



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

打击内部跳板

——传统端点的EDR运维实战

安天 | 端点安全部

CONTENTS

目 录

01

Log4j漏洞在EDR场景的运维实践

02

安全场景化的EDR采集

03

辅助决策的EDR深度检测和精准响应

04

EDR的典型场景应用



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

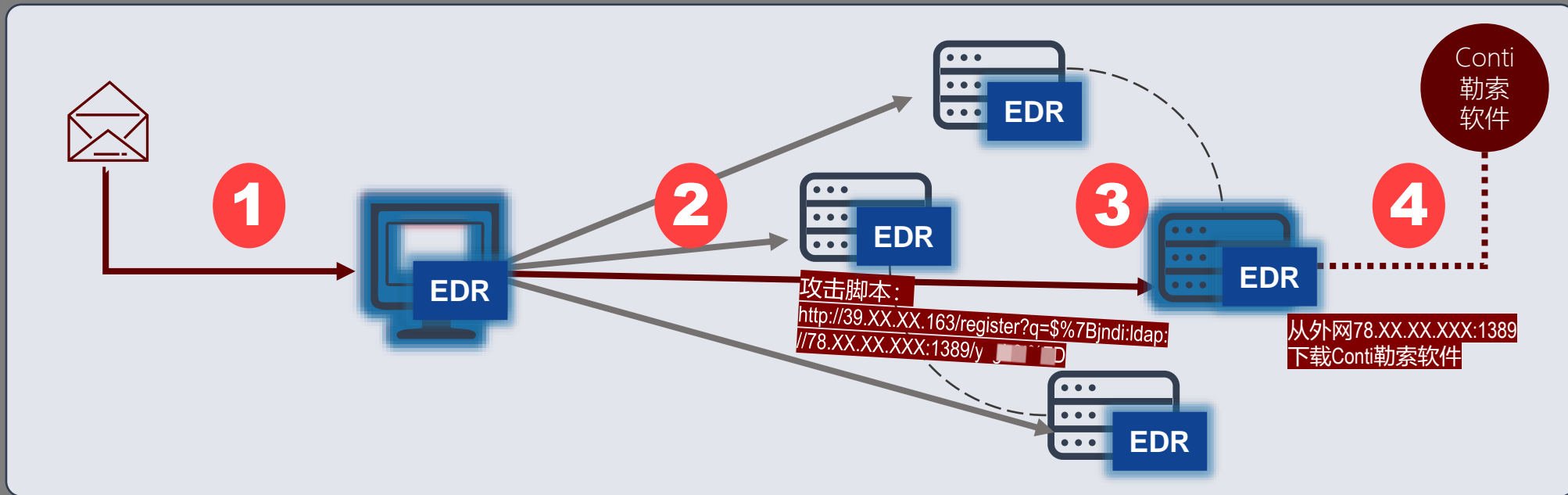
01

Log4j漏洞在EDR场景的 运维实战

Log4j漏洞的攻击场景假定

1 钓鱼邮件附件下载到工作机

2 以工作机为跳板，向内网web服务器发送带有JNDI的GET请求



3 其中一台服务器被漏洞利用成功，通过外网域名下载Conti勒索软件

4 Conti勒索软件本地执行

Log4j漏洞的EDR运维过程

告警

管理员察觉PC终端和Web服务器产生告警信息。

调查

管理员对告警展开调查，发现PC终端进程行为中，存在大量IP地址，URL中包含参数，进一步比对PC终端和Web服务器终端的IP地址。

响应

管理员全网检索匹配内容，对PC断网隔离，阻断进程，对Web服务器上带有log4j参数进程阻断执行并进行安全加固。

告警详情

告警概览

告警等级	发现时间	告警对象	告警描述
3	2022-01-10 15:33:40	eee876886f190a38455778634a35a1d975414e83f225f11e3e792706301fe	发现病毒文件,病毒名称Trojan; 病毒存在勒索行为.....
告警来源	检测规则	状态	
主动防御	云查杀引擎检测	已阻止	

终端信息

终端名称	IP	分组	操作账号
Web服务器-北机房	78	运维组	

文件详情

文件名:	eee876886f190a38455778634a35a1d975414e83f225f11e3e792706301fe	行为类型:	勒索病毒(Trojan[Ransom]Win32.Conti.mak)
路径:	C:\Program Files (x86)\jdk-11.0.1\bin	文件大小:	101KB
数字签名:	/	父进程:	java.exe
发现时间:	2022-01-10 15:43:10	上报时间:	2022-01-10 15:43:10
Att&CK标 签:	T1486		
MD5:	04029E121A0CFA5991749937DD22A1D9		
sha1	07a21675a8f19518d3b050e1W06a21de1da6c07		
sha256:	ee06f9724af41b130tacea13353069129e98450230fe9f632d53d50bb0a0703c		

告警行为

序号	详情	处理状态
----	----	------

告警详情

告警概览

告警等级	发现时间	告警对象	告警描述
3	2022-01-10 15:33:40	Technology\PromotionReview.docx.exe	发现网络嗅探
告警来源	检测规则	状态	
行为检测	网络嗅探规则	已告警	

终端信息

终端名称	IP	分组	操作账号
WIN-DAKEQI	10.	研发组	Administrator

文件详情

文件名:	Technology\PromotionReview.docx.exe	行为类型:	网络嗅探
路径:	C:\Users\xxxx\Desktop\Technology\PromotionReview.docx.exe	文件大小:	25KB
数字签名:	/	父进程:	C:\Windows\explorer.exe
发现时间:	2022-01-10 15:33:40	上报时间:	2022-01-10 15:33:40
Att&CK标 签:	T1595		
MD5:	04029E121A0CFA5991749937DD22A1D9		
sha1	F43D96B316E30AE1A3494AC580624F68EA1BF054		
sha256:	9F914D4270FE216501044ACD85A32D58AAEF1419D404FDDFA5D3E48F66CCD9F		

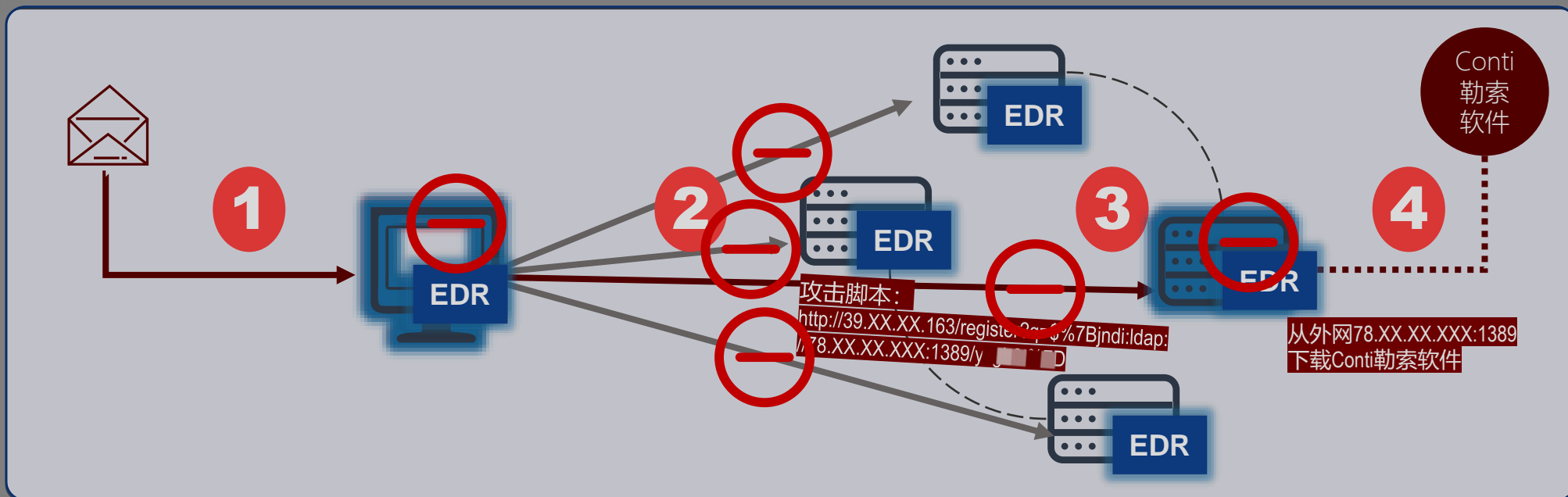
告警行为

序号	详情	处理状态
----	----	------

Log4j漏洞的EDR运维过程

1 钓鱼邮件附件下载到PC

2 以终端为跳板扫描内网web服务器，扫描存在log4j漏洞的服务器



3 漏洞利用成功，连接C2服务器
下载Conti勒索软件

4 Conti勒索软件本地执行

Log4j漏洞的EDR运维过程

告警

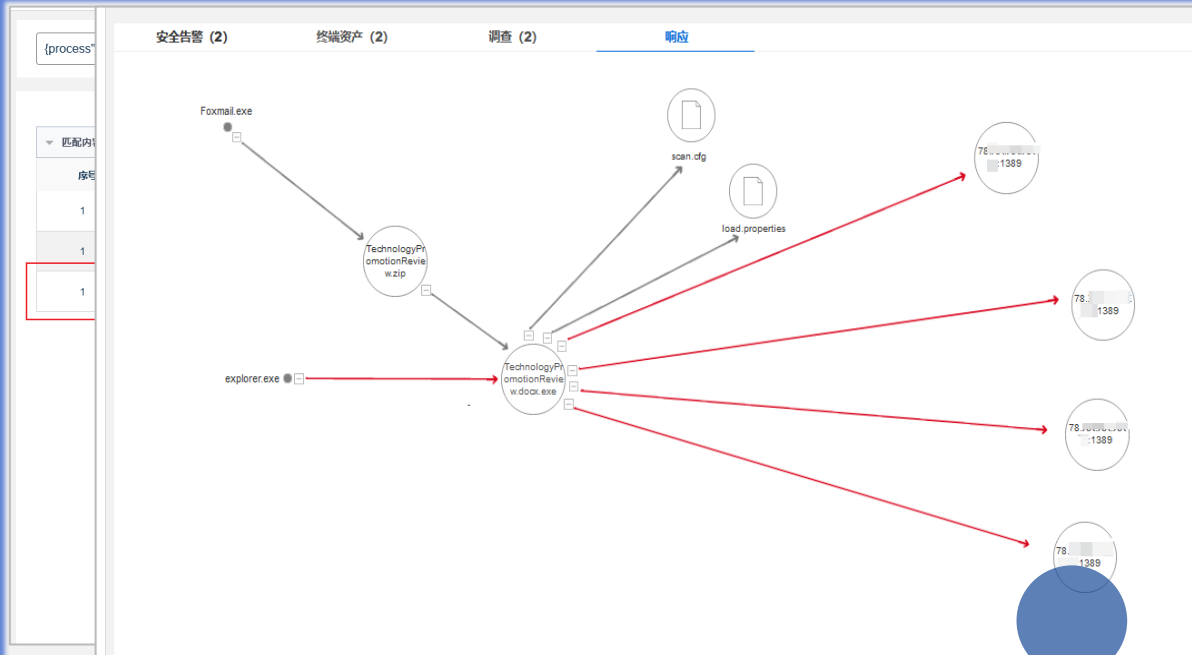
管理员察觉PC终端和Web服务器产生告警信息。

调查

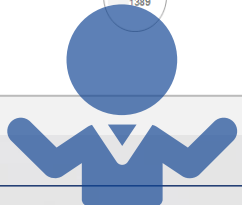
管理员对告警展开调查，发现PC终端进程行为中，存在大量IP地址，URL中包含参数，进一步比对PC终端和Web服务器终端的IP地址。

响应

管理员全网检索匹配内容，对PC断网隔离，阻断进程，对Web服务器上带有log4j参数进程阻断执行并进行安全加固。

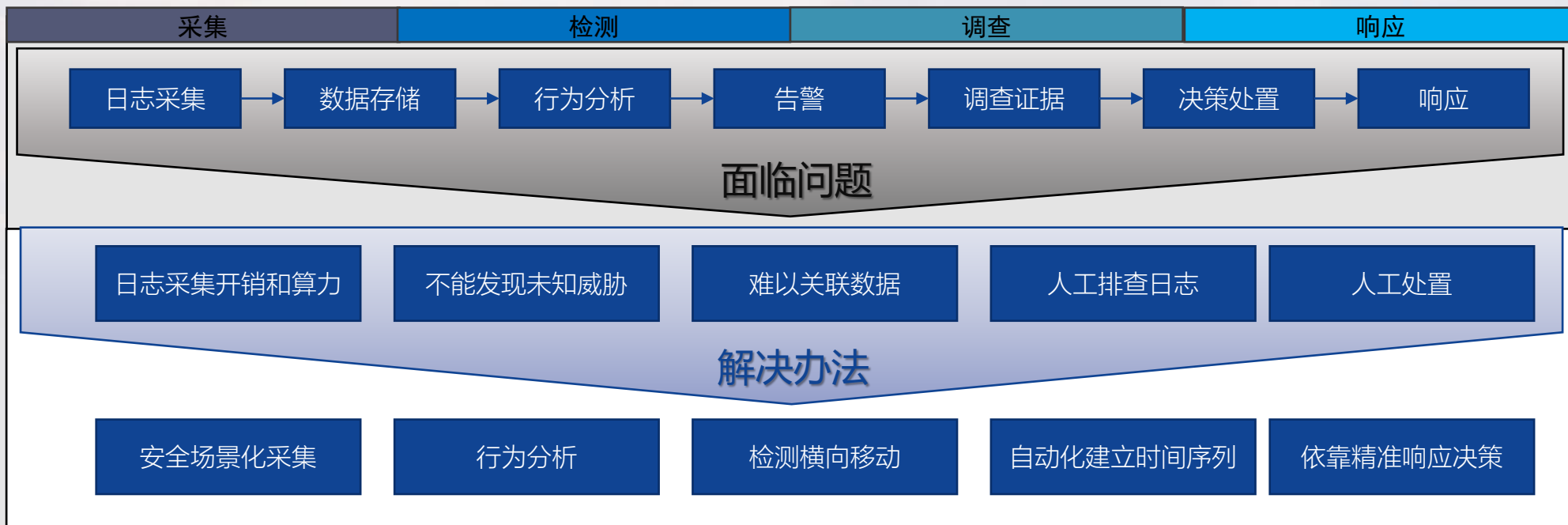


```
1 function check()
2   local bRet = CFile:IsFileExist("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") -- 判断文件是否存在
3   if bRet then
4     local bRet = CProcess:IsProcessExist
5     if bRet then
6       local nFaildCount, nKillCount = CProcess:KillProcess
7       if bRet then
8         local nFaildCount, nKillCount = CProcess:KillProcess
9         sPath("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") -- 结束进程
10        print('结束进程成功数量:', nKillCount)
11        print('结束进程失败数量:', nFaildCount)
12      end
13    end
14  end
15  if CFile:IsFileExist("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") then -- 判断文件是否存在
16    if CFile:FileDelete("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") then -- 删除文件
17      print("TechnologyPromotionReview.docx.exe 文件删除成功!")
18    end
19  end
20  if CFile:IsFileExist("%CSIDL_WINDOWS%\TechnologyPromotionReview.zip") then -- 判断文件是否存在
21    if CFile:FileDelete("%CSIDL_WINDOWS%\TechnologyPromotionReview.zip") then -- 删除文件
22      print("TechnologyPromotionReview.zip 文件删除成功!")
23    end
24  end
25  if CFile:IsFileExist("%CSIDL_WINDOWS%\qsdjyh3243ffg.exe") then -- 判断文件是否存在
26    if CFile:FileDelete("%CSIDL_WINDOWS%\qsdjyh3243ffg.exe") then -- 删除文件
27      print("qsdjyh3243ffg.exe 文件删除成功!")
28    end
29  end
30  if CFile:IsFileExist("%CSIDL_WINDOWS%\gssgdjyjhfgs.exe") then -- 判断文件是否存在
31    if CFile:FileDelete("%CSIDL_WINDOWS%\gssgdjyjhfgs.exe") then -- 删除文件
32      print("gssgdjyjhfgs.exe 文件删除成功!")
33    end
34  end
35  -- 添加防火墙拦截规则
36  Firewall:AddRule('block', 'http://.*/register?q=%$7Bjndi:ldap:')
37  end
38  end
39  end
40  end
41  end
42  end
43  check() -- 执行检测函数
```



再问EDR

- 海量端点治理本身就是重大漏洞和关联分析响应的一部分，无论传统端点是否存在这个漏洞，它都与治理关联。
- 原有的单机主防加病毒引擎检测，只能构成威胁的识别和阻断的基础，还需要更多的上下文环境、多点间的相关数据关联形成上层的判断决策；
- 单纯以保护对象为中心的视角场景覆盖不足，从打击内部攻击跳板的角度，对出站流量的攻击识别同样重要。



安全场景化采集

采集PC端点和Web服务器的进程、网络、文件等系统行为



自动关联分析

通过工作机和Web服务器的IP进行事件关联

精准溯源和响应

通过告警信息，层层抽丝剥茧，调查威胁调用链，快速掌握攻击者攻击手段，并精准溯源和响应

深度调查

了解了安全事件的上下文及相关主机的账号、进程、软件等信息



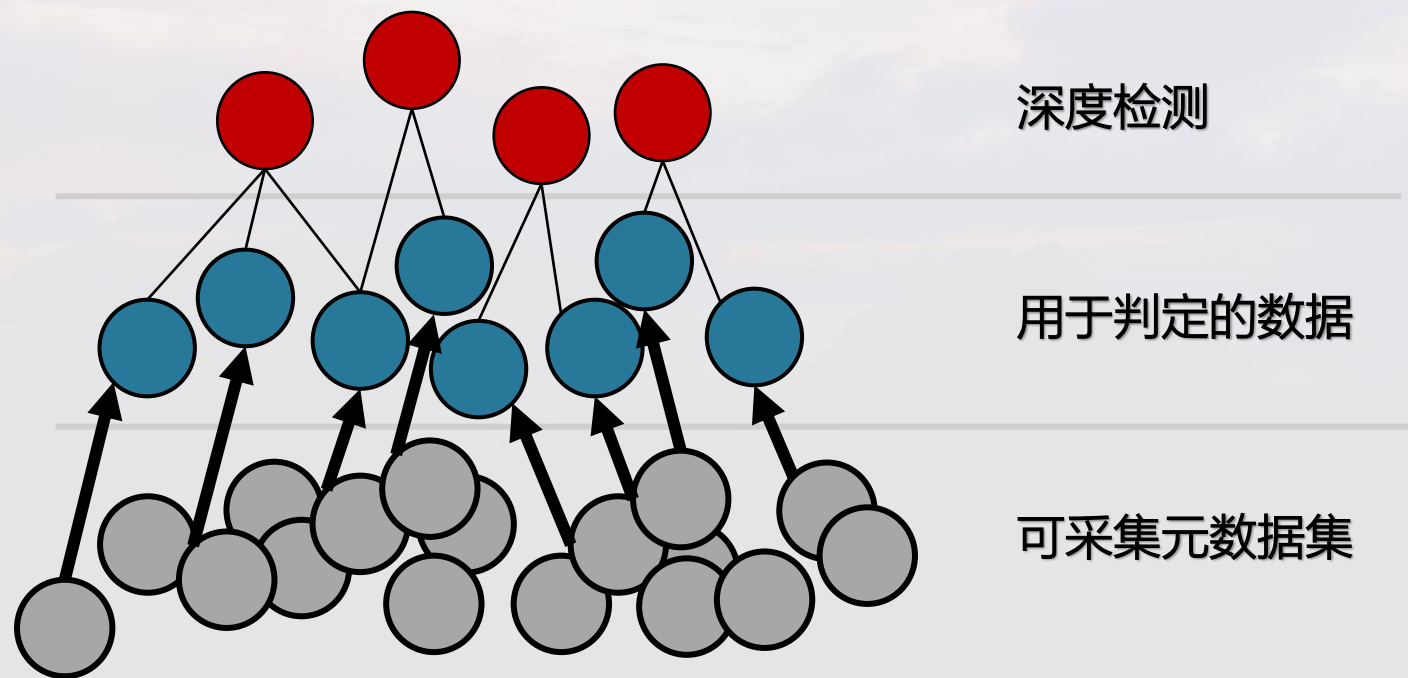
网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

02 安全场景化的EDR采集

采集数据支撑深度检测

- EDR的工作对象不是特征码，是基于主机场景的元数据化采集；
- 端点的元数据是海量的分散的，端点的算力是有限的
- 深度检测只需要一部分线索来进行判定



基于安全场景的数据采集方案

	01 资产清点场景	02 安全策略场景	03 威胁检测场景	04 风险检测场景
采集目的	资产数据清晰化 提供终端调查线索	配置核查 关键变更通知 关键配置展示	漏洞扫描 威胁检测 主动防御	风险检查 行为分析 异常检测
采集内容	硬件信息 软件信息 移动介质	系统服务 组策略 开机启动项 计划任务	补丁信息 文件信息 进程启动信息 病毒扫描信息	终端日志 用户登陆信息 网络数据
采集方式	遍历 系统API调用	系统API调用 三层hook	遍历 驱动感知	API调用 终端防火墙
采集频率	周期性采集	周期性采集 变更实时采集	实时采集	实时采集

智甲EDR的采集特色

侦察 (10)	资源开发 (7)	初始访问 (9)	执行 (12)	持久化 (19)	提权 (10)	防御规避 (40)	凭证访问 (15)	发现 (20)	横向移动 (9)	收集 (17)	命令与控制	数据导出 (9)	影响 (13)
主动扫描	获取基础设施	水坑攻击	利用命令和脚本	模拟用户	滥用提升控制权限	滥用提升控制权限	暴力破解	发现用户	利用进程服务	生成加密收集的数据	使用应用程序	自动导出数据	删除帐户权限
搜集受害者主机信息	入侵帐户	利用面向公众的应用程序	利用容器管理器	利用Git服务	操纵访问令牌	操纵访问令牌	从存储密码的位置获取凭证	发现应用程序窗口	发现注册表	通过可移动介质通信	限制传输数据大小	限制传输数据大小	窃取数据
搜集受害者身份信息	入侵基础设施	利用外部远程服务	部署容器	利用自动化工具	利用自动化工具	利用自动化工具	利用凭证访问漏洞	发现远程系统	发现进程系统	执行内部命令式攻击	使用非C2协议回传	使用非C2协议回传	造成系统影响的数据加密
搜集受害者网络信息	能力开发	利用主机软件漏洞	利用主机软件漏洞	利用初始化工具	在主机上建立映像	在主机上建立映像	强制认证	发现浏览器书签	发现软件	远程服务器会话劫持	使用物理后门回传	使用物理后门回传	篡改数据
搜集受害者组织信息	建立帐户	添加硬件	利用进程间通信	添加浏览器扩展	创建修改操作系统	创建修改操作系统	伪造Web凭证	发现系统信息	发现系统信息	收集野贴数据	收集野贴数据	收集野贴数据	篡改数据
通过网络钓鱼收集信息	能力获取	网络钓鱼	利用API	篡改客户端软件	部署容器	部署容器	输入凭证	发现系统地理位置	发现系统地理位置	收集云存储对象的数据	收集云存储对象的数据	收集云存储对象的数据	篡改数据
从第三方开源渠道获取信息	环境查看	通过可移动介质	利用计划任务工作	事件触发执行	直接访问卷	直接访问卷	利用中间人攻击 (MITM)	发现系统网络配置	发现系统网络配置	通过可移动介质复制	收集信息库数据	收集信息库数据	篡改数据
搜集公开网站域库信息	入侵供应链	入侵供应链	利用共享模块执行	利用漏洞提权	执行范围保护	执行范围保护	修改身份验证过程	发现系统网络配置	发现系统网络配置	收集本地系统数据	收集本地系统数据	收集本地系统数据	篡改数据
搜集公开网站域信息	利用有效帐户	利用有效帐户	利用第三方软件部署工具	事件触发执行	网络策略修改	网络策略修改	网络嗅探	发现文件和目录	发现文件和目录	收集网络共享数据	收集网络共享数据	收集网络共享数据	篡改数据
搜集受害者自有网站	利用有效帐户	利用有效帐户	利用外部远程服务	执行进程劫持	进程注入	进程注入	窃取应用程序访问令牌	发现网络共享	发现网络共享	使用非标准端口	使用非标准端口	使用非标准端口	篡改数据
			指导用户执行	执行进程劫持	利用计划任务工作	利用计划任务工作	窃取凭证	网络嗅探	网络嗅探	数据留存	数据留存	数据留存	篡改数据
			利用Windows管理规范 (WMI)	植入容器镜像	修改身份验证过程	修改身份验证过程	窃取Web会话Cookie	发现密码策略	发现密码策略	收集电子邮件	收集电子邮件	收集电子邮件	篡改数据
			利用有效帐户	启动Office应用程序	删除主机中的信标	删除主机中的信标	双因子认证拦截	发现主机接入设备	发现主机接入设备	输入捕捉	输入捕捉	输入捕捉	篡改数据
				在操作系统前启动	网络执行命令	网络执行命令	不安全的凭证	发现策略组	发现策略组	浏览器中间人攻击 (MitM)	浏览器中间人攻击 (MitM)	浏览器中间人攻击 (MitM)	篡改数据
				利用计划任务工作	伪装	伪装				发现云存储对象	发现云存储对象	发现云存储对象	篡改数据
				利用服务器软件组件	修改身份验证过程	修改身份验证过程				发现中间人攻击 (MitM)	发现中间人攻击 (MitM)	发现中间人攻击 (MitM)	篡改数据
				使用流量指令	修改云计算基础设施	修改云计算基础设施				发现中间人攻击 (MitM)	发现中间人攻击 (MitM)	发现中间人攻击 (MitM)	篡改数据
				修改注册表	利用有效帐户	利用有效帐户				发现策略组	发现策略组	发现策略组	篡改数据
					利用有效帐户	利用有效帐户				发现策略组	发现策略组	发现策略组	篡改数据

- ### 可作为攻击事件的回溯依据
- 更全面的记录端点环境变更历史，包括文件新增情况、进程行为、注册表变化等，提供溯源依据；
 - 通过将攻击事件中使用的攻击技术映射到 ATT&CK，更好的理解对手的攻击方式。

- ### 聚焦更重要的数据
- 针对攻击手段可能留下的数据痕迹，例如用户登录记录、外设文件使用记录等，进行专项采集；
 - 针对系统组件被恶意利用，如Regsvr32.exe、PowerShell调用等，加强数据采集。

息的提取，无法获取系统级、驱动层的信息，但往往这些数据才是支撑分析和画像最重要的依据。



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

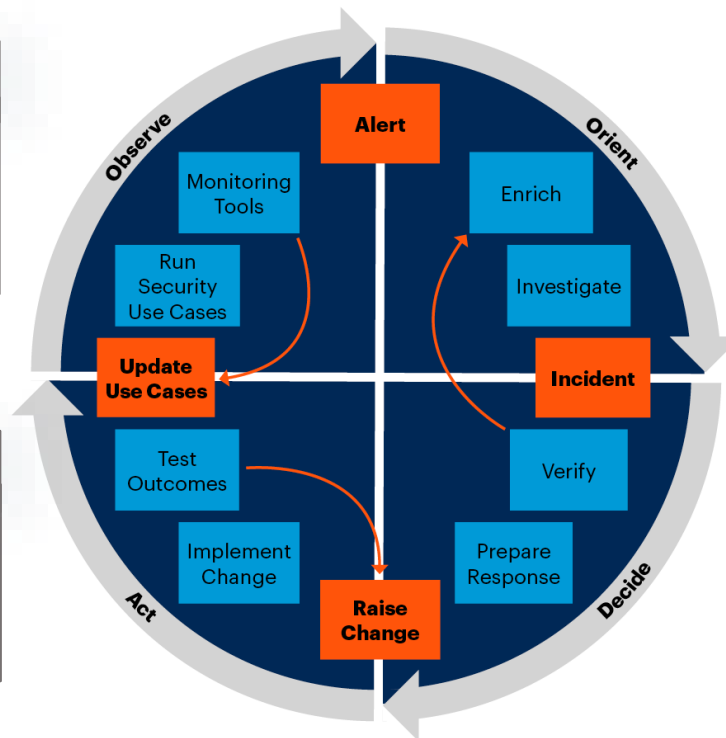
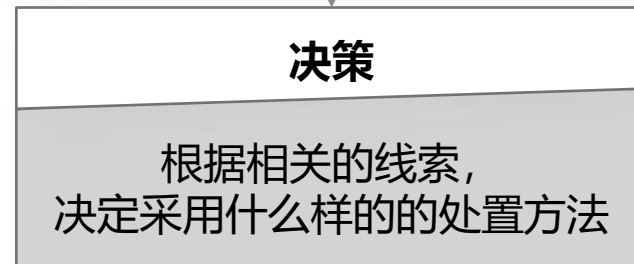
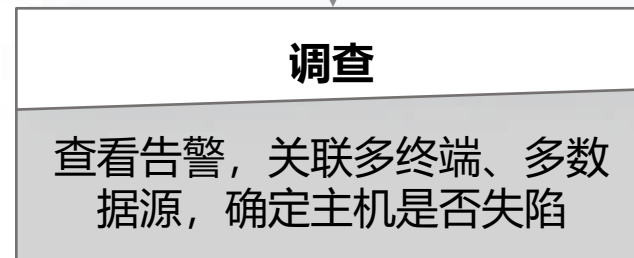
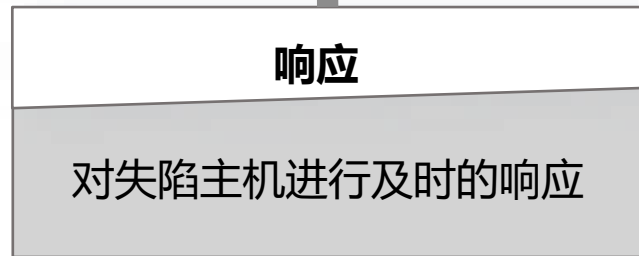
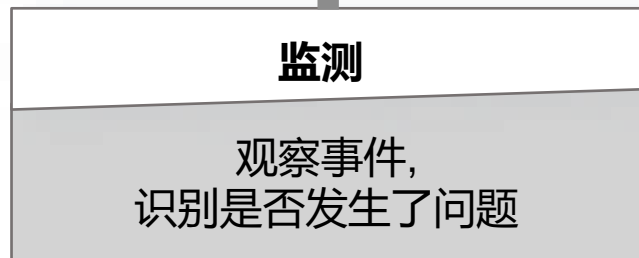
安天 | 智者安天下

03

辅助决策的EDR深度检测 和精准响应

安全运维人员决策过程

SOC Detection Process Flow



Source: Gartner
719029_C

<https://www.gartner.com/document/3997133?ref=solrImgSearch&refval=311966345> Gartner.

安全运维人员决策过程——监测

- 只有1%的事件才会形成告警，要提高告警的准确度，减少安全人员的运维精力；
- 提供一个基于安全场景的变化关系，时间窗口内上下文数据以及多点间的数据分布为基础的告警内容，以进行更深度的判断和预测

管理员使用EDR更好监测威胁

应用上下文

完整的取证时间线

多点数据关联

威胁可视化

高质量的威胁情报
信息

机器学习模型

用户行为分析

集中呈现

管理员缺乏全局可见性

系统应用日志

安全资产数据

主机性能数据

用户行为数据

系统配置数据

安全运维人员决策过程——监测

- 日志对安全事件定位、安全策略实施状况的评估都是必不可少的证据。
- 日志数据是异构的，排查难度较大，重复劳动多。
- EDR应对端点日志的告警，有明确的统一的结构化的告警格式、告警等级；



快速查找名称或IP

< 返回

人工响应 分类设置 查看配置 禁用 删除 导出

搜索内容

<input type="checkbox"/>	详情	发现时间	事件状态	等级	事件描述	响应状态	重要程度
<input type="checkbox"/>	▶	2022-01-09 09:20:10	异常	2	监控到ningo-PC(10...)产生告警, 描述: 主文件表(MFT)包含损坏的文件记录	未响应	一般
<input type="checkbox"/>	▶	2022-01-09 09:15:32	异常	4	监控到DES-Server(10...)产生告警, 描述: 数据库身份验证失败	未响应	重要
<input checked="" type="checkbox"/>	▼	2022-01-10 15:45:10	异常	5	检测到dakeqi-PC (10...) Windows系统登录失败 -- 未知的用户名或错误密码	未响应	重要

基本信息 关联日志

告警信息

规则ID: 18130 规则分组: 主机异常状态登录 告警等级: 5级

告警描述: Login session opened

异常原因: Logon Failure - Unknown user or bad password

日志类型: Microsoft-Windows-Security-Auditing

日志原文: 2022 Jan 10 15:33:40 WinEvtLog: Security: AUDIT_FAILURE(4625): Microsoft-Windows-Security-Auditing: (Administrator): no domain: dakeqi-PC: An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: dakeqi Account Domain: dakeqi-PC Failure Information: Failure Reason: %%2313 Status: 0xc000006d Sub Status: 0xc000006a Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: DAKEQI Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted

[▶](#) 2022-01-10 15:33:40 异常 5 检测到ZWK-PC (10...) Linux系统ssh登录失败--未知的用户名或错误密码 未响应 重要

安全运维人员决策过程——调查

一个告警事件，
查看两台终端告警详情



<input type="checkbox"/>	等级	发现时间	告警类型	告警对象	告警描述	事件标签	终端名称	终端IP	告警数量	状态
<input type="checkbox"/>	5	2022-01-10 15:43:10	行为告警	eaee076886f19ba384f55778634a35a1d975414e83f22f6111e3e7927705301fe	发现病毒文件,病毒名称Trojan: 病毒存在勒索行为.....	病毒 勒索	Web服务器-北机房	██████████	1	未处理
<input checked="" type="checkbox"/>	3	2022-01-10 15:33:40	网络告警	TechnologyPromotionReview.docx.exe	发现网络嗅探	网络探测	WIN-DAKEQI	██████████	1	未处理

多数据源

入侵检测

沙箱联动

云引擎

ATT&CK映射

威胁情报

日志分析

行为分析

漏洞检测

威胁检测

异常检测

多终端

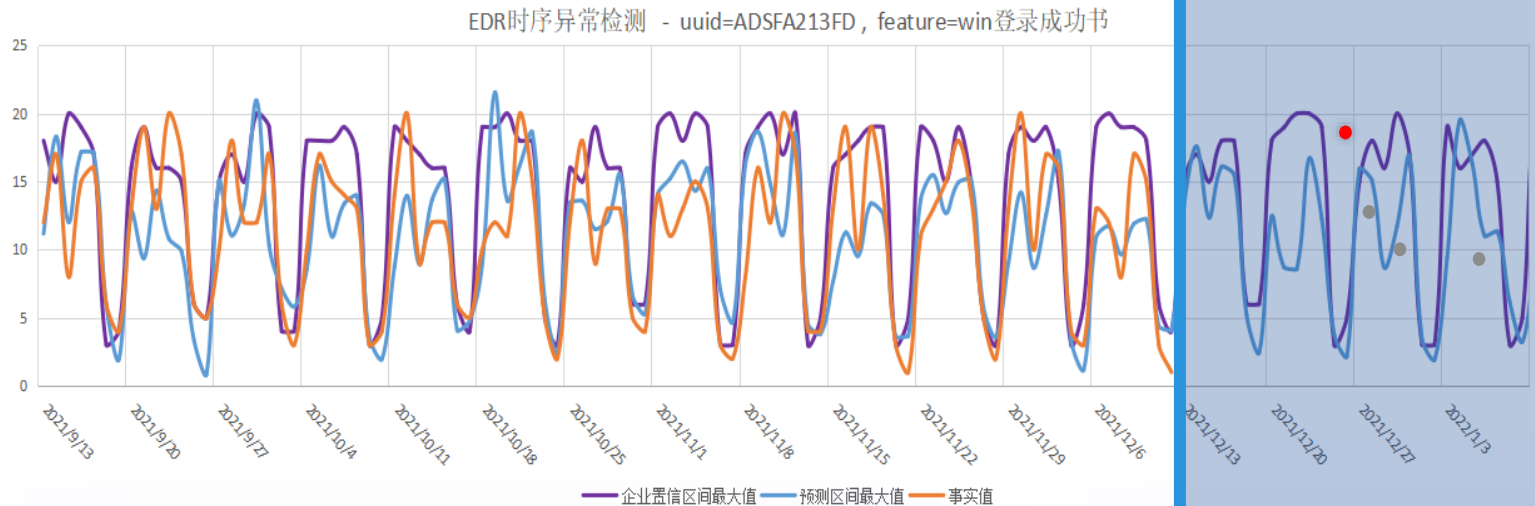
Linux

信创

Win

Mac

安全运维人员决策过程——调查



数据说明:

- 数据: 近3个月的近千台终端用户登录频次数据
- 模型: 通过时序预测模型来建模;
- 异常判定: 当实时累加统计某个终端的登录事实值, 如果同时偏离预测值和整体性值的置信区间, 判定为行为异常。

日常运维监控告警

- 运维人员需要实时监控系统内的行为异常告警。智甲EDR提供了异常检测的能力。

异常检测模型

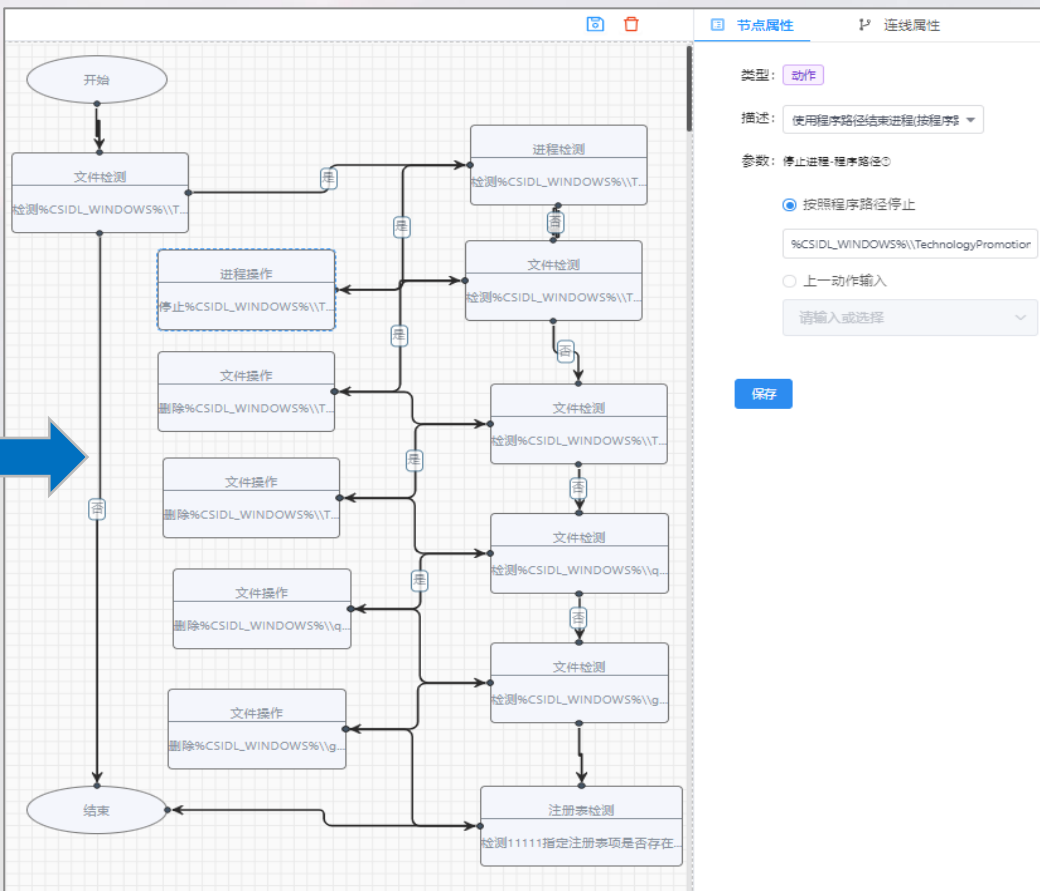
- 异常检测模型: 根据多端点采集的用户历史数据, 通过持续的机器学习模型构建正常的行为基线并持续更新, 自适应发现偏离于基线的异常行为。

安全运维人员决策过程——响应

安天智甲支持细粒度响应动作

```
1 function check()
2   local bRet = CFile:IsFileExist("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") -- 判断文件是否存在
3   if bRet then
4     local bRet = CProcess:IsProcessExis\
5     tByPath("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") -- 判断进程是否存在
6     if bRet then
7       local nFaildCount, nKillCount = CProcess:KillProces\
8       sByPath("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") -- 结束进程
9       print('结束进程成功数量:', nKillCount)
10      print('结束进程失败数量:', nFaildCount)
11    end
12  end
13  if CFile:IsFileExist("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") then -- 判断文件是否存在
14    if CFile:FileDelete("%CSIDL_WINDOWS%\TechnologyPromotionReview.docx.exe") then -- 删除文件
15      print("TechnologyPromotionReview.docx.exe 文件删除成功!")
16    end
17  end
18  end
19  if CFile:IsFileExist("%CSIDL_WINDOWS%\TechnologyPromotionReview.zip") then -- 判断文件是否存在
20    if CFile:FileDelete("%CSIDL_WINDOWS%\TechnologyPromotionReview.zip") then -- 删除文件
21      print("TechnologyPromotionReview.zip 文件删除成功!")
22    end
23  end
24  end
25  if CFile:IsFileExist("%CSIDL_WINDOWS%\qsdjyh3243ffg.exe") then -- 判断文件是否存在
26    if CFile:FileDelete("%CSIDL_WINDOWS%\qsdjyh3243ffg.exe") then -- 删除文件
27      print("qsdjyh3243ffg.exe 文件删除成功!")
28    end
29  end
30  end
31  if CFile:IsFileExist("%CSIDL_WINDOWS%\gssgdfyjhfsgg.exe") then -- 判断文件是否存在
32    if CFile:FileDelete("%CSIDL_WINDOWS%\gssgdfyjhfsgg.exe") then -- 删除文件
33      print("gssgdfyjhfsgg.exe 文件删除成功!")
34    end
35  end
36  end
37  -- 添加防火墙拦截规则
38  Firewall:AddRule('block', 'http://.*/register?q=$%7Bjndi:ldap:')
39  end
40  end
41  end
42  end
43  check() -- 执行检测函数
```

安天智甲支持可视化预编排响应脚本





网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

04 EDR的典型场景应用

反病毒、主动防御能力和EDR分析能力保障端点安全



反病毒、主动防御能力和EDR分析能力保障端点安全



全运维流程保障端点安全

事前	事中		事后		
预防	防护	检测	调查取证	响应	运营
<ul style="list-style-type: none">漏洞补丁管理配置核查USB管控流量管控元数据采集	<ul style="list-style-type: none">病毒检测主动防御勒索防护虚拟补丁防护应用控制	<ul style="list-style-type: none">行为分析异常检测入侵检测情报关联	<ul style="list-style-type: none">资产清点端点信誉多源关联进程调用链	<ul style="list-style-type: none">全面处置动作宏病毒修复病毒清除终端隔离	<ul style="list-style-type: none">威胁可视化告警呈现统计报表云端联动全网追溯



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

谢谢大家



安天冬训营 wtc.antiy.cn