



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

SOAR如何编排指引细粒度的端点处置

安天平台产品部

威胁框架：细粒度对抗

長纓縛展

長纓待展

CONTENTS

目 录

01

面临的挑战

02

什么是SOAR

03

安天SOAR案例

04

安天SOAR架构

05

安天SOAR特点

智者安天下



长缨待展

威胁框架：细粒度对抗

01

面临的挑战

面临的挑战

响应时间过长
解决安全事件的平均时长约4.35天。



培养周期长人员流失大
培训初级安全分析师通常需要8个月，1/4的安全分析师2年就会转岗。



专业人员不足

约80%的公司企业没有足够的分析师运营其SOC，安全从业人员缺口约140万。



自动化程度不足

62%的受访者希望有自动化工具的辅助。



DEMISTO的SOAR行业报告

智者安天下



长缨待展

威胁框架：细粒度对抗

02

什么是SOAR

什么是SOAR



Security Orchestration, Automation and Response 安全编排自动化与响应

SOAR 是从安全编排和自动化 (SOA) ,
安全事件响应平台 (SIR) 和威胁情报平台 (TIP) 整合而来。

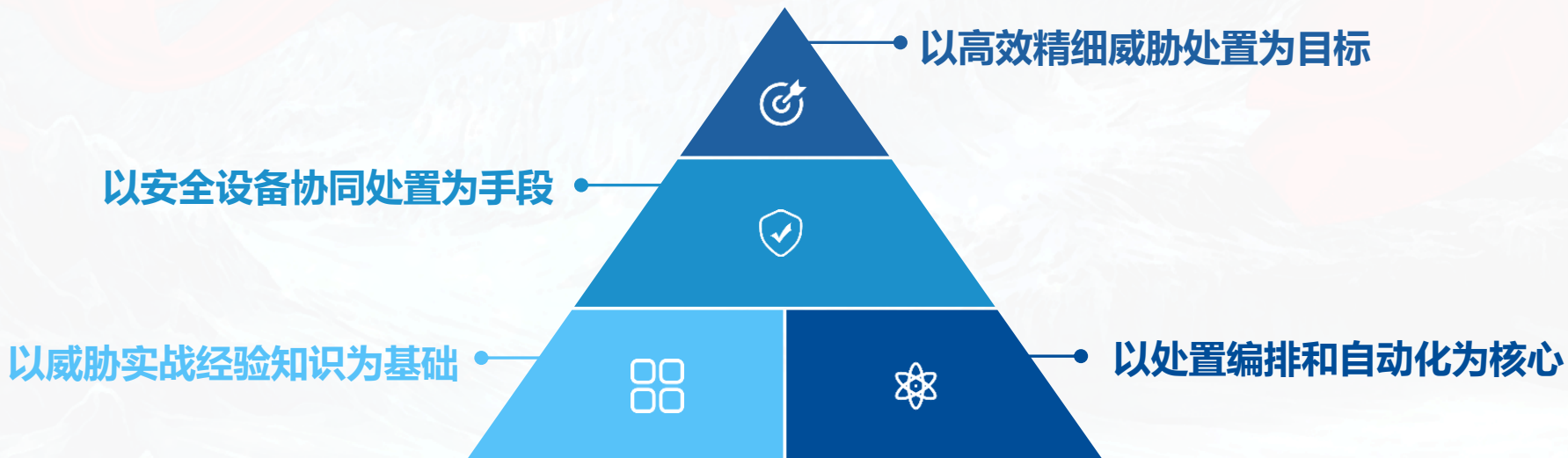


SOAR是一类从各种来源获取输入，并应用工作流来拉通各种安全过程与规程，从而为安全运营人员提供机器协助的解决方案。这些过程和规程可以被编排（通过与其它技术的集成）并自动执行以达成预期结果，譬如分诊管理，事件响应，威胁情报，合规性管理和威胁猎捕。

SOAR are solutions that add machine assistance to human security operators by taking inputs from various sources and applying workflows aligned to processes and procedures. Those procedures can then be orchestrated (via integrations with other technologies) and automated to achieve a desired outcome, such as triage management, incident responders, threat intelligence, compliance managers, and threat hunting.

来源：<https://www.gartner.com>

安天对SOAR的认知



智者安天下



长缨待展

威胁框架：细粒度对抗

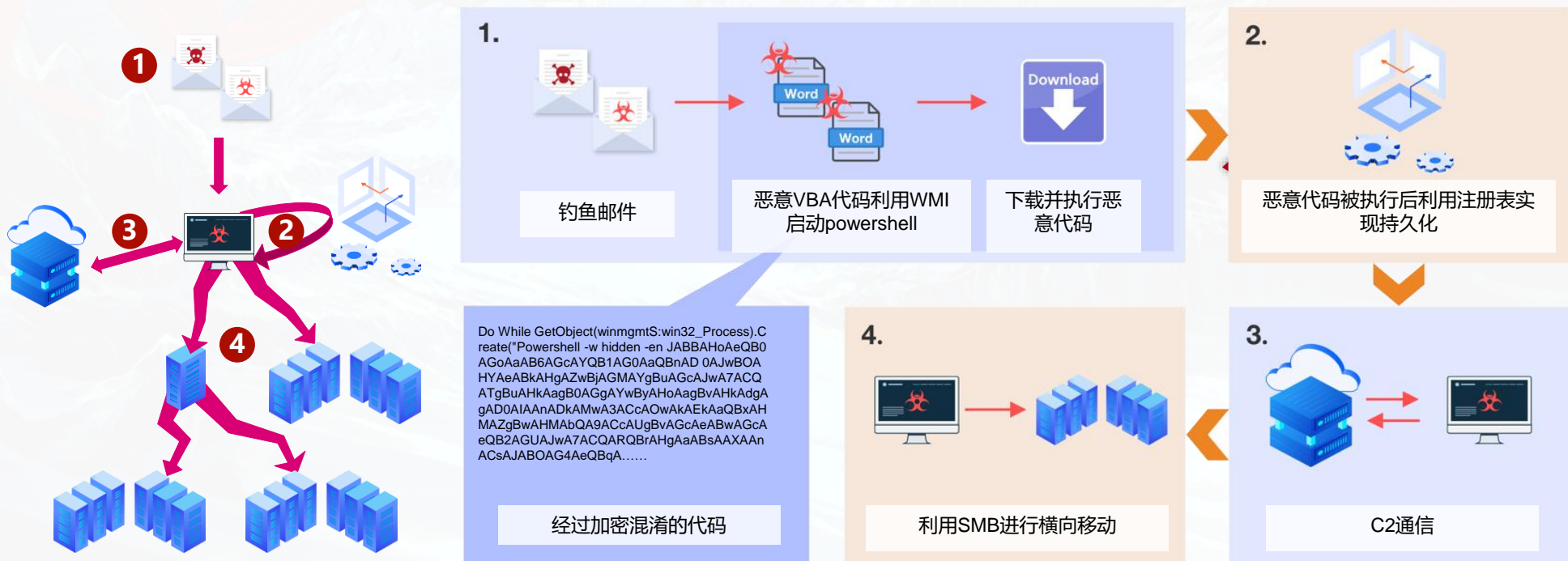
03

安天SOAR案例

案例一内网Emotet传播事件：攻击过程还原

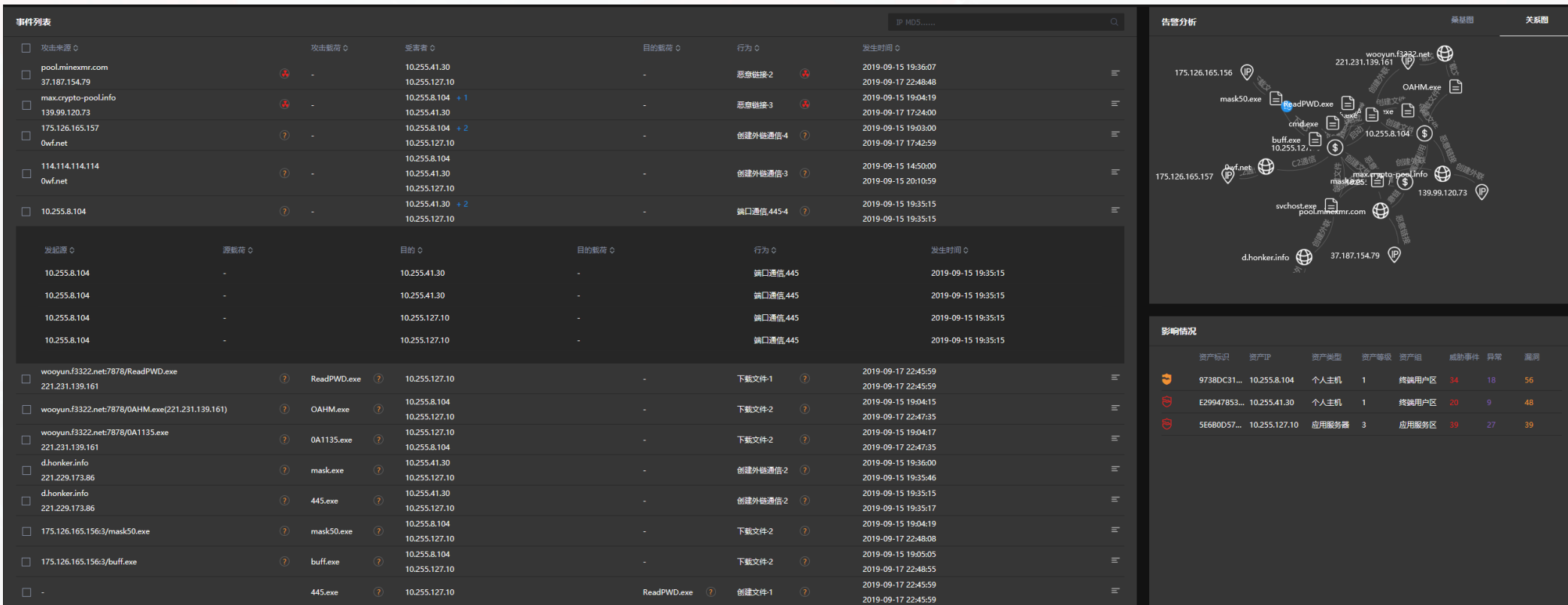


态势感知系统发现网域内突然出现大量的445端口请求，并伴有大量的使用自签证书的SSL通信，经专业应急响应人员排查后发现这是一起利用COVID-19为诱饵分发钓鱼邮件传播Emotet恶意代码的安全事件



来源《利用疫情传播Emotet银行木马攻击事件梳理与分析》

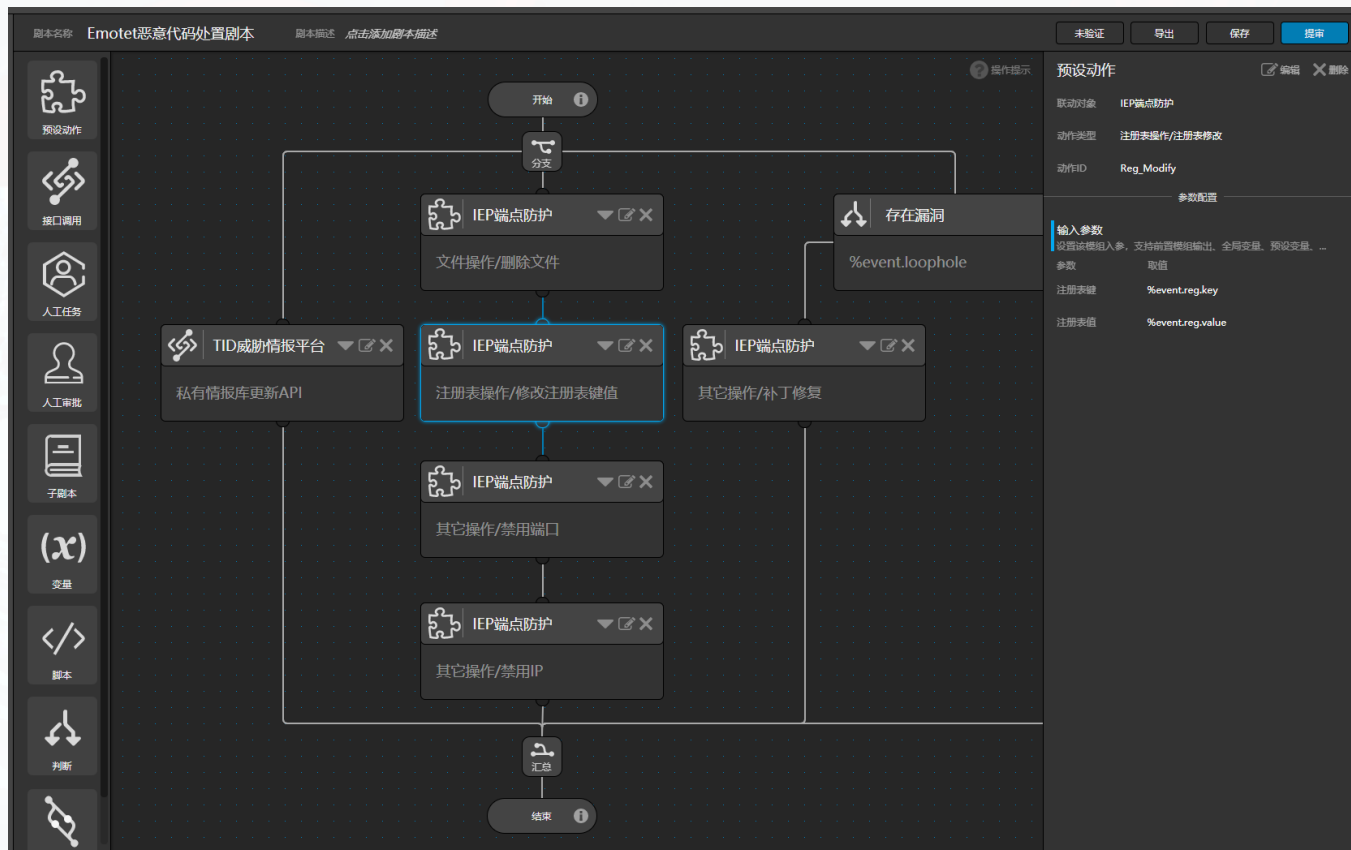
案例一内网Emotet传播事件：态势感知系统威胁告警



案例一内网Emotet传播事件：处置流程的精细化编排



- 根据自动分析的结果，匹配处置剧本。
- 为尽可能复原威胁行为造成的影响，在原有剧本基础上，根据该恶意代码的行为，针对性调整。
- 将IoC等信息更新至威胁情报平台，用于后续内部相关事件的精准发现。

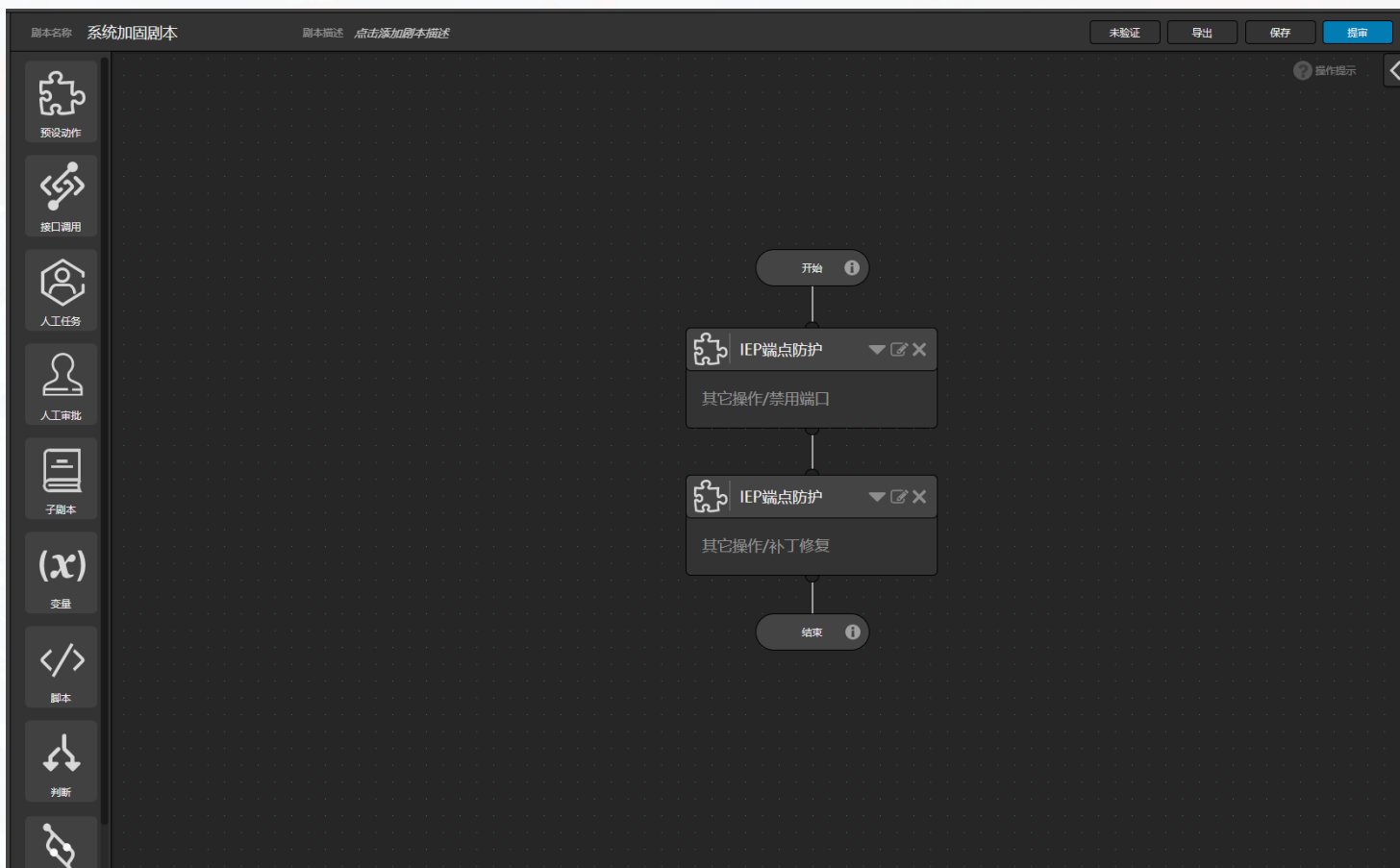


案例一内网Emotet传播事件：处置流程的精细化编排



为了实现系统的安全运营，不仅要
对已感染主机进行恶意代码清除，
也需要对其他未受影响的终端采
取缓解、加固等预防性措施

- 对涉事资产及关联资产，封禁445端口
- 为网内存在此漏洞的资产更新漏洞补丁



案例一内网Emotet传播事件：处置脚本编辑器



- 提供细粒度可视化处置脚本编辑器
- 基于终端管控软件提供的处置操作原语编写处置脚本
- 提供注册表(4)、计划任务(3)、文件(4)、进程(4)、脚本(5)、其他(5+)等共25+种操作原语

```
1 // emotet威胁处置脚本
2 {
3     "name":"emotet威胁处置",
4     "actions":[
5         {
6             "action":"File_Delete",
7             "filenames":["C:\\Windows\\SysWOW64\\f9jwqSbS.exe"],
8             "condition":""
9         },
10        {
11            "action":"Reg_Modify",
12            "path":"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",
13            "key":"@",
14            "value":""
15        },
16        {
17            "action":"Other_Disabled_Port",
18            "port":[445,3309]
19        },
20        {
21            "action":"Other_Fix_patch",
22            "kbname":["ms17-010"]
23        },
24        {
25            "action":"Other_Disabled_Ip",
26            "ips":["103.12.133.7","https://inovatips.com/9yorcan/wb fkk/"]
27        }
28    ]
29 }
```

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SOAR提供ARR编辑器，并可以在部分场景中自动生成处置脚本供网管审核。

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]

案例一内网Emotet传播事件：生成处置包



- 审批通过后系统自动生成处置脚本
- 根据编写者ID和私钥采用国密算法签名，并提交审核和永久留存，以降低处置能力被滥用风险。
- 派发处置包至验证设备进行功能测试并校验
- 按照可定义分发策略将处置包派发至相关设备，并将操作记录留存

```
},
{
  "action": "Reg_Modify",
  "path": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",
  "key": "@",
  "value": ""
},
{
  "action": "Other_Disabled_Port",
  "port": [445, 3309]
},
{
  "action": "Other_Fix_patch",
  "kbname": ["ms17-010"]
},
{
  "action": "Other_Disabled_Ip",
  "ips": ["103.12.133.7", "https://inovatips.com/9yorcan/wbfbk/"]
}
]
}

-----BEGIN SIGNATURE SIGNATURE-----
iQEzBAEBCAAdFj...3lDRgACgkQL7dAkK3U
CCA0CAgA1JVYk...:FD1R4LrQxkS8KNH+i+
d//5V8s+TSqKh...:LsjYfyNUT95C2gH0Un
kwUjluKRThiM/...:dCvspYF6/Go50FkLTA
1m0/Y+1AARJ7c...:tFGjDR18Lz2gs9DzBw
rT9AKvhDMSsdT...:m0Czjm0F+vycqRFsss
v8thLRmduEK1m...
=UHSv
-----END SIGNATURE SIGNATURE-----
```

案例二 CVE-2019-11043漏洞告警



安天铸岳资产管理平台通过漏扫发现业务服务器存在CVE-2019-11043漏洞，系统自动关联了存在相同漏洞的另外三台服务器，同时丰富了漏洞知识信息。

发现4台资产存在高危漏洞:php-fpm远程代码执行漏洞 (CVE-2019-11043)

漏洞类型: 软件漏洞 漏洞分类: 远程代码执行漏洞 首次发现: 2019-10-23 19:30:30 事件来源: 集中安全运维系统

漏洞信息

漏洞名称: php-fpm远程代码执行漏洞
漏洞类型: 软件漏洞
漏洞分类: 远程代码执行漏洞
CVSS2.0评分: 7.5
CVSS3.0评分: 9.8
漏洞分类: 7.5
CVE编号: CVE-2019-11043
CNVD编号: CNVD-2019-36855
CNNVD编号: CNNVD-201910-1456

漏洞介绍
Nginx与php-fpm服务器上存在远程代码执行漏洞，由于Nginx的fastcgi_split_path_info模块在处理非300的请求时，对路径符'in'处理不当使得PATH_INFO值为空，从而导致php-fpm组件在处理PATH_INFO时存在漏洞，攻击者通过精心的构造和利用，可以导致远程代码执行。

厂商
PHP

解决方案
1.PHP官方已于10月12号发布补丁，详情参考链接，建议受影响用户升级进行修复。2.检查nginx配置，如果存在以下易受攻击配置，建议删除：
fastcgi_split_path_info ^(.*\\.php)(/)?\$;
fastcgi_param PATH_INFO \$fastcgi_path_info;
参考链接: https://bugs.php.net/patch-display.php?bug_id=78599&patch=0001-Fix-bug-78599-env_path_info-underflow-can-lead-to-RC.patch&revision=latest

影响版本
PHP 7.0
PHP 7.1
PHP 7.2
PHP 7.3

参考链接
<https://bugs.php.net/bug.php?id=78599>
<https://lab.wallarm.com/php-remote-code-execution-0-day-discovered-in-real-world-ctf-execrise/>
<https://github.com/heeex/phaup-fpizdam>

漏洞信息发布时间: 2019-09-23 09:54:08
漏洞信息更新时间: 2019-09-23 09:54:08

资产清单

网络类型	资产类型	设备名称	使用人	IP地址	部署位置	部门	资产归属	所属区域	资产组	漏洞发现时间	漏洞修复时间	处置状态
办公网	计算设备-办公...			10.255.						2020-11-1 13:00:31	-	待处理
办公网	计算设备-办公...			10.255.						2020-11-1 13:00:17	-	待处理
办公网	计算设备-办公...			10.255.						2020-11-1 12:59:41	-	待处理
办公网	计算设备-办公...			10.255.						2020-11-1 12:59:21	-	待处理

共50条 20条/页 < 1 2 3 4 5 > 前往 5 页

案例二 CVE-2019-11043漏洞处置



脚本名称 漏洞CVE-2019-11043缓解措施 脚本描述 点击添加脚本描述

未验证 导出 保存 投审

操作提示

预设动作 编辑 删除

联动对象 IEP端点防护

动作类型 文件操作/编辑文件

动作ID File_Modify

参数配置

输入参数 设置该模块输入参数，支持前置模板输出、全局变量、预设变量、...

参数 取值

处理对象 全部 指定路径

文件 /etc/nginx/modsec/main.conf

修改命令

```
SecRule REQUEST_URI "@rx %0(a|A|d|D)" \
  \"id:1,phase:1,t:lowercase,deny\"
```

开始

IEP端点防护

文件操作/编辑文件

IEP端点防护

脚本/执行命令
-Nginx reload

结束

- 根据资产所属业务属性选择缓解措施
- 根据安天的补丁库、漏洞信息库生成缓解脚本
- 修改Nginx配置文件增加

```
SecRule REQUEST_URI "@rx %0(a|A|d|D)" \
  \"id:1,phase:1,t:lowercase,deny
```
- 重载Nginx

```
reload Nginx
```


智者安天下

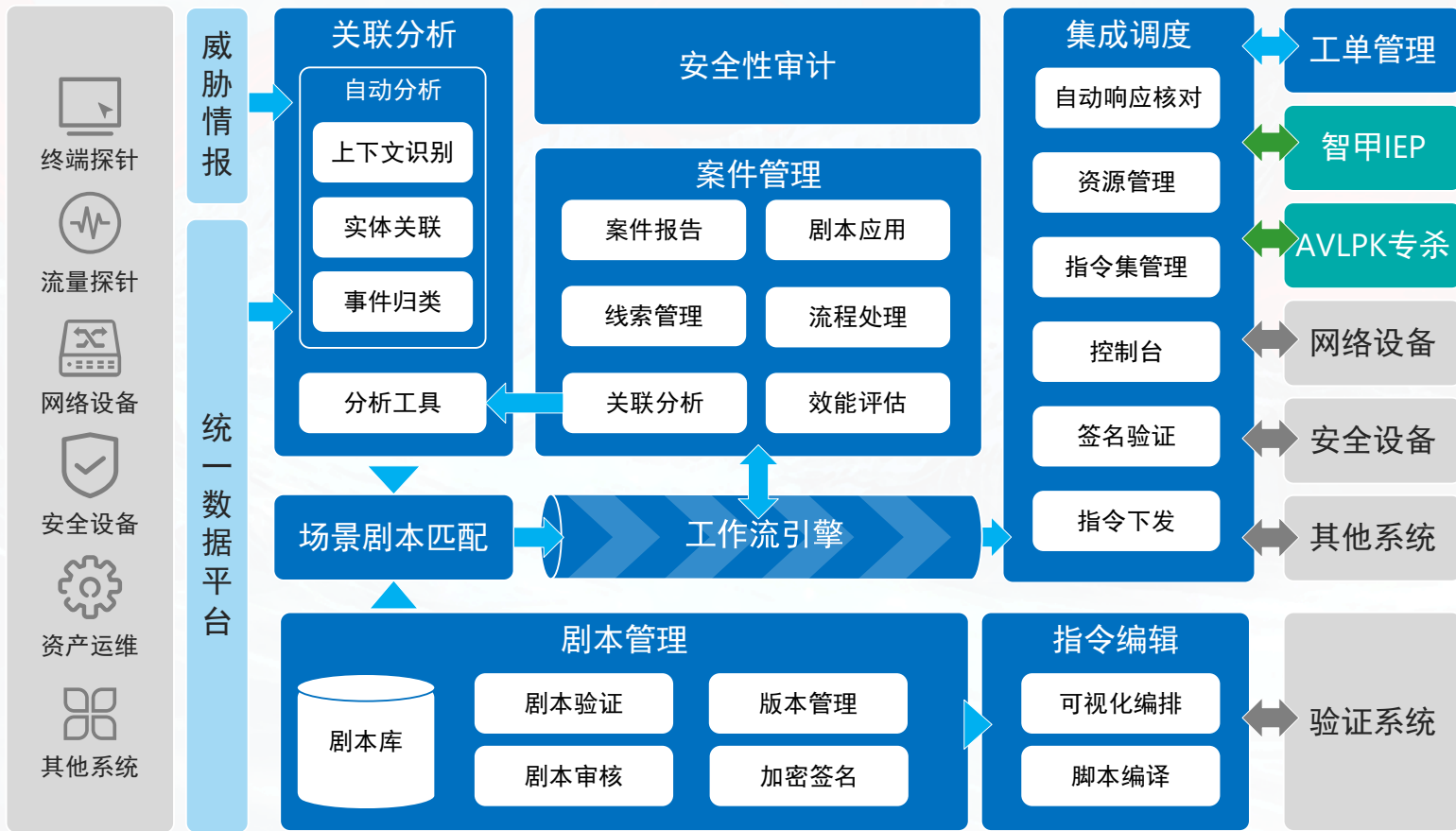


长缨待展

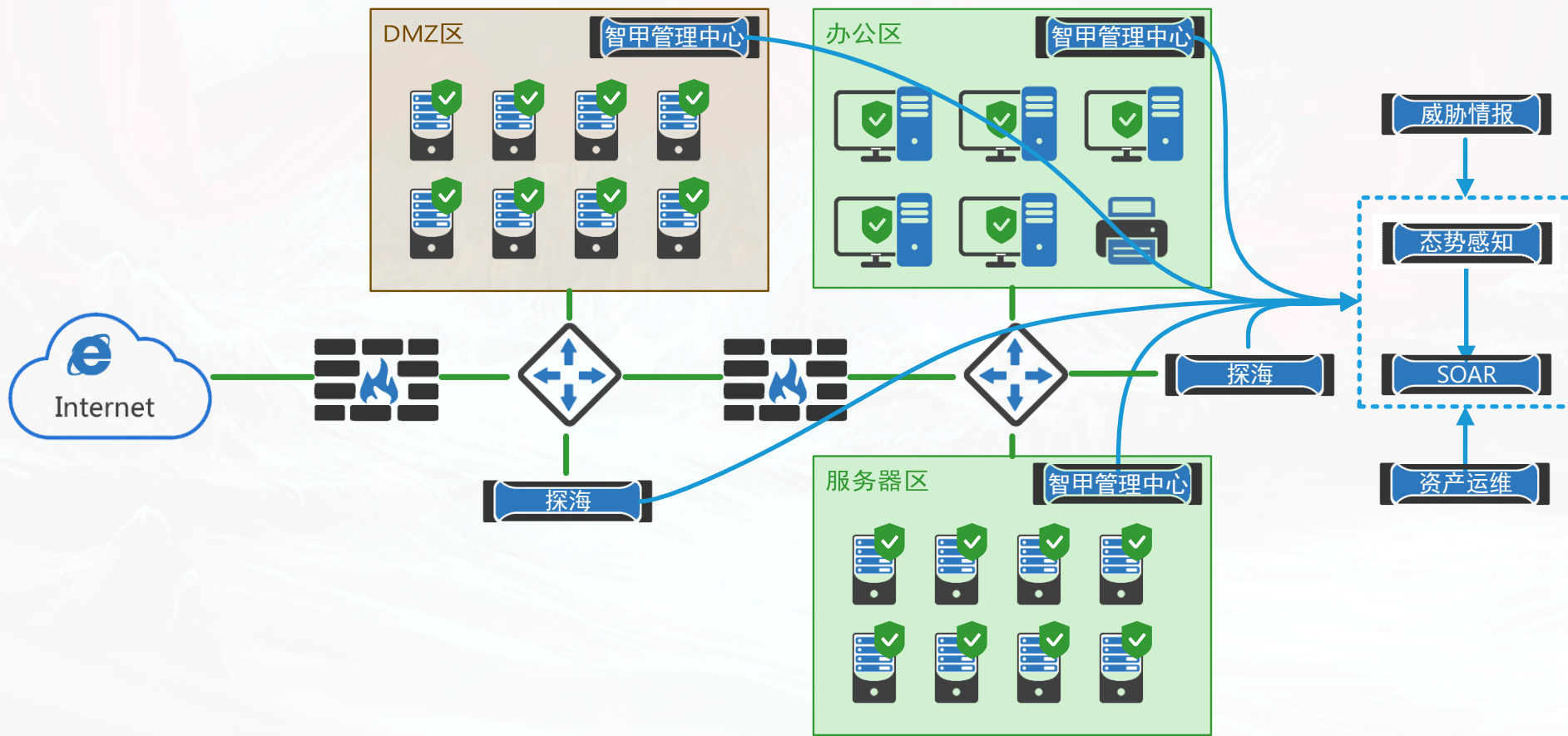
威胁框架：细粒度对抗

04 安天SOAR架构

SOAR功能架构



SOAR部署结构



智者安天下



长缨待展

威胁框架：细粒度对抗

05

安天SOAR特点

安天SOAR的能力



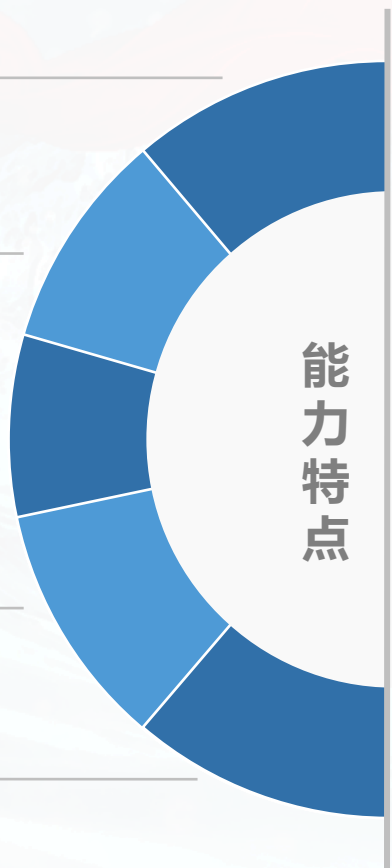
安全能力编排化

自动响应剧本化

脚本编辑可视化

关联分析流程化

响应处置自动化



能力特点

安全运营



效能可评估



效果可验证



能力可演进



操作可追溯

安天SOAR的价值



专业的威胁处置能力



安天SOAR建立在安天智甲终端防护软件提供的细粒度防御处置基础之上，结合安天CERT提供的恶意代码专杀工具为用户提供精细、灵活、高效的威胁处置能力。





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

谢谢大家

长缨缚展

威胁框架：细粒度对抗