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

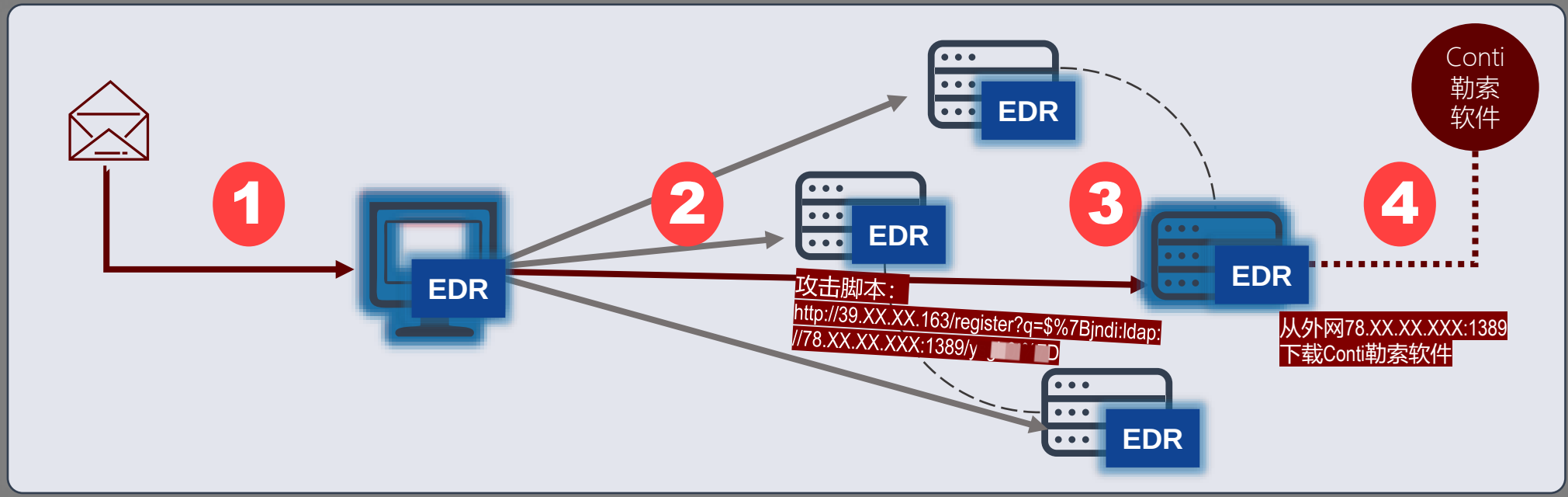
目 录

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

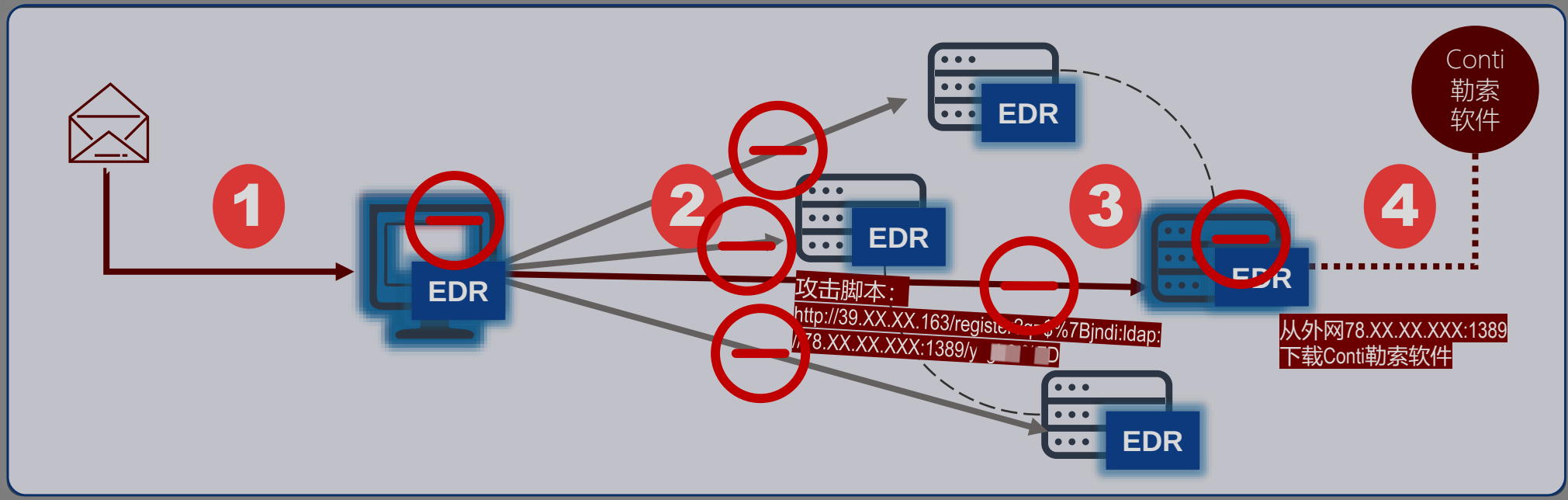
Log4j漏洞的EDR运维过程

告警	调查	响应
管理员察觉PC终端和Web服务器产生告警信息。	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。	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。

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

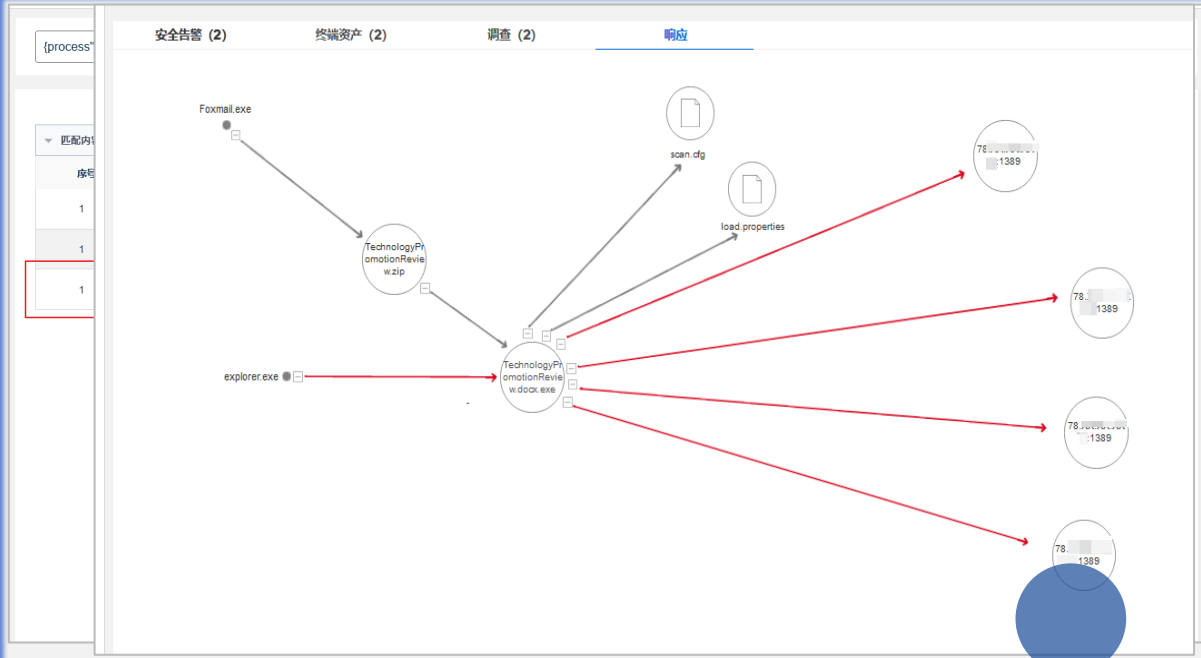


3 漏洞利用成功，连接C2服务器下载Conti勒索软件

4 Conti勒索软件本地执行

Log4j漏洞的EDR运维过程

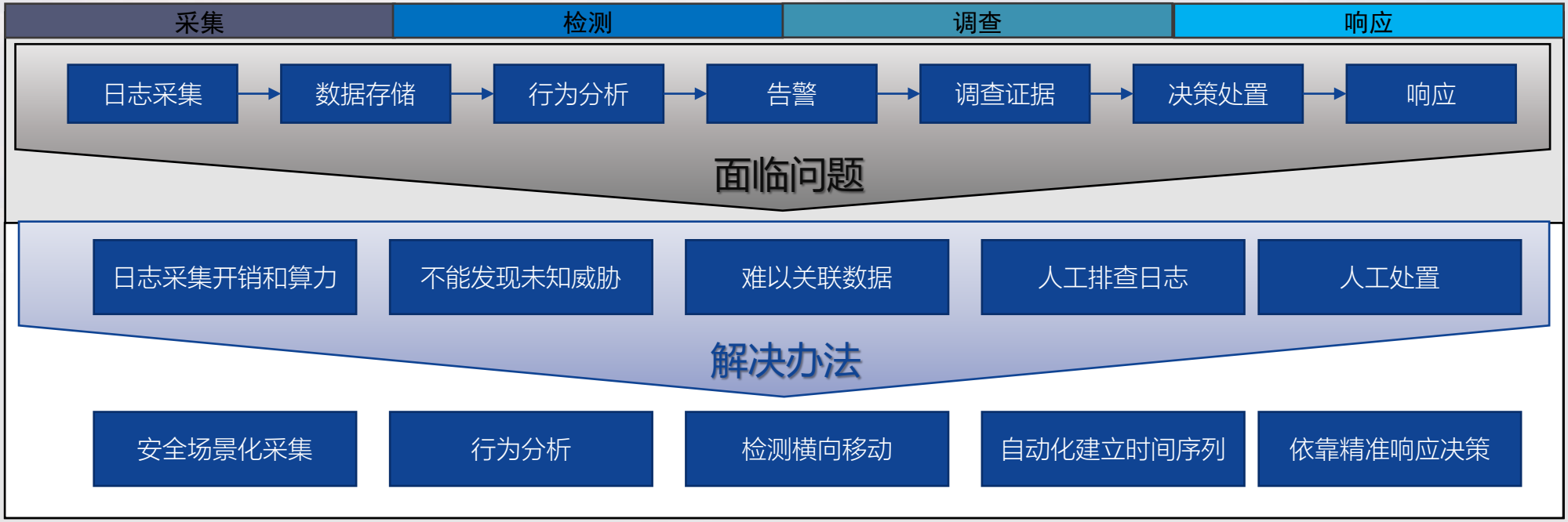
告警	调查	响应
管理员察觉PC终端和Web服务器产生告警信息。	管理员对告警展开调查，发现PC终端进程行为中，存在大量IP地址，URL中包含参数，进一步比对PC终端和Web服务器终端的IP地址。	管理员全网检索匹配内容，对PC断网隔离，阻断进程，对Web服务器上带有log4j参数进程阻断执行并进行安全加固。




```lua
function check()
    local bRet = CFile:IsFileExist("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") -- 判断文件是否存在
    if bRet then
        local bRet = CProcess:IsProcessExis\
            tByPath("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") -- 判断进程是否存在
        if bRet then
            local nFaildCount, nKillCount = CProcess:KillProces\
                sByPath("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") -- 结束进程
            print('结束进程成功数量:', nKillCount)
            print('结束进程失败数量:', nFaildCount)
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") then -- 删除文件
                print("TechnologyPromotionReview.docx.exe 文件删除成功!")
            end
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\TechnologyPromotionReview.zip") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\TechnologyPromotionReview.zip") then -- 删除文件
                print("TechnologyPromotionReview.zip 文件删除成功!")
            end
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\qsdyjh3243ffg.exe") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\qsdyjh3243ffg.exe") then -- 删除文件
                print("qsdyjh3243ffg.exe 文件删除成功!")
            end
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\gssgdfyjhfsgg.exe") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\gssgdfyjhfsgg.exe") then -- 删除文件
                print("gssgdfyjhfsgg.exe 文件删除成功!")
            end
        end

        -- 添加防火墙拦截规则
        Firewall:AddRule('block', 'http://.*/register?q=$%7Bjndi:ldap:')

    end
end

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着这个漏洞，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。



EDR在Log4j攻击场景的作用

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

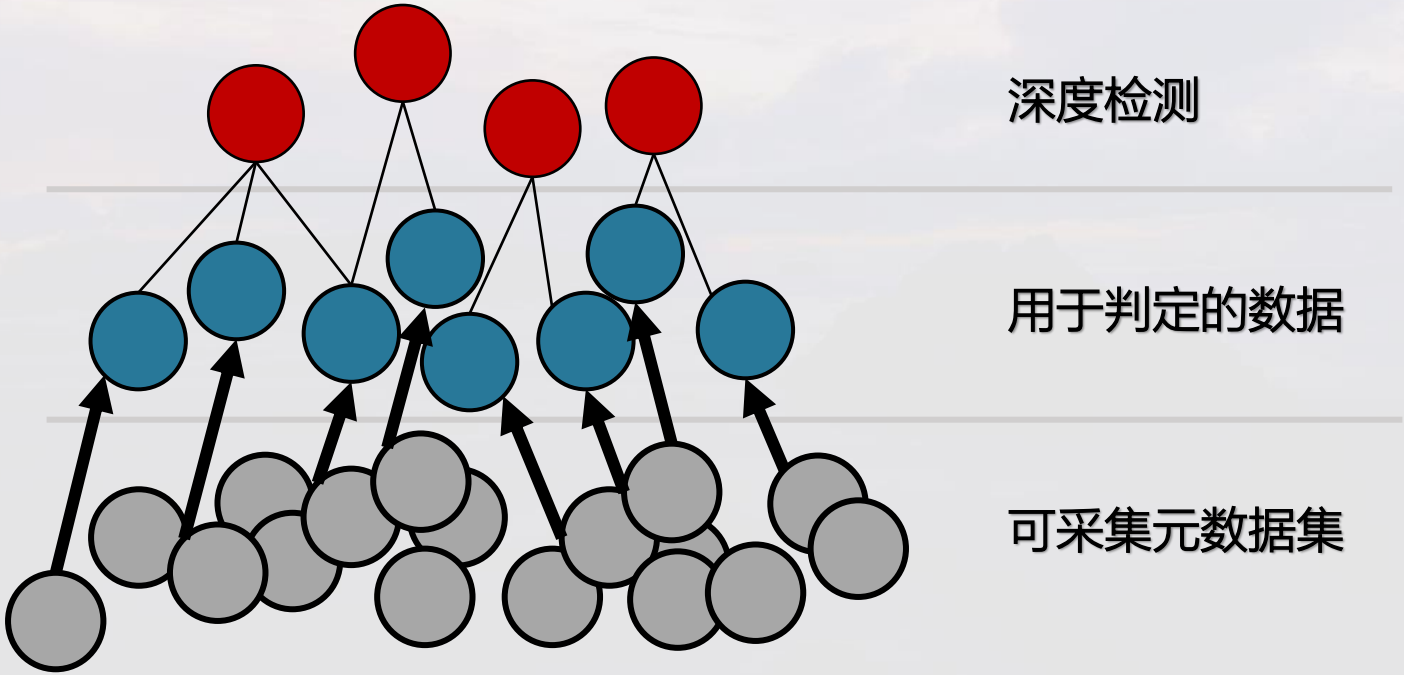
深度调查

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

02 安全场景化的EDR采集

采集数据支撑深度检测

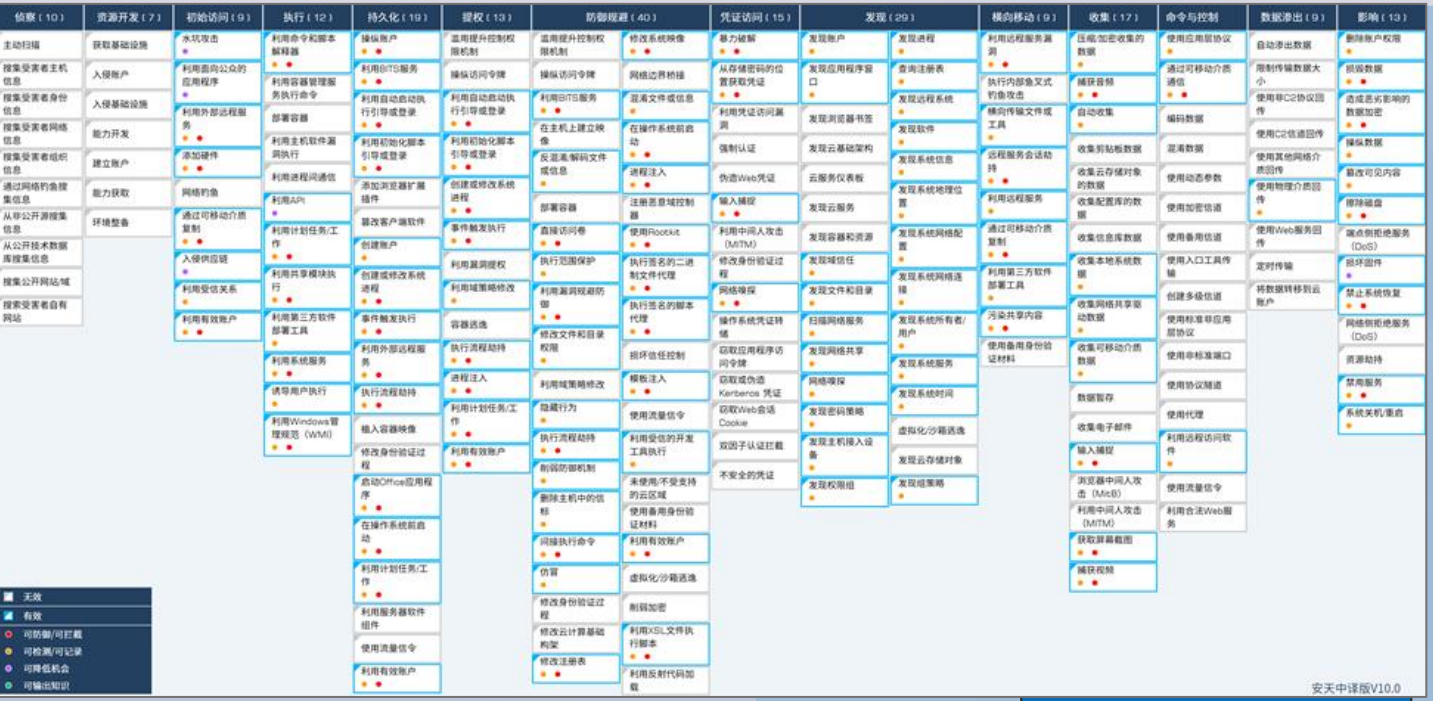
- EDR的工作对象不是特征码，是基于主机场景的元数据化采集；
- 端点的元数据是海量的分散的，端点的算力是有限的
- 深度检测只需要一部分线索来进行判定



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



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。

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。

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

监测

观察事件，
识别是否发生了问题

调查

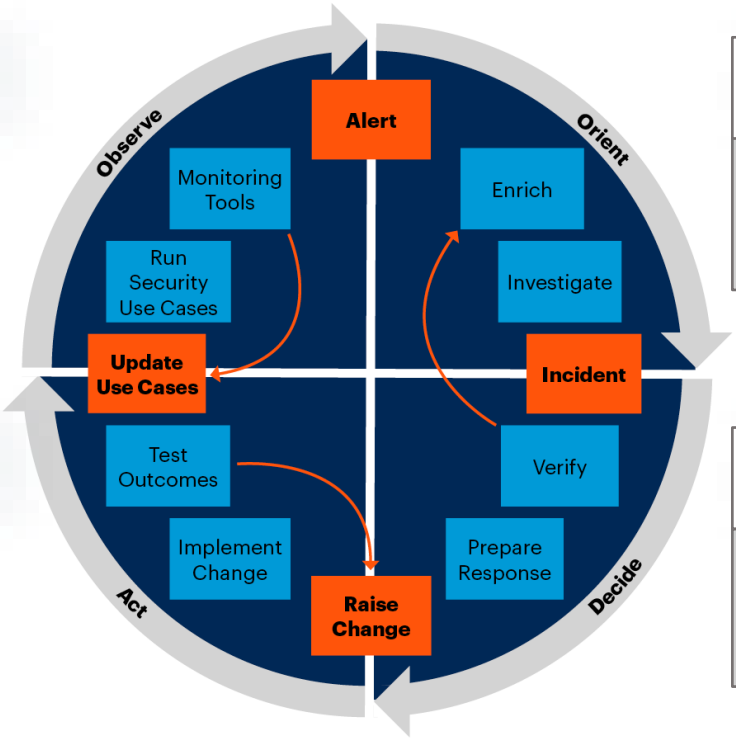
查看告警，关联多终端、多数据源，确定主机是否失陷

响应

对失陷主机进行及时的响应

决策

根据相关的线索，
决定采用什么样的的处置方法

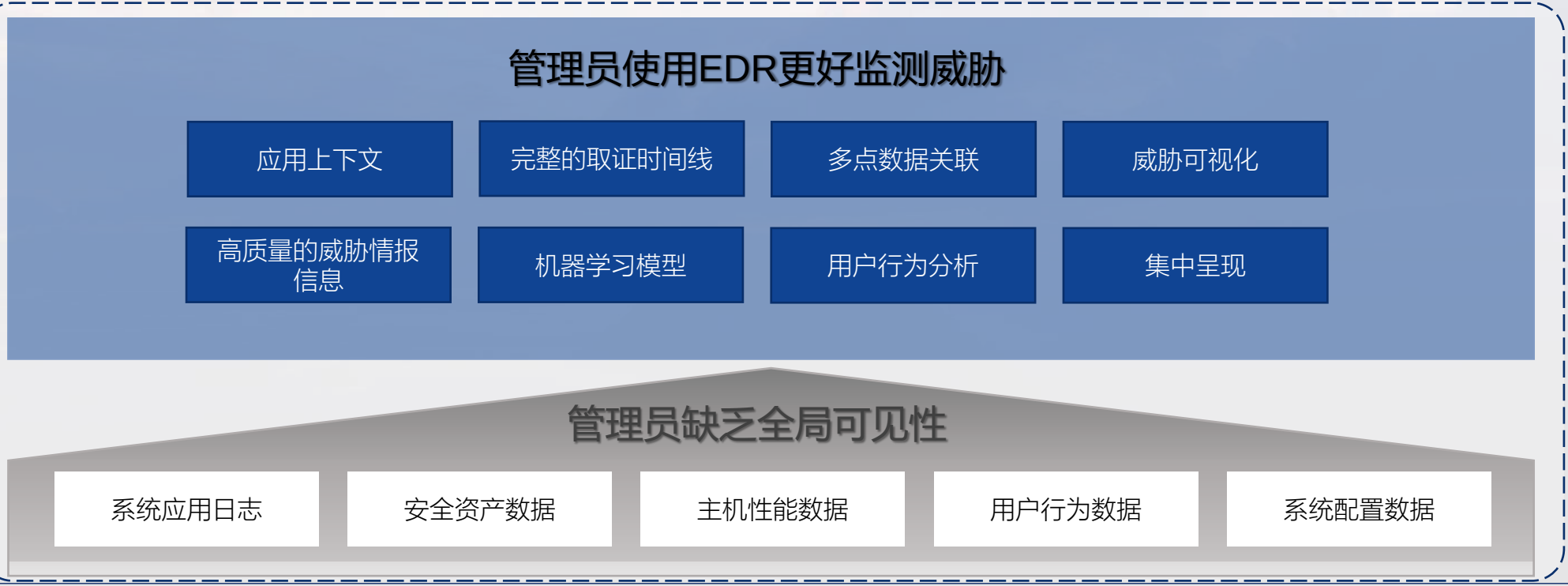


Source: Gartner
719029_C

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



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；

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

多数据源

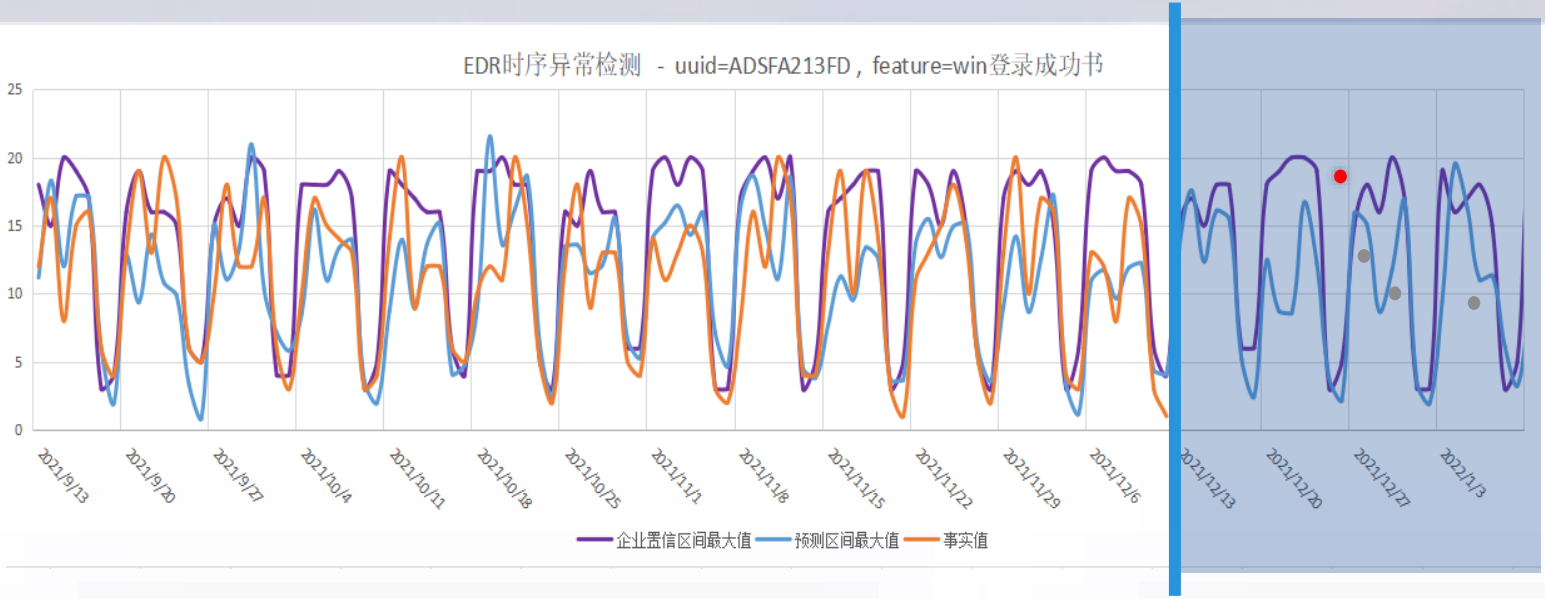
入侵检测　沙箱联动　云引擎　ATT&CK映射　威胁情报

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

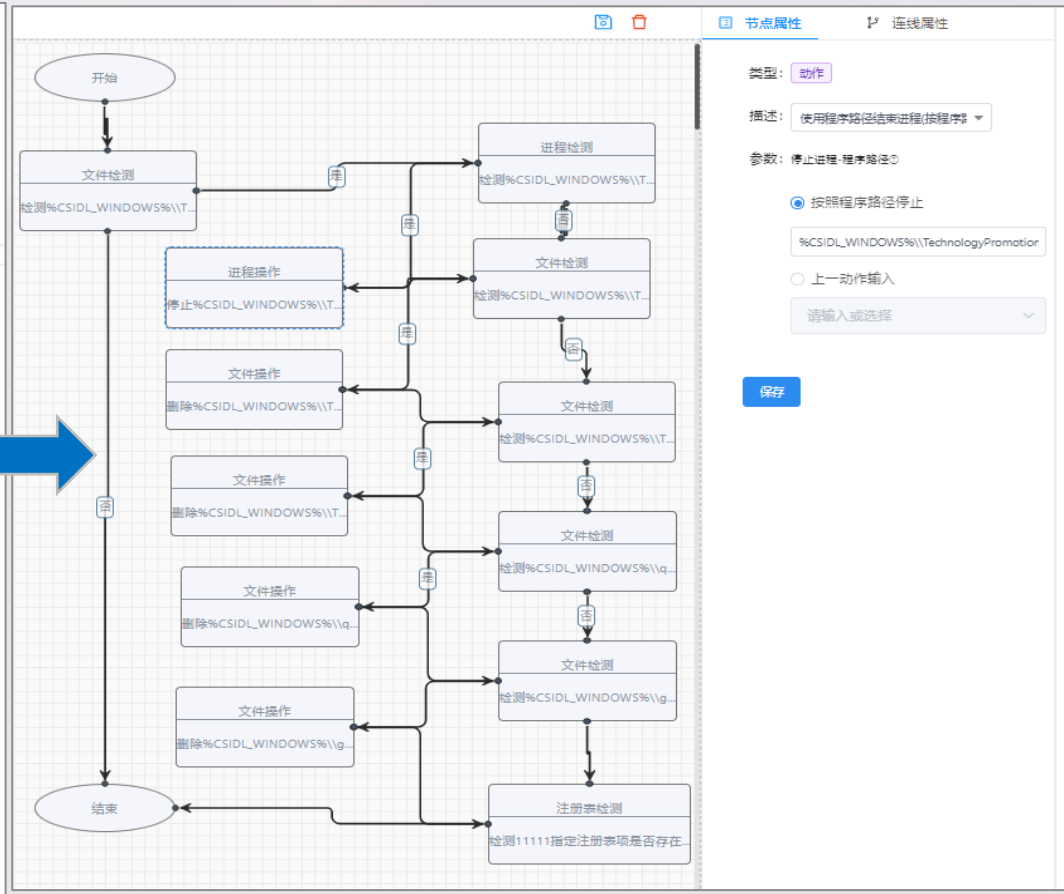
- 异常检测模型：根据多端点采集的用户历史数据，通过持续的机器学习模型构建正常的行为基线并持续更新，自适应发现偏离于基线的异常行为。

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

```
function check()
    local bRet = CFile:IsFileExist("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") -- 判断文件是否存在
    if bRet then
        local bRet = CProcess:IsProcessExis\
            tByPath("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") -- 判断进程是否存在
        if bRet then
            local nFaildCount, nKillCount = CProcess:KillProces\
                sByPath("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") -- 结束进程
            print('结束进程成功数量:', nKillCount)
            print('结束进程失败数量:', nFaildCount)
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\TechnologyPromotionReview.docx.exe") then -- 删除文件
                print("TechnologyPromotionReview.docx.exe 文件删除成功!")
            end
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\TechnologyPromotionReview.zip") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\TechnologyPromotionReview.zip") then -- 删除文件
                print("TechnologyPromotionReview.zip 文件删除成功!")
            end
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\qsdyjh3243ffg.exe") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\qsdyjh3243ffg.exe") then -- 删除文件
                print("qsdyjh3243ffg.exe 文件删除成功!")
            end
        end

        if CFile:IsFileExist("%CSIDL_WINDOWS%\\gssgdfyjhfsgg.exe") then -- 判断文件是否存在
            if CFile:FileDelete("%CSIDL_WINDOWS%\\gssgdfyjhfsgg.exe") then -- 删除文件
                print("gssgdfyjhfsgg.exe 文件删除成功!")
            end
        end

        -- 添加防火墙拦截规则
        Firewall:AddRule('block', 'http://.*/register?q=$%7Bjndi:ldap:')

    end
end

check() --执行检测函数
```

- 安天智甲支持可视化预编排响应脚本



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

主机EPP构成了实时响应
即时阻断环

漏洞与补丁管理
外设管控
网络管控
主机入侵检测
数据加密
主机防火墙
系统锁定
程序管控
高级威胁检测

威胁检测引擎

主动防御

数据泄露缓解
安全场景化采集
实时监控
脚本编排
事件响应
威胁猎杀
事件调查
集中化远程响应
端点可见性

主机EDR构成了一个准实时的异步响应环节环

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
• 漏洞补丁管理 • 配置核查 • USB管控 • 流量管控 • 元数据采集	• 病毒检测 • 主动防御 • 勒索防护 • 虚拟补丁防护 • 应用控制	• 行为分析 • 异常检测 • 入侵检测 • 情报关联	• 资产清点 • 端点信誉 • 多源关联 • 进程调用链	• 全面处置动作 • 宏病毒修复 • 病毒清除 • 终端隔离	• 威胁可视化 • 告警呈现 • 统计报表 • 云端联动 • 全网追溯

谢谢大家

安天冬训营 wtc.antiy.cn