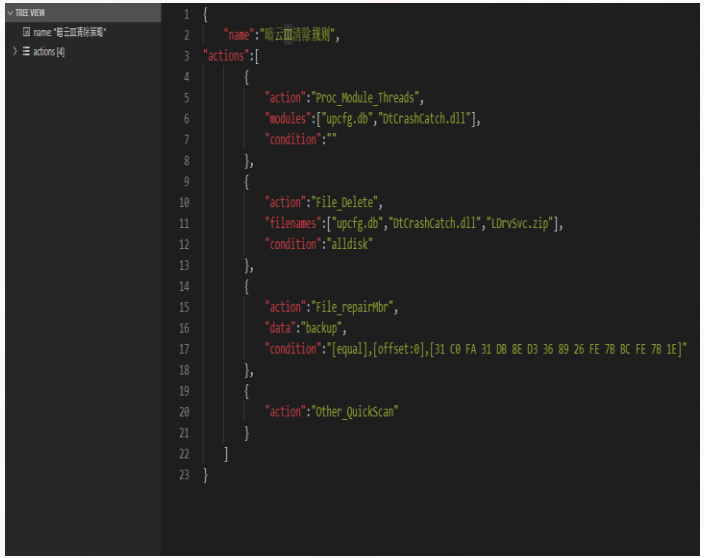
ARR处置规则支持判定条件，用于触发相应处置:

File_Delete
condition:
全盘：alldisk，系统磁盘：systemdisk，磁盘根目录：diskroot，全盘指定深度：alldisk_deep:1-100
移动设备:udisk

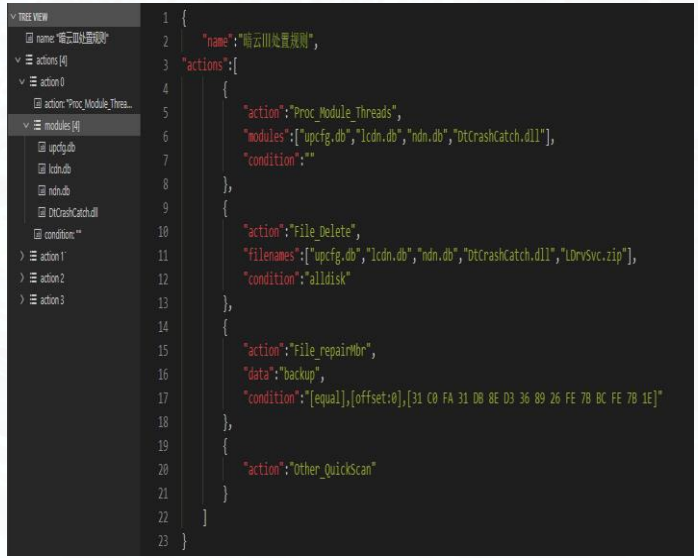
File_repairMbr
condition:
[判定方式],[偏移],[对比内容]
[equal/Unequal],[offset:0],[31 c0 fa]

借助SOAR和专杀工具实现特殊威胁处置

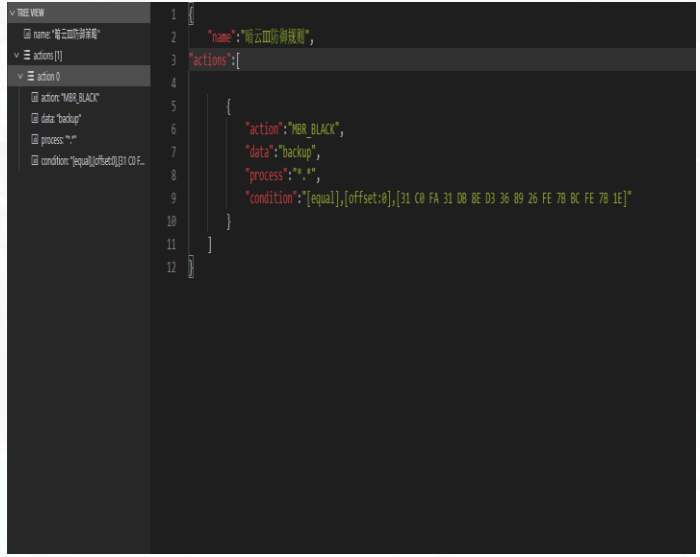
针对一些具有极高复杂度或者顽固性的病毒，智甲支持与SOAR平台联动，由SOAR平台生成更加复杂的处置策略，并由智甲进行执行。针对无法安装智甲客户端的主机，可以通过专杀工具实现威胁处置工作



清除规则



处置规则



防御规则

产品防御策略可配置、可运营

防御与感知能力不能是静态的，而是要可以根据环境不同实现动态调整，智甲具有安全管理中心，可为用户提供可交互的防御策略配置和运维能力。

03 总结与未来展望

智甲细粒度防御能力建设的几点经验

01 端点的稳定性是第一位的

02 优先对高频攻击技术进行投入

03 细粒度防御不是简单的防御点堆叠

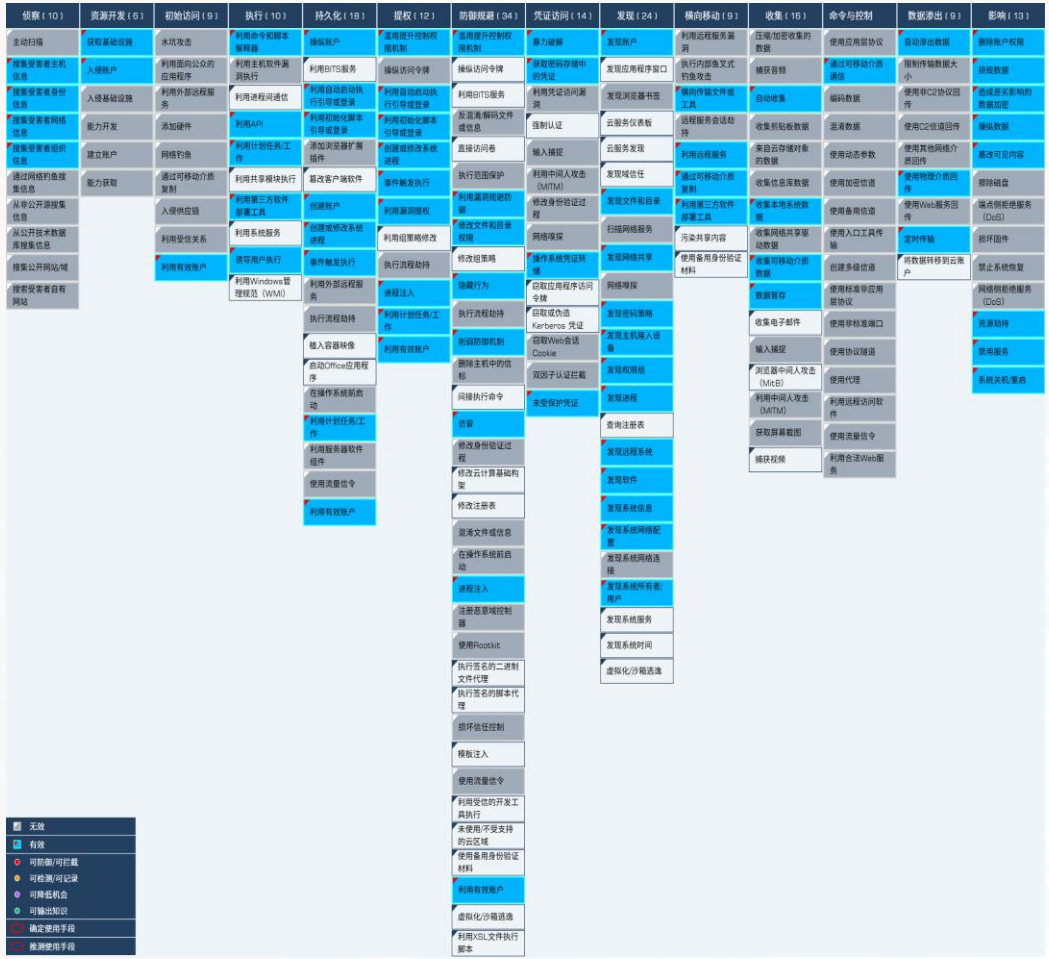
深入分析正常和异常行为差异将是未来持续的工作重点

准确判断

威胁框架对攻击技术进行了较为全面的枚举，但是实际环境中大量正常软件也会利用这些技术，如果不进行精准划分，将导致大量误报或者无用数据的生产，而能够更加准确的判断是异常行为还是正常行为将是将防御能力落地的关键。

- 加大数据采集和分析粒度，从程序身份、行为特征、关系链等多个更细粒度去采集程序的相关信息，建立更加丰富的情报库
- 参与用户环境精细化运维，以往安全厂商的运维服务主要是系统升级等常规工作，我们认为未来安全厂商应加大用户环境的安全运维工作，以运维服务推动产品优化
- 对于已有数据要及时更新，任何技术或者业务都是动态变化的，正常软件也并非一直安全而不被利用，因此要始终关注变化，及时调整产品的检测规则。

信创系统也需要细粒度的防御与处置



信创系统必然是高级网空威胁行为体重点分析研究、研发针对性木马和漏洞利用工具的重点目标，更需要加强防范。与此同时，在国产化系统中的挖矿木马、勒索病毒已经出现，信创系统更需要构建细粒度防御与处置能力。

我们退无可退！