



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

# 从Log4j漏洞看安全运营



朱林

# CONTENTS

## 目 录

01

Log4j事件回顾

---

02

安全运营现状与体系化建设

---

03

如何有效应对类似漏洞

---

04

安全运营产品关键能力

---



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

# 01 Log4j事件回顾

# 安全圈大事-Log4j2漏洞

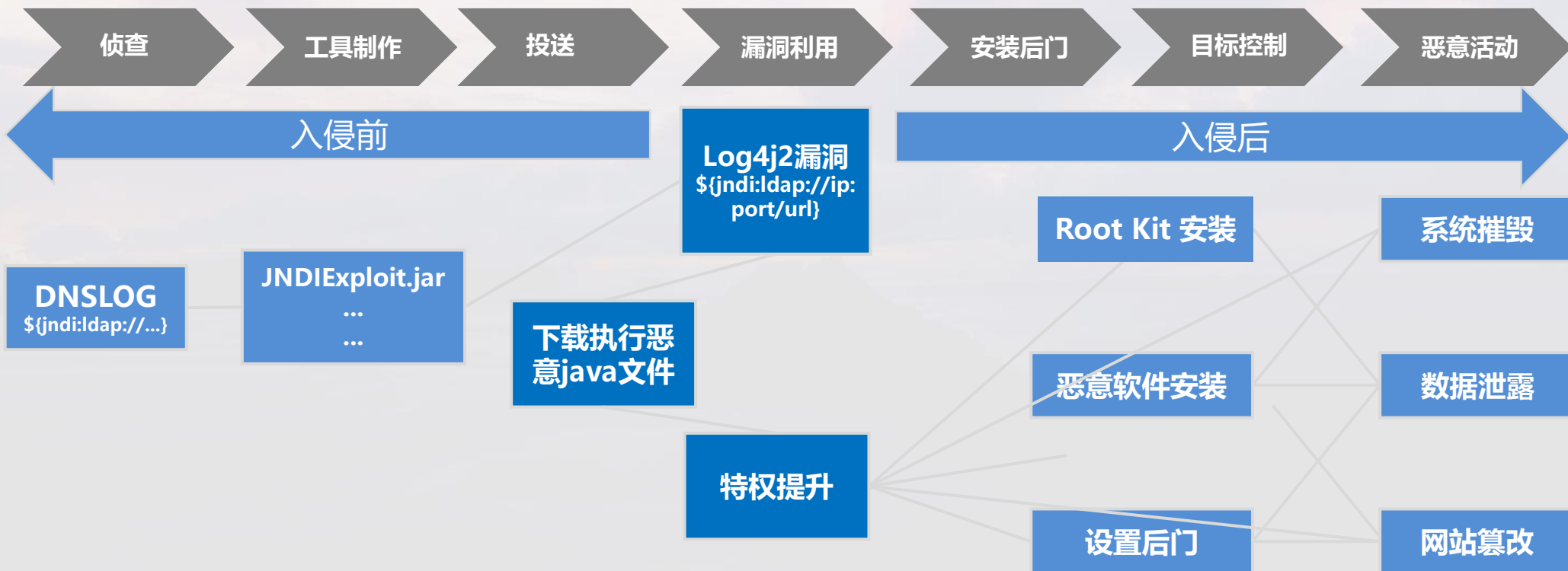
- 2021年12月9日，Log4j2漏洞引爆安全圈。
- 从9号到目前为止，围绕Log4j/Log4j2的相关漏洞已达6个。
- 其中Log4j2中存在的JNDI注入漏洞比较严重，当程序记录用户输入的数据作为日志时，即可触发此漏洞，成功利用此漏洞可以在目标服务器上执行任意代码。
- 根因：Log4j2提供的lookup功能允许开发者通过一些协议读取环境配置，但并未对输入进行严格判断。
- 影响：攻击者控制受害者的电脑和服务器，可获取数据库敏感数据，挖矿，高危命令操作等造成极大的损失。



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**





## 外围防护

- WAF
- IPS
- HIDS
- EDR



漏洞修复

持续跟踪



漏洞扫描验证

事件闭环处理

攻击溯源分析

复盘





## 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！



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

# 02 安全运营现状与体系化建设

## 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>

## 1.防护监测

持续性动态监测  
安全设备事件



## 3.调查处置

对安全事件分析还原  
快速进行止损、善后



## 5.完善加固

执行修复方案  
增强防护和监测能力

## 2.响应分析

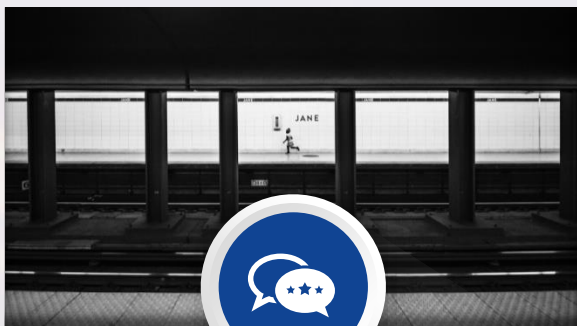
对事件进行快速响应  
对告警或信息进行确认



## 4.复盘评估

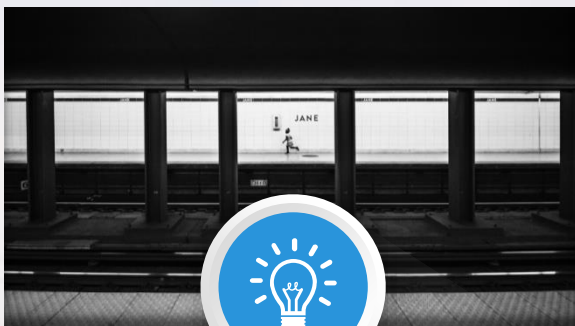
复盘事件原因  
完善修复方案





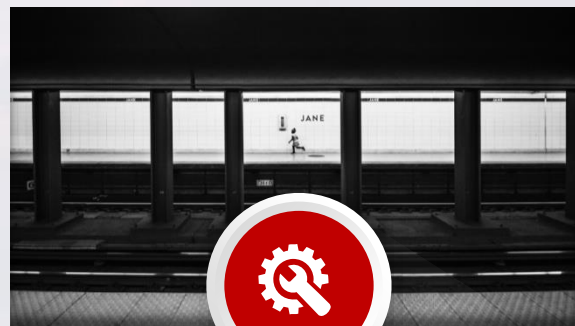
## 安全防护与预警

- 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		平时大屏			战时大屏		
综合态势	告警态势	威胁情报	风险评估	事件调查	应急响应	指挥调度	重大安保
漏洞态势	资产态势	协同分析	溯源取证	漏洞追踪	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

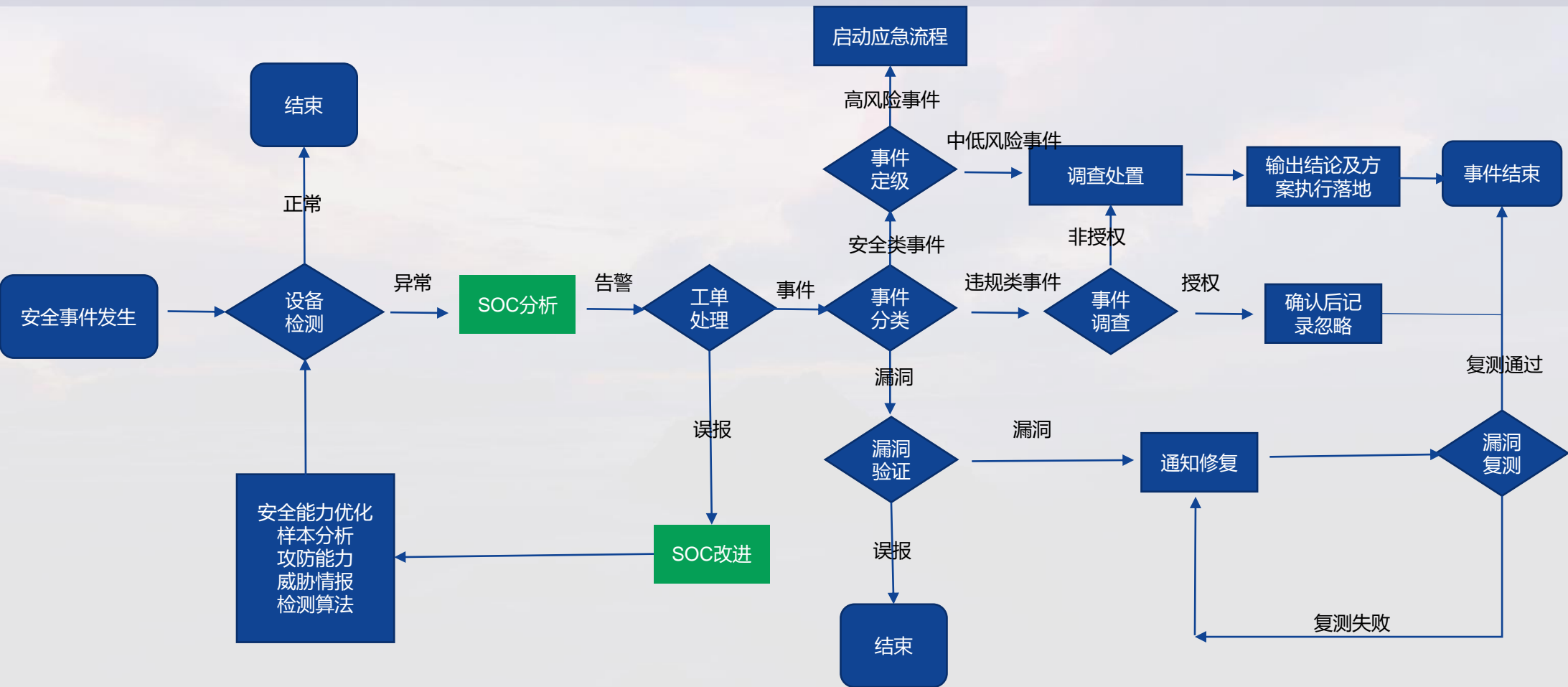
资产管理	安全威胁监测分析		异常行为分析		安全事件分析
资产自动发现 资产风险值 漏洞检测	毒木蠕 数据泄露 非法外联	端口扫描 提权 SSH跳板登录	账号异常 行为异常 密码猜测	绕行访问 高危操作 敏感文件访问	溯源追踪 多源关联分析 分析报告

### 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



## 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

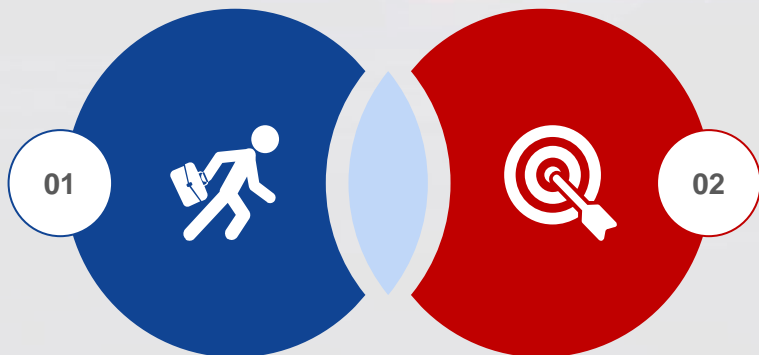
## 04 规范手段

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!

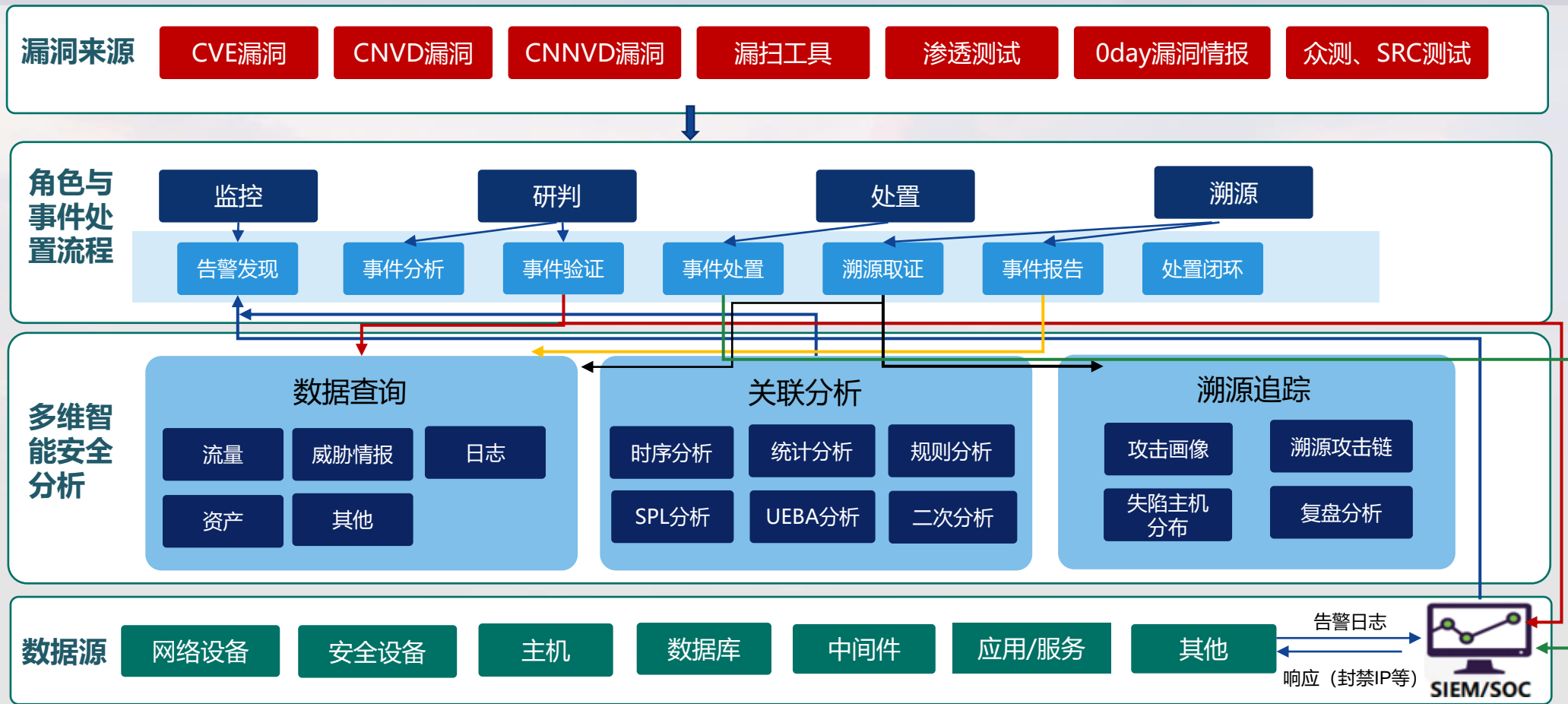


网络空间威胁对抗与防御技术研讨会  
暨 第九届安天网络安全冬训营

亂雲飛渡

# 03 如何有效应对类似漏洞

# 漏洞处置流程





## 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



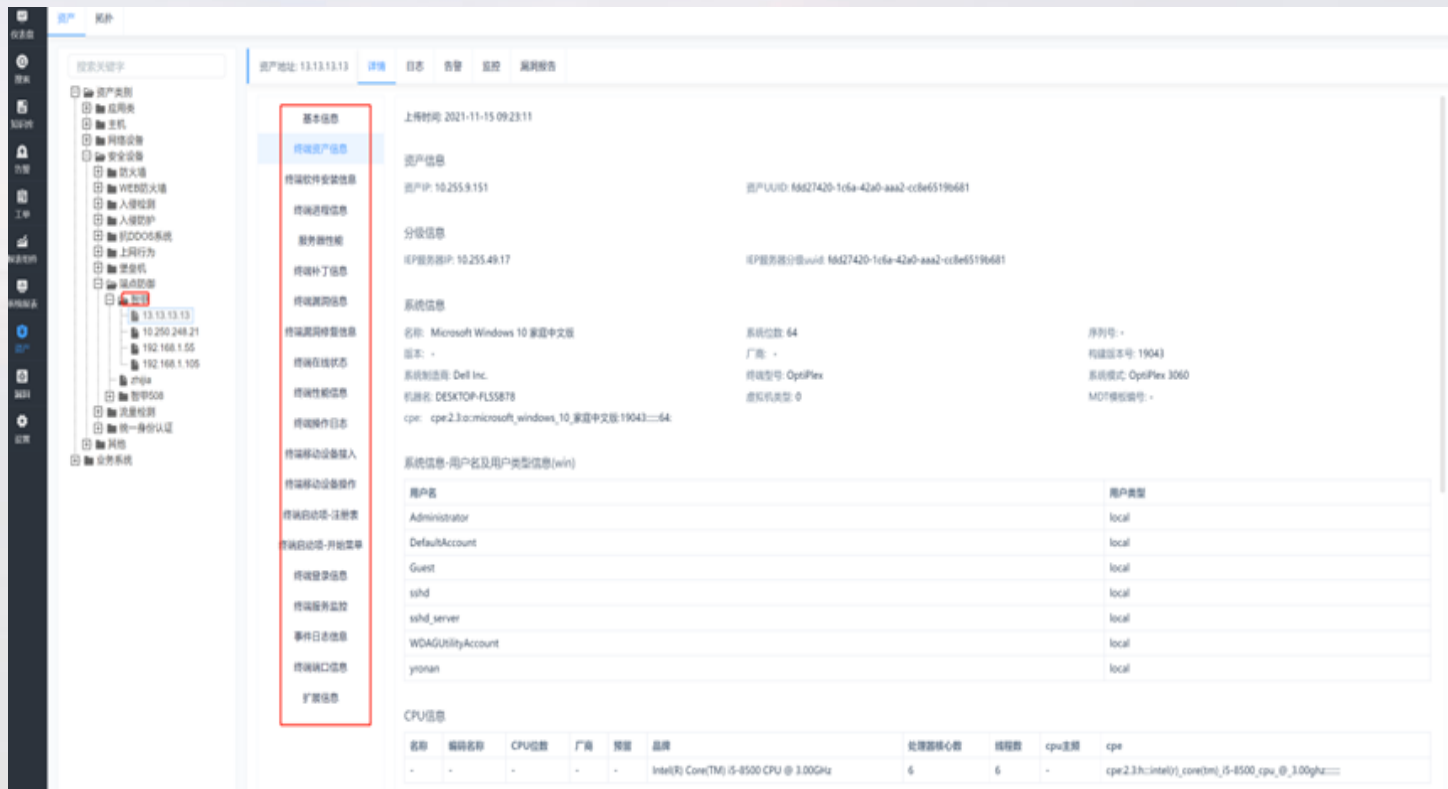
## 及时止损

- 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。



The screenshot displays the ANTIY asset management interface. On the left, a sidebar shows a tree view of assets, with the selected asset '13.13.13.13' highlighted. The main panel shows detailed information for this asset, including:

- 基本信息**: 上传时间: 2021-11-15 09:23:11
- 资产信息**: 资产IP: 10.255.9.151, 资产UUID: 66627420-1c6a-42a0-aaa2-ccb65196681
- 分簇信息**: IP服务簇分簇id: 66627420-1c6a-42a0-aaa2-ccb65196681
- 系统信息**: 名称: Microsoft Windows 10 家庭中文版, 系统位数: 64, 版本: -, 系统制造商: Dell Inc., 序列号: -, 制造商: OptiPlex 3060, 初始名: DESKTOP-FL55878, 虚拟机型号: 0, cpe: cpe:2.3:os:microsoft\_windows\_10\_家庭中文版:19043---64, MOI详细编号: -
- 系统信息-用户名及用户类型信息(win)**:

用户名	用户类型
Administrator	local
DefaultAccount	local
Guest	local
sshd	local
sshd_server	local
WDAGUtilityAccount	local
yjman	local
- CPU信息**:

名称	编码名称	CPU位数	厂商	类别	品牌	处理器核心数	线程数	cpu逻辑	cpe
-	-	-	-	-	Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz	6	6	-	cpe:2.3:cpu:intel(i5-8500)cpu_@_3.00ghz---

# 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!**

## 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



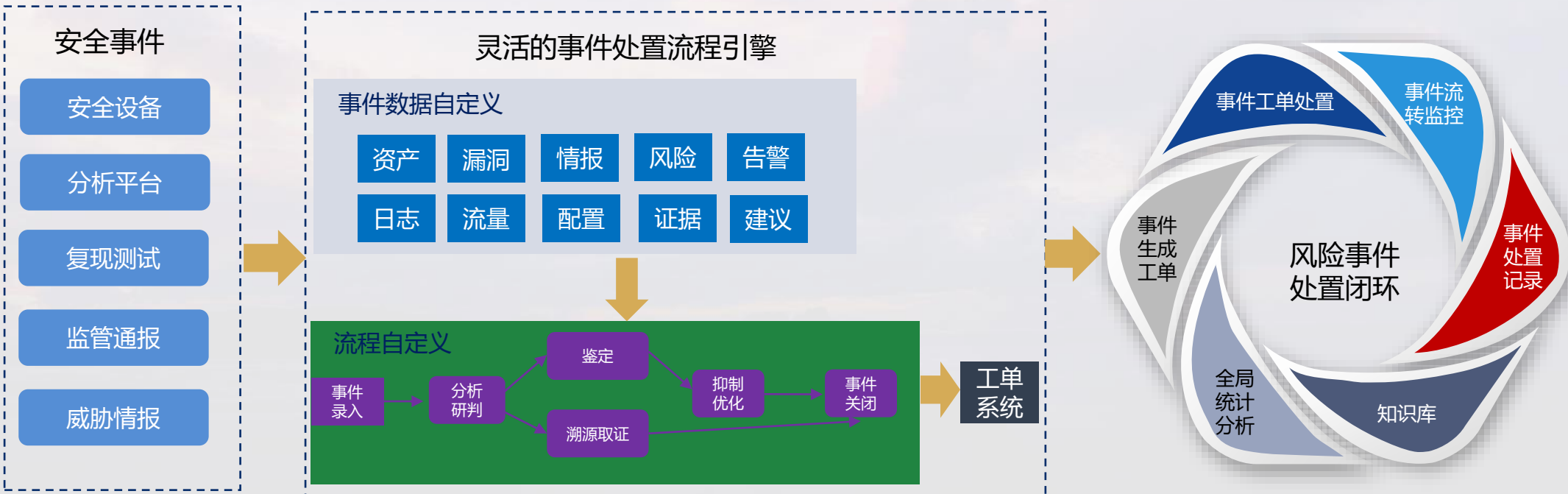
## 防病毒

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





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

# 04 安全运营产品关键能力

## 多数据源采集

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

## 大数据存储

ES  
CLICKHOUSE

- 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

## 灵活数据解析

- 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

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。

## 多条事件单维度分析

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。

## 多条事件多维度分析

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。

## 时序关联分析

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。

## 统计关联分析

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。

## 二次分析

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。

## 动态字典分析

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。

搜索规则: |fields eventDate,hostip,content |behavior eventDate hostip maxspan=3d brate=0.2 12小时内 搜索

事件 统计信息

共 0 页 15条页 < 1 > 前往 1 页

序号	hostip	percent	content	eventDate
1	192.168.1.124	0.14167835	Nov 20 09:11:18 WIN-QTTE6DHS81L.secisland.com MSWinEventLog 1 Security 23749 Wed Nov 20 09:11:19 2019 5158 Microsoft-Windows-Security-Auditing N/A N/A Success Audit WIN-QTTE6DHS81L.secisland.com 筛选平台连接 66185168	2019-11-20 09:11:18
2	192.168.1.124	0.14167835	Nov 20 09:12:24 WIN-QTTE6DHS81L.secisland.com MSWinEventLog 1 Security 23751 Wed Nov 20 09:12:24 2019 5158 Microsoft-Windows-Security-Auditing N/A N/A Success Audit WIN-QTTE6DHS81L.secisland.com 筛选平台连接 66185324	2019-11-20 09:12:24
3	192.168.1.124	0.14167835	Nov 20 09:12:33 WIN-QTTE6DHS81L.secisland.com MSWinEventLog 1 Security 23759 Wed Nov 20 09:12:33 2019 5158 Microsoft-Windows-Security-Auditing N/A N/A Success Audit WIN-QTTE6DHS81L.secisland.com 筛选平台连接 66185399	2019-11-20 09:12:33
4	192.168.1.124	0.14167835	Nov 20 09:23:55 WIN-QTTE6DHS81L.secisland.com MSWinEventLog 1 Security 23772 Wed Nov 20 09:23:55 2019 4624 Microsoft-Windows-Security-Auditing N/A N/A Success Audit WIN-QTTE6DHS81L.secisland.com 登录 66186908	2019-11-20 09:23:55

SPL统计异常IP (低频访问)

```
index="bp_dbor" limit 0,100
| fields msg,level,priority,dst_ip,alert_type,src_ip,dst_port,name,action,time
| lookup black_port.csv dst_port
| stats count(*) values[level] as level,values[priority] as priority,values[action] as action,values[alert_type] as alert_type,values[name] as name,values[msg] as msg,min(_time) as first_time,max(_time) as latest_time,values[dst_port] as dst_port,values[tag] as tag by src_ip,dst_ip | eval tag=CONCAT(tag,"") | search tag=""
```

9个事件耗时 0.074s [2021-09-10 17:12:44 至 2021-09-10 17:27:44]

事件(9) 统计信息(9)

msg	level	count	priority	dst_ip	alert_type	src_ip	first_time	name	dst_port	action	tag	latest_time
RemoteCst	WARNING	1	low	81.144.233.93	Access	103.157.26.254	1631265904000	Black List	3389	drop	black	1631265904000
RemoteCst	WARNING	1	low	58.251.21.200	Access	159.75.250.27	1631265968000	Black List	3389	drop	black	1631265968000
RemoteCst	WARNING	1	low	192.168.51.11	Access	180.169.252.124	1631265930000	Black List	445	drop	black	1631265930000
RemoteCst	WARNING	1	low	192.168.51.12	Access	180.169.252.124	1631265820000	Black List	445	drop	black	1631265820000
RemoteCst	WARNING	2	low	192.168.51.30	Access	180.169.252.124	1631265925000	Black List	445	drop	black	1631265930000
RemoteCst	WARNING	1	low	192.168.52.1	Access	180.169.252.124	1631265820000	Black List	445	drop	black	1631265820000
RemoteCst	WARNING	1	low	192.168.52.17	Access	180.169.252.124	1631265825000	Black List	445	drop	black	1631265825000
RemoteCst	WARNING	1	low	221.179.16.202	Access	223.247.210.140	1631265919000	Black List	3389	drop	black	1631265919000
RemoteCst	WARNING	1	low	58.251.33.226	Access	58.251.33.83	1631265919000	Black List	445	drop	black	1631265919000

SPL查询ddos攻击日志信息

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。

## 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。

## 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。



## 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。



## 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。





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](http://wtc.antiy.cn)