资源代价与安全算力

从Log4j漏洞看安全运营

SecIsland The Data Security Company
朱林

CONTENTS

目 录

01 Log4j事件回顾

安全圈大事-Log4j2漏洞

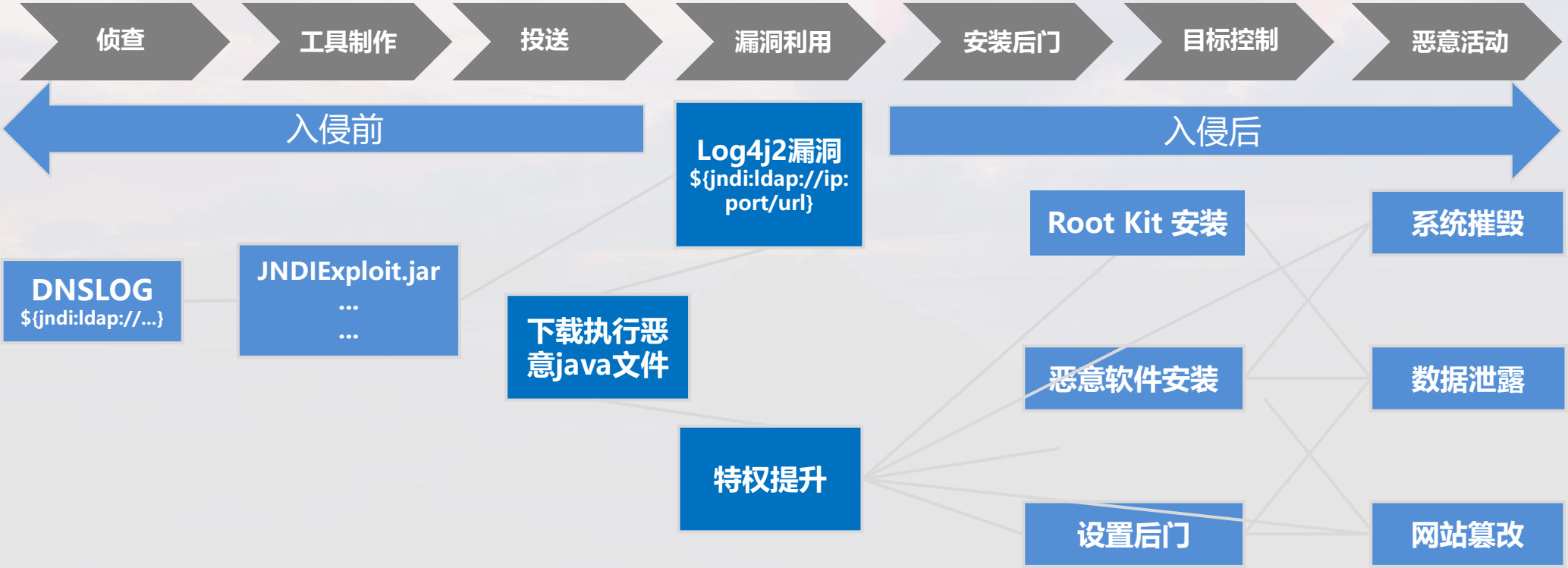
- 2021年12月9日，Log4j2漏洞引爆安全圈。
- 从9号到目前为止，围绕Log4j/Log4j2的相关漏洞已达6个。
- 其中Log4j2中存在的JNDI注入漏洞比较严重，当程序记录用户输入的数据作为日志时，即可触发此漏洞，成功利用此漏洞可以在目标服务器上执行任意代码。

- 根因：Log4j2提供的lookup功能允许开发者通过一些协议读取环境配置，但并未对输入进行严格判断。
- 影响：攻击者控制受害者的电脑和服务器，可获取数据库敏感数据，挖矿，高危命令操作等造成极大的损失。

CVE	severity	CVSS Score	Kind	Fixed version
CVE-2021-44832	Moderate	6.6	RCE	2.17.1
CVE-2021-45105	High	7.5	DoS	2.17.0
CVE-2021-45046	Critical	9.0	RCE	2.16.0
CVE-2021-44228	Critical	10.0	RCE	2.15.0
CVE-2021-42550	Moderate	6.6	RCE	Log4j 1.x
CVE-2021-4104	high	8.1	RCE	Log4j 1.2

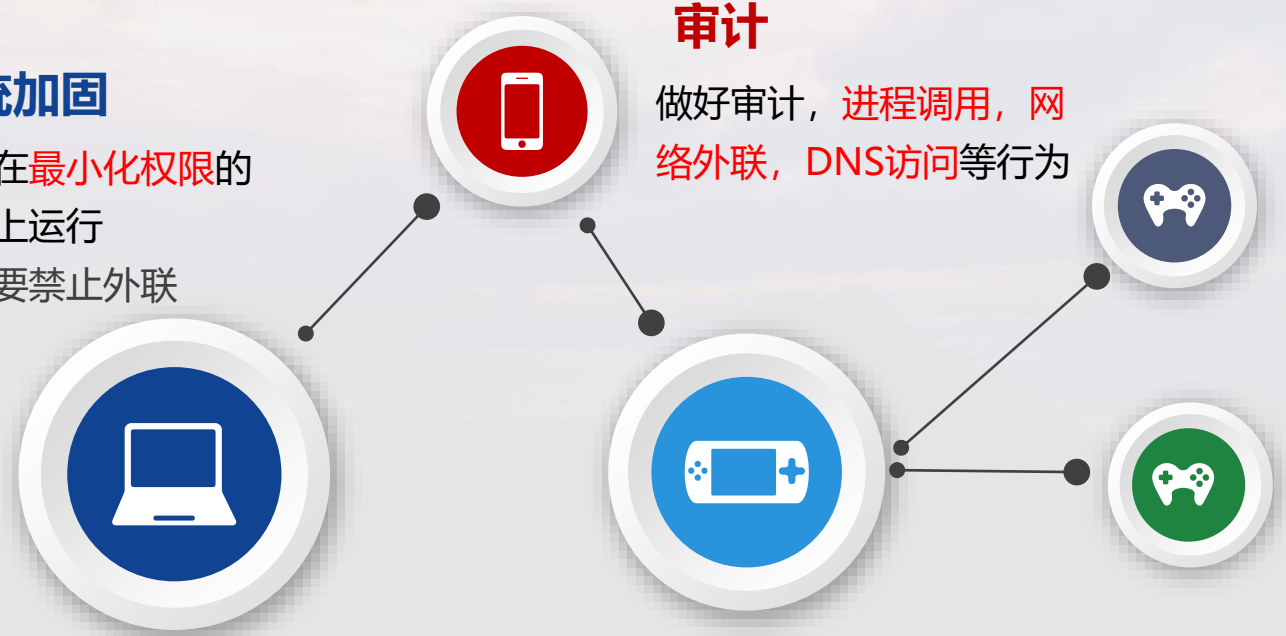
杀伤链看漏洞

基于杀伤链模型，将Log4j2漏洞利用分解成七大步骤。



漏洞复盘-事前

- 事前不知道漏洞存在，所以没有办法直接规避
- 但可以在事前做好的一些防护来减少甚至规避风险
- 可以对事中漏洞处理提供信息



系统加固

进程在最小化权限的账号上运行

非必要禁止外联

审计

做好审计，进程调用，网络外联，DNS访问等行为

开发

用Java Security Manager进行java开发加固

资产管理

对业务进行管理，包括开发语言，使用的框架，使用的依赖包等

防护

提前部署RASP

漏洞复盘-事中-无方案

漏洞复盘-事中-有方案

外围防护

- WAF
- IPS
- HIDS
- EDR

漏洞修复

持续跟踪

漏洞复盘-事后

漏洞扫描验证

事件闭环处理

攻击溯源分析

复盘

漏洞折射的出来的问题

1.基础建设不扎实

- 资产梳理不清
- 资产标签覆盖不全
- 无法快速盘点影响面
- 漏洞处置无闭环管理
- 补丁、弱口令、配置不当

2.攻击检测、溯源分析不足

- 安全设备堆砌
- 无统一分析平台，孤岛式防御
- 告警误报率高
- 无法第一时间发现未知攻击
- 缺乏溯源分析和调查取证能力

3.安全运营体系建设不全

- 无应急预案，无有效组织，权责混乱
- 无验证过程，盲目处置
- 处置流程不完善，事件追踪不及时
- 缺乏协同处置能力，效率低下
- 安全事件无法闭环

安全运营：真正对安全结果负责！

02 安全运营现状与体系化建设

安全运营定义

职业欠钱

“为了实现安全目标，提出安全解决构想、验证效果、分析问题、诊断问题、协调资源解决问题并持续迭代优化的过程”。

01 以始为终

- 以目标为导向
- 安全与业务相结合

02 持续迭代

- 是一个持续迭代的过程
- 只有进行时
- 量化是持续迭代的手段

03 手段不限

管理和技术不分彼此

04 态度转换

由被动解决问题，向主动寻找问题转换

《我理解的安全运营》，职业欠钱，2018.7，https://zhuonion.zhihu.com/p/39467201

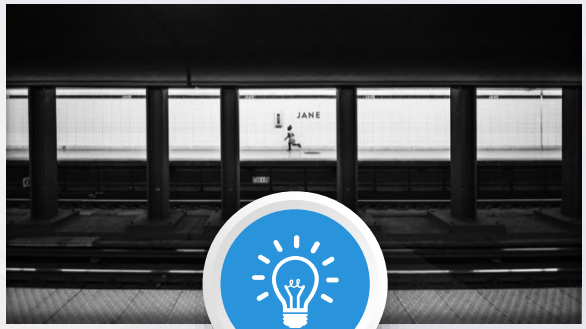
完整的安全运营体系


1.防护监测
持续性动态监测
安全设备事件
2.响应分析
对事件进行快速响应
对告警或信息进行确认
3.调查处置
对安全事件分析还原
快速进行止损、善后
4.复盘评估
复盘事件原因
完善修复方案
5.完善加固
执行修复方案
增强防护和监测能力

安全运营核心内容

安全防护与预警

- 威胁检测
- 态势感知
- 安全预警



安全监控与分析

- 终端监控
- 流量监控
- 日志分析
- 入侵检测

事件响应与处置

- 分析定级
- 处置方案
- 总结改进

安全运营框架：人、流程、技术有机结合

安全组织与管理

- 组织架构
- 岗位职责
- 绩效考核
- 风险管理
- 合规管理
- 流程管理
- 制度管理
- 知识管理

安全运营分析

态势感知

- 综合态势
- 告警态势
- 漏洞态势
- 资产态势

平时大屏

- 威胁情报
- 风险评估
- 事件调查
- 协同分析
- 溯源取证
- 漏洞追踪

战时大屏

- 应急响应
- 指挥调度
- 重大安保
- 协同处置
- 复盘推演
- 研判分析

支撑产品：安全管理平台（集中采集、存储、多维智能关联分析、可视化）

纵深防御关联分析

资产管理	安全威胁监测分析		异常行为分析		安全事件分析
资产自动发现 资产风险值 漏洞检测	毒木蠕 数据泄露 非法外联	端口扫描 提权 SSH跳板登录	账号异常 行为异常 密码猜测	绕行访问 高危操作 敏感文件访问	溯源追踪 多源关联分析 分析报告

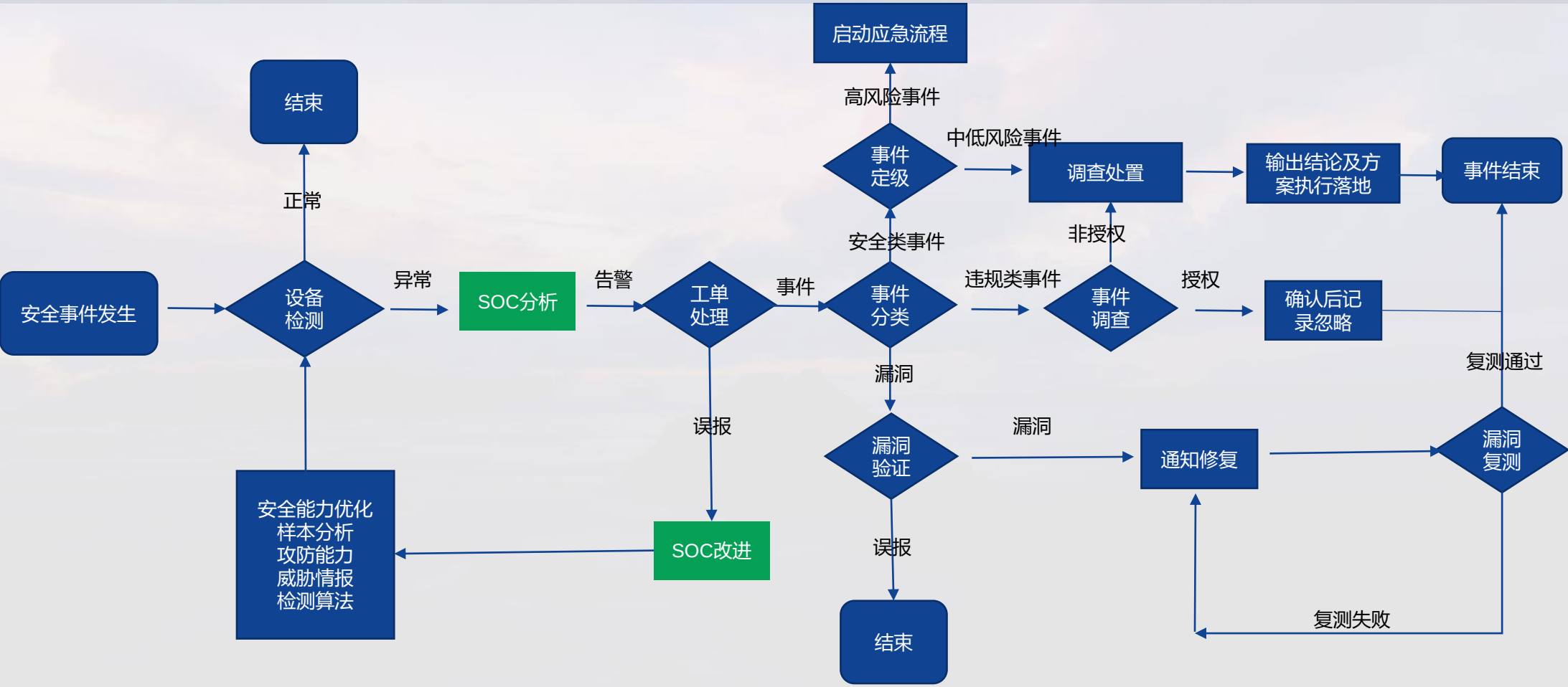
单点防护技术体系

物理安全 | 边界安全 | Web安全 | 移动安全 | 云安全 | 终端安全 | 应用安全 | ……

安全服务

- 代码审计
- 安全培训
- 安全加固
- 安全运维
- 攻防演练
- 应急响应
- 安全咨询
- 风险评估
- 漏洞扫描
- 渗透测试

事件处置流程


启动应急流程
结束
高风险事件
事件定级
中低风险事件
调查处置
输出结论及方案执行落地
事件结束
正常
安全类事件
非授权
安全事件发生
设备检测
异常
SOC分析
告警
工单处理
事件
事件分类
违规类事件
事件调查
授权
确认后记录忽略
复测通过
漏洞
误报
漏洞验证
漏洞
通知修复
漏洞复测
安全能力优化
样本分析
攻防能力
威胁情报
检测算法
SOC改进
误报
结束
复测失败

安全运营流程闭环要素

01 事件分类

参照《信息安全事件分类分级指南》

- 网络扫描窃听事件
- 后门攻击事件
- 漏洞攻击事件
- 拒绝服务攻击事件
- 网络钓鱼事件

02 职责分工

三组联动

- 分析组：监控设备告警、分析告警影响、全网排查
- 处置组：决策、资产定位、应急响应、工具准备
- 消息组：下达上传、事件闭环、汇总
- 值班表

03明确流程

PDCERT模型

- 6个阶段：准备、诊断、抑制、根除、恢复、跟踪
- 明确各类安全事件中三个组的工作内容
- 常见抑制措施：网络隔离、关机、修改DNS、黑名单

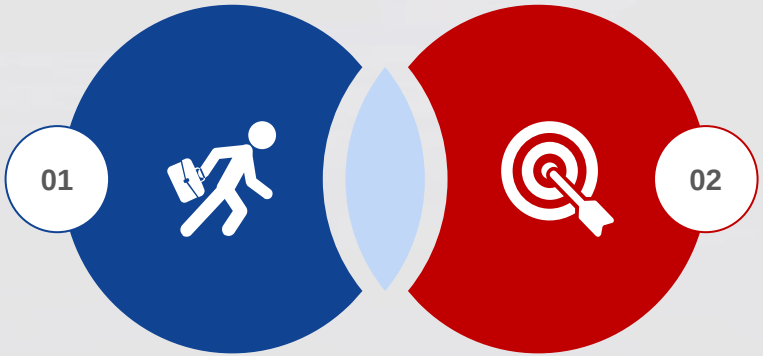
04 规范手段

沟通和汇报

- 违反保密规定，无意泄露信息
- 内外沟通渠道分离
- 日报、周报
- 每日复盘会议
- 工作总结

一靠机制

- 日例会
- 周回顾
- 月总结



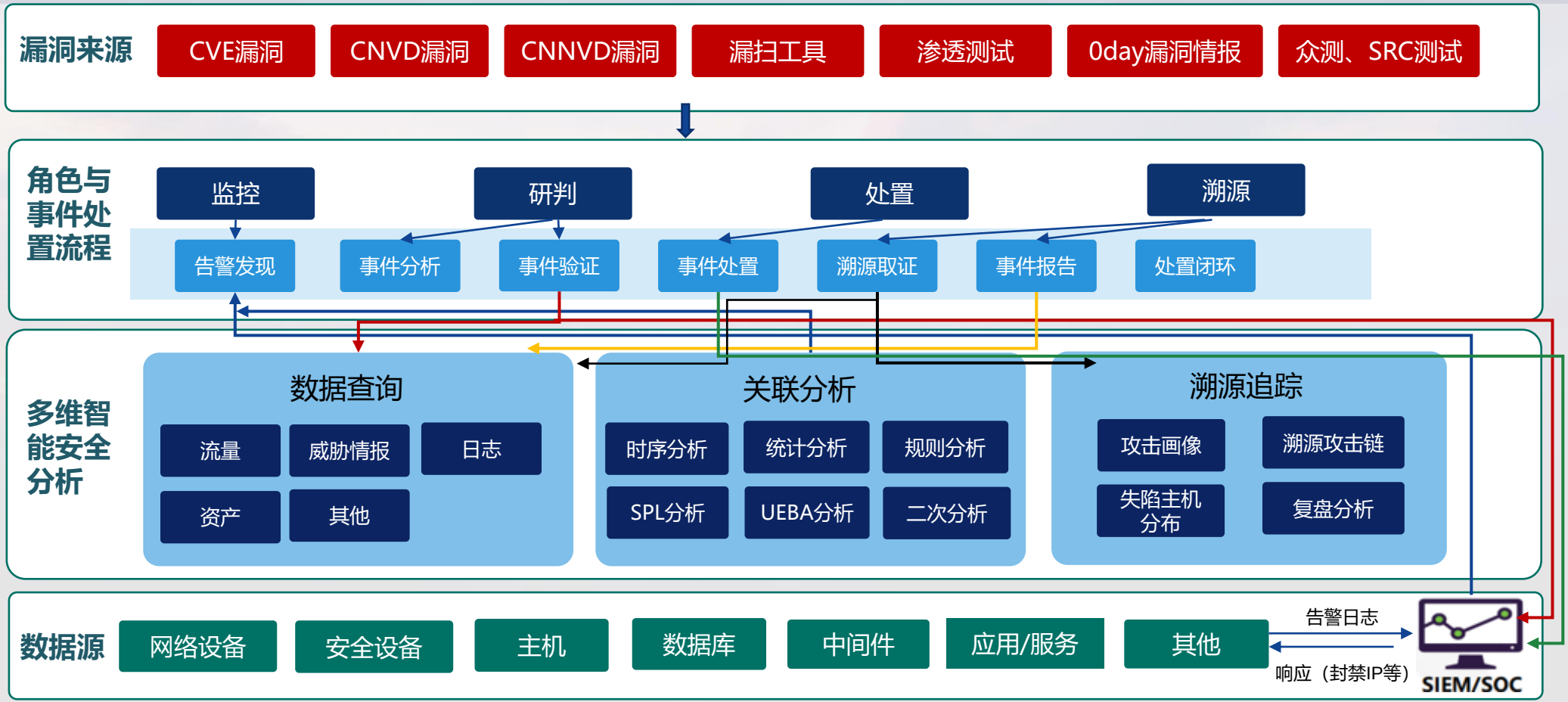
二靠平台

- 流程平台工单流转逻辑
- 重要流程审核机制

流程保障不能靠人！

03 如何有效应对类似漏洞

漏洞处置流程


漏洞来源
CVE漏洞
CNVD漏洞
CNNVD漏洞
漏扫工具
渗透测试
0day漏洞情报
众测、SRC测试
角色与事件处置流程
监控
研判
处置
溯源
告警发现
事件分析
事件验证
事件处置
溯源取证
事件报告
处置闭环
多维智能安全分析
数据查询
流量
威胁情报
日志
资产
其他
关联分析
时序分析
统计分析
规则分析
SPL分析
UEBA分析
二次分析
溯源追踪
攻击画像
溯源攻击链
失陷主机分布
复盘分析
数据源
网络设备
安全设备
主机
数据库
中间件
应用/服务
其他
告警日志
响应（封禁IP等）
SIEM/SOC

安全事件各阶段重点工作

未雨绸缪

- 细粒度资产梳理（透视资产详情、业务关系、分析影响面）
- 异常行为分析预警
- 基线核查及安全加固
- 实时关注业界漏洞及威胁情报

火眼金睛

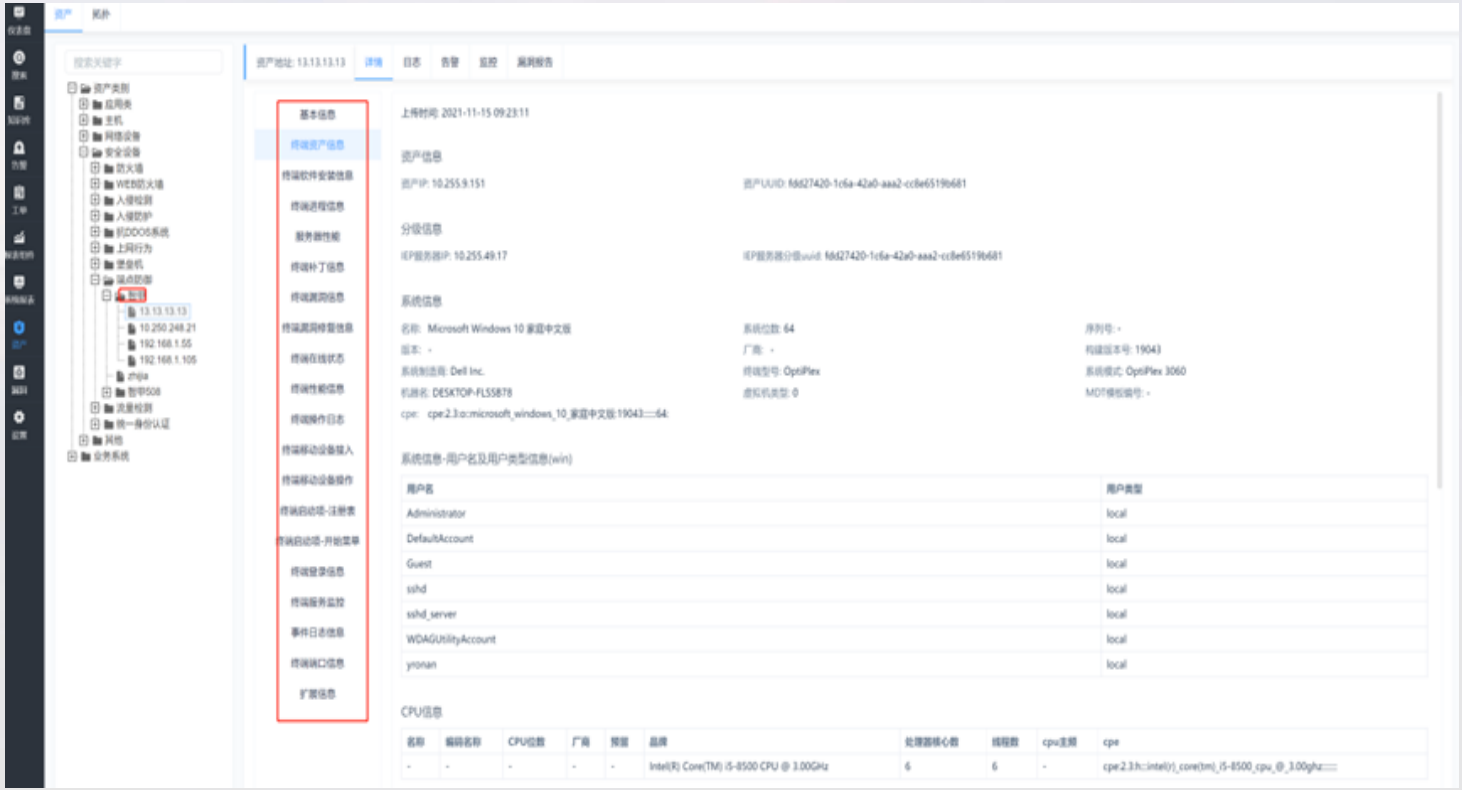
- 基于多数据源监测告警
- 基于漏洞特征检测
- 纵深关联分析减少误报
- 漏洞复现验证告警有效性

及时止损

- 威胁分析与处置
- 漏洞检测与修复闭环
- 复盘分析与持续优化
- 流程编排自动化提升效率

筑牢基础：细粒度资产管理

- 采集资产的细粒度信息：业务、补丁、安装软件版本、漏洞、开放端口、服务、进程、注册表等。
- 一键搜索资产所有信息：例如一键搜索所有依赖Log4j2库的应用系统，提升精准处置效率。
- 资产关系：通过资产关系确定漏洞利用的影响大小。



多面防护：关联多类预警提高准确性

主机防护

防火墙、防病毒

HIDS

数据防护

数据库高危操作告警

数据库敏感文件访问告警

网络防护

限制访问源IP

非允许IP登录告警

非法外联告警

端口扫描告警

应用防护

日志采集必须完整

账户梳理

行为分析

网络连接分析

进程分析

非常见命令执行

- 多次登录失败
- 内网扫描
- 可疑账户行为
- 可疑网络通讯
- 可以非法外联
- 数据外传
- ……

Threat!

常态化落地：基线核查及安全加固

补丁

期间：月度补丁
分布式漏扫工具：高危漏洞全部修复，否则关机处理（含测试环境）
漏洞修复：快速推动漏洞修复。

弱口令

AD弱口令：脚本检查
系统弱口令：HIDS
应用弱口令：脚本检查

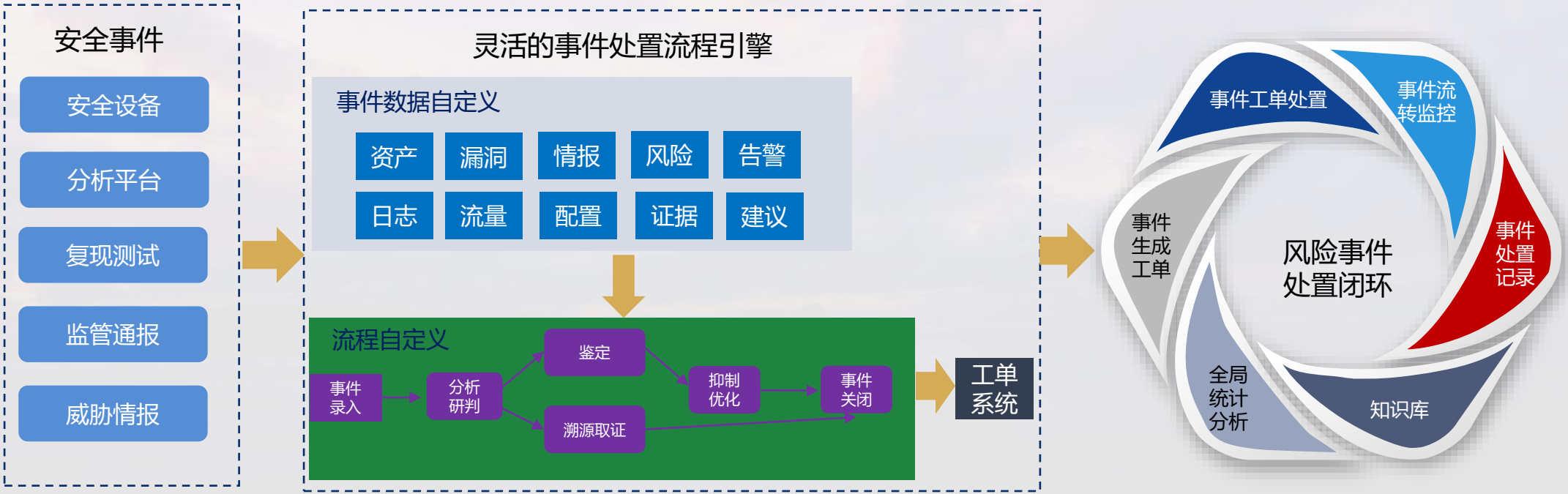
防病毒

Windows：覆盖率
Linux:EDR进行扫描

误配置

渗透测试
HIDS
权限设置过大、demo目录

流程编排自动化提升协同处置效率



04 安全运营产品关键能力

多源数据大数据存储

- Syslog
- Sftp
- ftp
- Jdbc
- Kafka
- Httppost
- Nxlog
- ……

- 按需存储，灵活可选
- clickhouse最高达10%数据压缩比
- es冷热数据分离，高性能存储及查询

- 界面配置无需动代码即可自定义解析规则
- 数十种解析函数，支持用户自定义函数
- 复杂json数组嵌套解析

智能化关联分析

单条事件分析	多条事件 单维度分析	多条事件 多维度分析	时序关联分析	统计关联分析	二次分析	动态字典分析
根据单条日志可以分析出来的异常行为。 非办公区域登录： 源IP not in workip &&事件类型=login &&结果=success。	根据多条日志单维度可以分析出来的异常行为。 密码猜测： 条件： 事件类型=login &&结果=fail 时间范围：三分钟 次数范围：大于6次。	根据多条日志多维度可以分析出来的异常行为。 端口扫描： 条件：事件来源=firewall &&类型!=deny 时间范围：一分钟次数范围：>1000次相同维度：源，目标IP不同维度：端口。	根据时间先满足一个规则，在满足一个规则。 密码猜测成功： 先满足密码猜测条件； 然后满足登录成功条件。	根据历史统计值进行对比分析。 流量异常行为分析： 统计历史的流量平均值。 当天的流量大于历史平均值的50%以上。	产生告警后在结合其他数据进行二次分析。 通过vpn进入系统进行扫描：发现内网有扫描告警，然后根据告警内网ip分析出公网ip信息。	有些数据量比较大的场景可以借助动态字典进行分析。 比如url新增异常，把url作为动态字典学习，当产生新的url后告警。低频攻击场景。

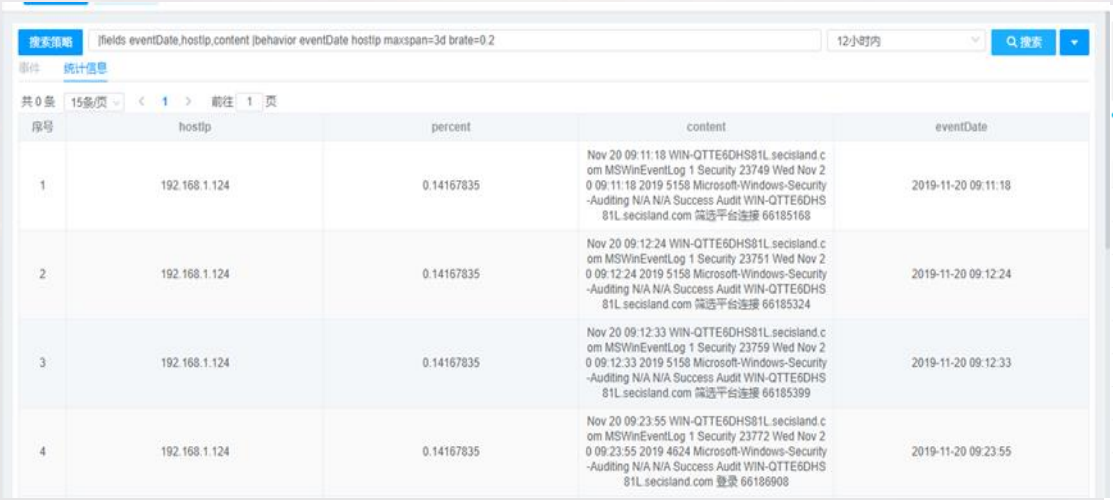
告警规则支持模糊匹配原始日志或流量关键字，简单的场景无需解析也可以通过命中原始数据关键字生成告警规则触发告警。

UEBA用户异常行为分析

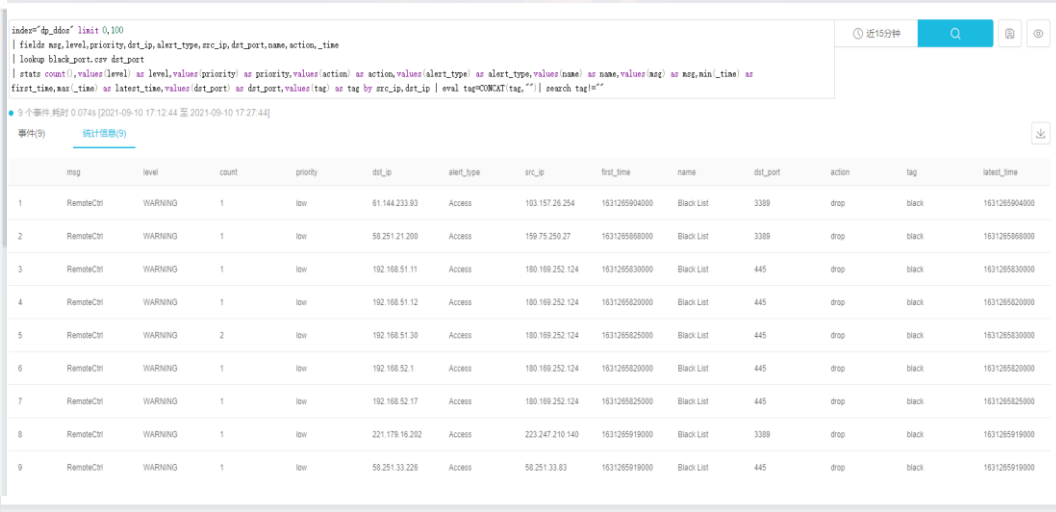
UEBA用户行为分析模型，首先确定构成正常系统的行为，然后识别偏离该正常系统的行为。通过人和资产行为分析，能够帮助企业及早发现数据泄露、违规操作、账户异常、业务异常、设备异常等风险事件，自动检测攻击和风险行为，减少解决这些异常事件所需的时间和资源，有效提升运维监控及安全运营效率。

SPL高效查询

SPL是Search Process Language的简称，它是一种搜索语言，能够实现从数据获取、分析、可视化整个过程。通过SPL可以快速查找可疑事件及行为，方便溯源分析，直接使用函数进行计算分析，无需编写代码。



SPL统计异常IP（低频访问）



SPL查询ddos攻击日志信息

SOAR流程自动化编排

自动化编排功能，具备可视化的流程编排工具，支持用户自定义剧本。对于发现的安全事件可自动启动预编排的响应流程，从而实现安全告警的自动化处置，从而实现事件快速、闭环处置。

剧本编排

具备成熟的可定制化的任务执行编排功能，活动之间支持复杂的逻辑处理，各任务之间能够自由组合并发挥整体作用。

自动化响应

具备智能化的响应机制，利用大数据技术，聚类分析以及溯源分析，输出分析结果自动触发响应机制。

集成控制

能够适配大部分主流厂商的安全产品接口，实现数据共享与远程控制和策略下发。

威胁情报共享

支持情报落地存储，支持吸收第三方情报或通过API网关对接第三方SaaS接口，内置情报全生命周期管理。

谢谢大家

安天冬训营 wtc.antiy.cn