安信证券安全运营实践分享

李维春 安信证券安全总监

CIS 网络安全创新大会
Cyber Security Innovation Summit

目录

网络安全创新大会
Cyber Security Innovation Summit

一、公司介绍

二、安全建设历程

三、安全运营

四、安全运营心得

- 公司总部设于深圳，成立于2006年
- 在北京、上海、广州、汕头和佛山等地45家分公司、333家证券营业部
- 控股股东为国家开发投资公司控股的国投资本股份有限公司
- 四家控股子公司：安信国际、安信乾宏投资、国投安信期货、安信证券投资
- 公司具有证券行业全业务牌照，2009-2018年连续10年获A级以上评级

2015年-2016年

快速止血阶段

1、全面风险评估，制定未来三年工作规划
2、互联网高危资产梳理及高危风险处置
3、建立自主渗透测试能力及漏洞管理机制
4、建立SDL管理机制及开发规范

2017-2018年

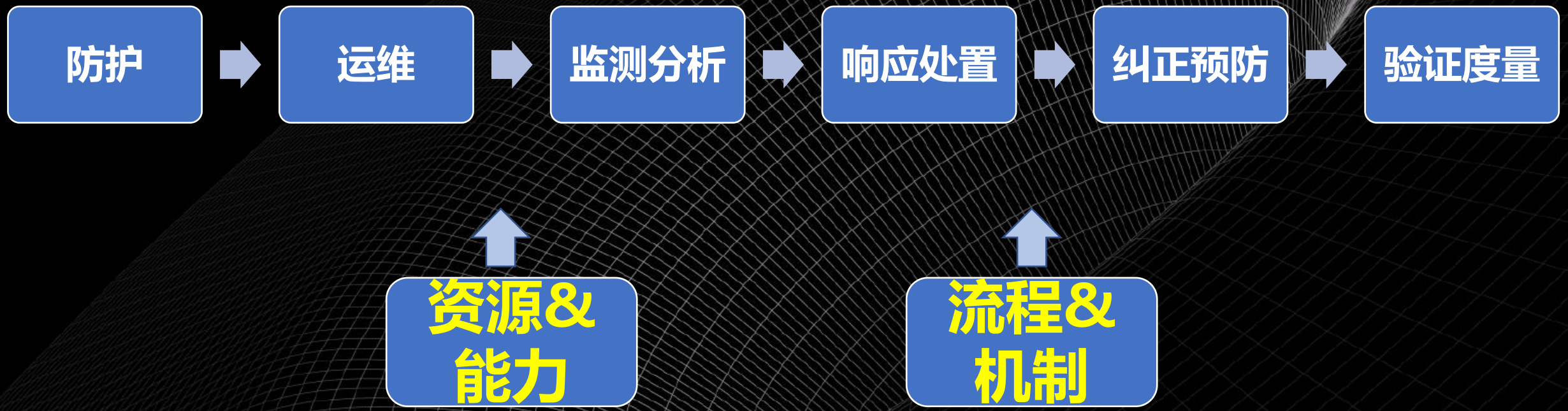
全面建设阶段

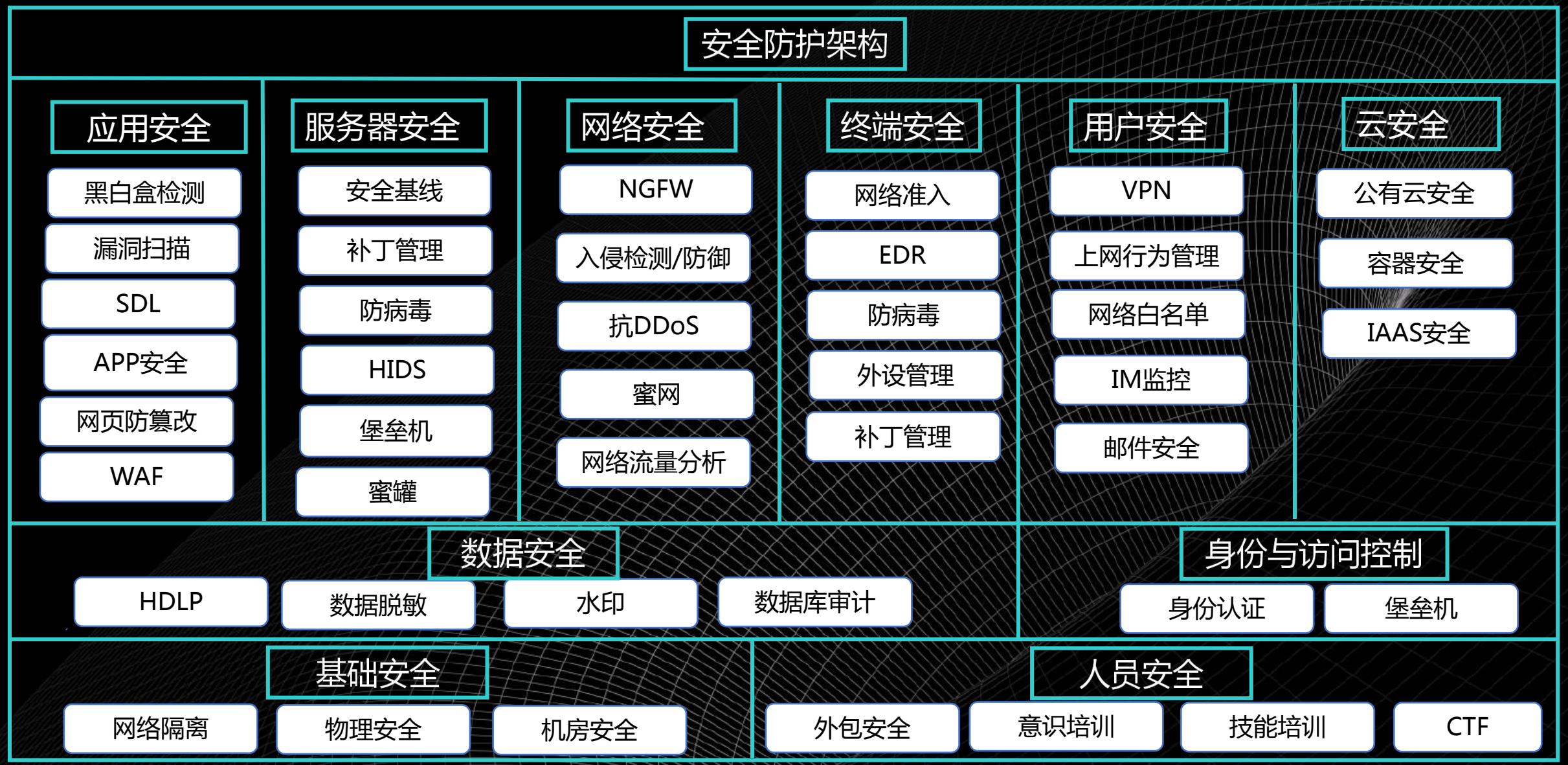
1、基于纵深防御的理念，分层建设安全运营中心、威胁感知与分析、WAF、IPS等手段
2、建立信息安全管理体系，通过ISO27001认证
3、建立安全意识培训体系及考核机制
4、夯实技术实力，代表国投集团参加央企首届网络安全攻防大赛并取得优良成绩

2019年-

优化提升阶段

1、通过护网攻防演练、红蓝对抗、安全众测等检查机制运转的有效性，不断提升安全运营能力
2、安全运营流程化、规范化管理
3、管理制度更新优化
4、DevSecOps、容器云安全、安全沙箱等新技术落地


防护
运维
监测分析
响应处置
纠正预防
验证度量
资源&
能力
流程&
机制


安全防护架构
应用安全
黑白盒检测
漏洞扫描
SDL
APP安全
网页防篡改
WAF
服务器安全
安全基线
补丁管理
防病毒
HIDS
堡垒机
蜜罐
网络安全
NGFW
入侵检测/防御
抗DDoS
蜜网
网络流量分析
终端安全
网络准入
EDR
防病毒
外设管理
补丁管理
用户安全
VPN
上网行为管理
网络白名单
IM监控
邮件安全
云安全
公有云安全
容器安全
IAAS安全
数据安全
HDLP
数据脱敏
水印
数据库审计
身份与访问控制
身份认证
堡垒机
基础安全
网络隔离
物理安全
机房安全
人员安全
外包安全
意识培训
技能培训
CTF

- 健康度检查

①检查Sensor安全监测功能是否正常运行

②检查Sensor到管理后端的网络通路是否通畅

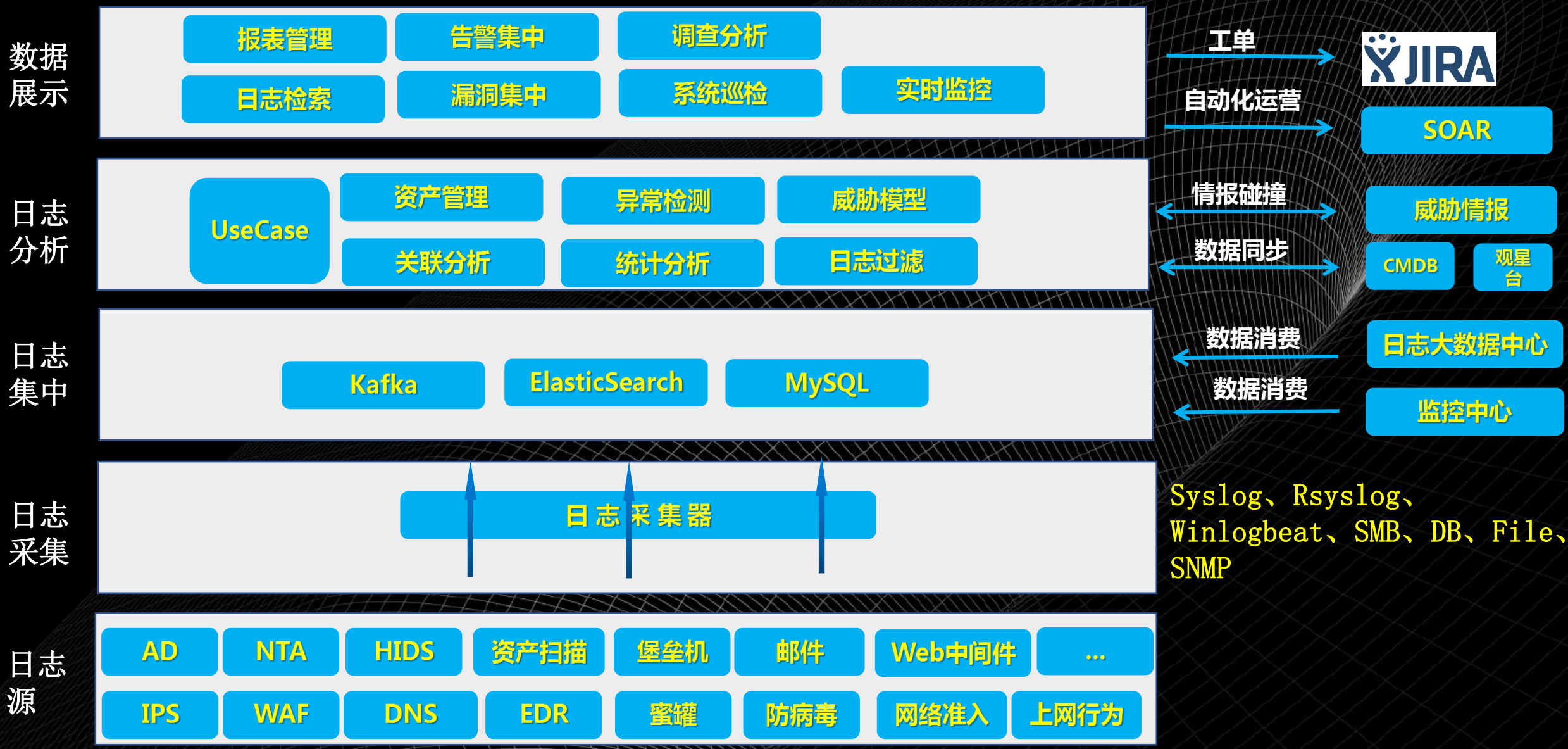
③检查Sensor所产生的告警信息到SOC平台的信息采集是否正常运行

④检查告警通知（邮件、短信与可视化 展示平台）是否正常运行

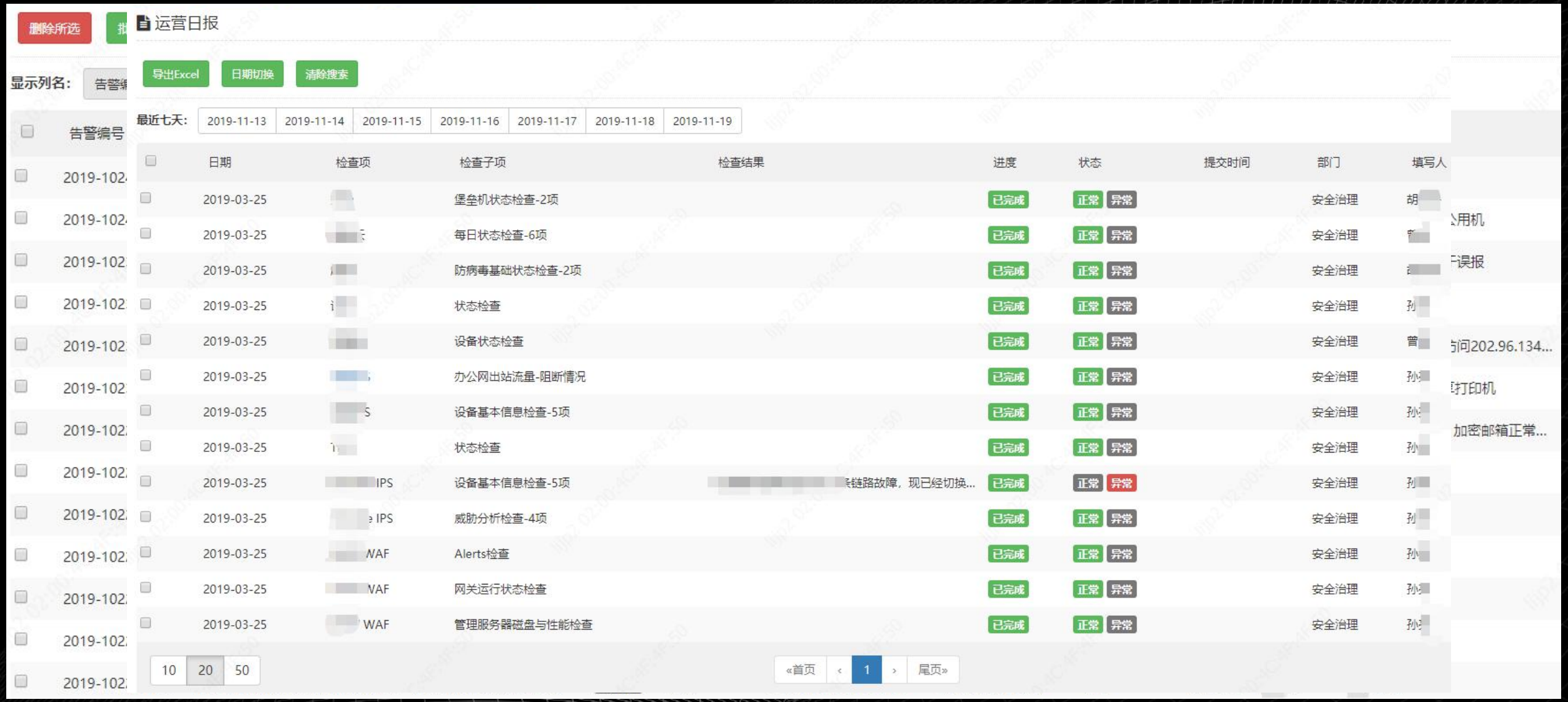
⑤检查Sensor、系统接入点是否变更、被规避

⑥检查流程控制点是否生效、发生变更、被规避

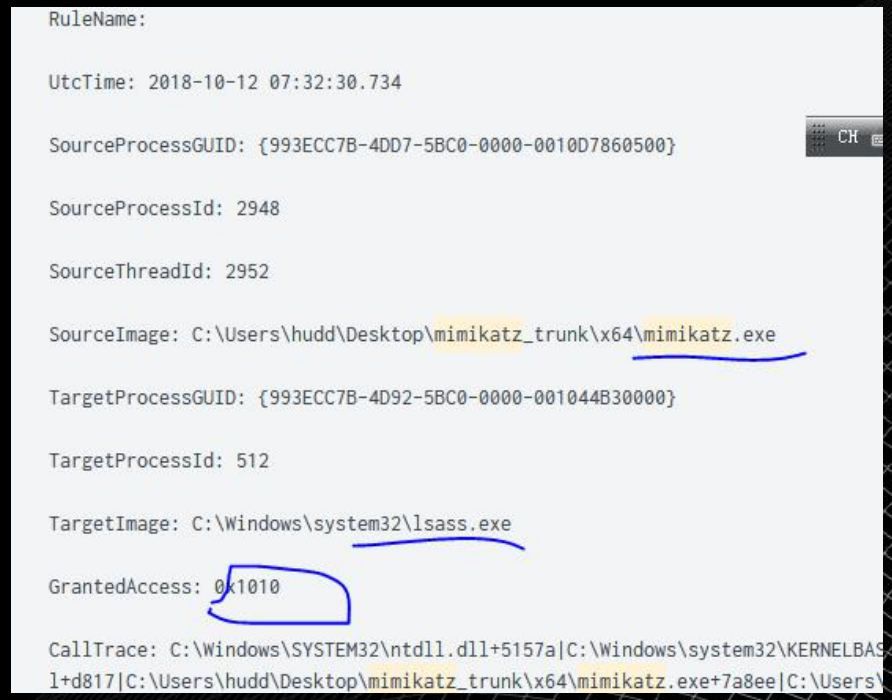
- 健康度问题纠正和预防


数据展示
报表管理
告警集中
调查分析
日志检索
漏洞集中
系统巡检
实时监控
日志分析
UseCase
资产管理
异常检测
威胁模型
关联分析
统计分析
日志过滤
日志集中
Kafka
ElasticSearch
MySQL
日志采集
日志采集器
日志源
AD
NTA
HIDS
资产扫描
堡垒机
邮件
Web中间件
...
IPS
WAF
DNS
EDR
蜜罐
防病毒
网络准入
上网行为
工单
JIRA
自动化运营
SOAR
情报碰撞
威胁情报
数据同步
CMDB
观星台
数据消费
日志大数据中心
数据消费
监控中心
Syslog、Rsyslog、
Winlogbeat、SMB、DB、File、
SNMP

安全告警集中展示和处理



UseCase 1：Mimikatz横向渗透检测



日志来源：Sysmon

检测规则：

```
index=__your_sysmon_data__ EventCode=10
TargetImage="C:\\WINDOWS\\system32\\lsass.exe"
(GrantedAccess=0x1410 OR
GrantedAccess=0x1010 OR
GrantedAccess=0x1438 OR
GrantedAccess=0x143a OR
GrantedAccess=0x1418)
CallTrace="C:\\windows\\SYSTEM32\\ntdll.dll+*|C:\\windows\\System32\\KERNELBASE.dll+20edd|UNKNOWN(*)"
| table _time hostname user SourceImage GrantedAccess
```

UseCase 2：RDP远程登录VIP用户告警

*告警详情

名称	数值
设备区域名	[redacted]0.255
源资产名称	[redacted]0.255
源地址	[redacted].38
访问结果	/Failure
访问方法	网络:用户或计算机登录到此计算机上从网络。
源区域名	[redacted].255
设备地址	[redacted].240
设备主机名	[redacted]
设备资产名称	[redacted].240
用户名称	[redacted]
用户SID	[redacted]
源主机名	[redacted]

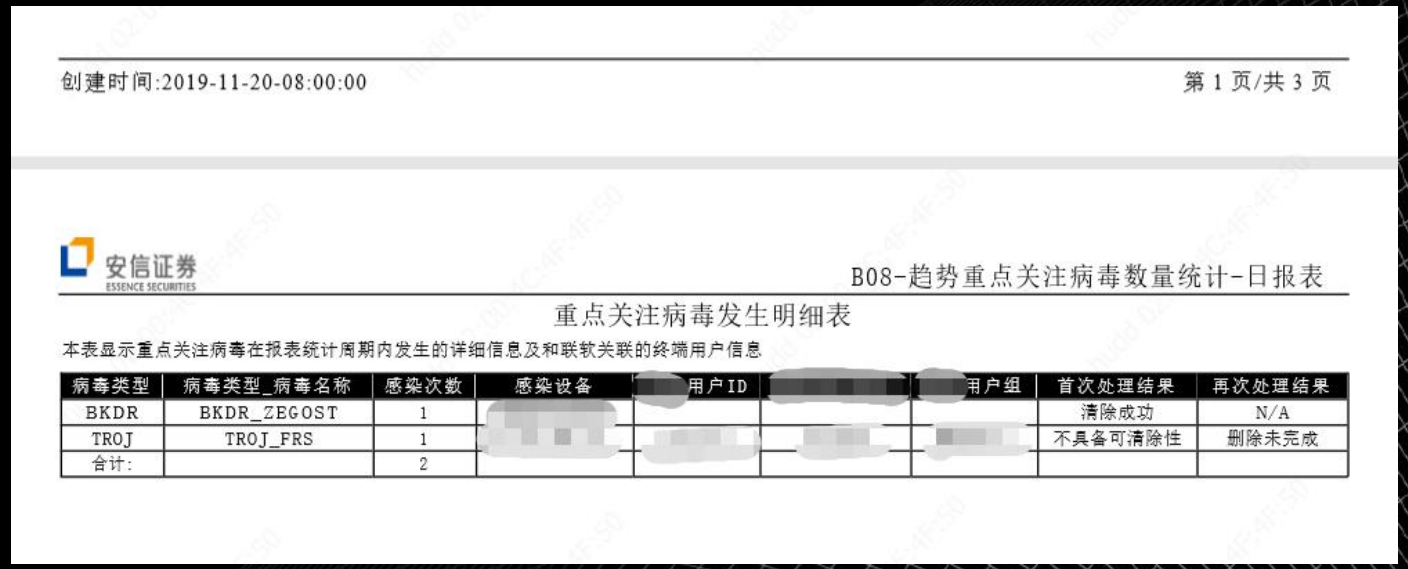
日志来源：Windows Security Event Log&Sysmon

检测规则：

```
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4624
        LogonType: 10

SourceNetworkAddress:
            - "::1"
            - "127.0.0.1"
    condition: selection
falsepositives:
    - Unknown
level: high
```

UseCase 3：重点病毒告警



创建时间:2019-11-20-08:00:00　　第 1 页/共 3 页

安信证券 ESSENCE SECURITIES

B08-趋势重点关注病毒数量统计-日报表

重点关注病毒发生明细表

本表显示重点关注病毒在报表统计周期内发生的详细信息及和联软关联的终端用户信息

病毒类型	病毒类型_病毒名称	感染次数	感染设备	用户ID	[redacted]	用户组	首次处理结果	再次处理结果
BKDR	BKDR_ZEGOST	1	[redacted]	[redacted]	[redacted]	[redacted]	清除成功	N/A
TROJ	TROJ_FRS	1	[redacted]	[redacted]	[redacted]	[redacted]	不具备可清除性	删除未完成
合计:		2						

日志来源：防病毒数据库
检测规则：未删除\隔离成功的蠕虫、木马病毒

合规型

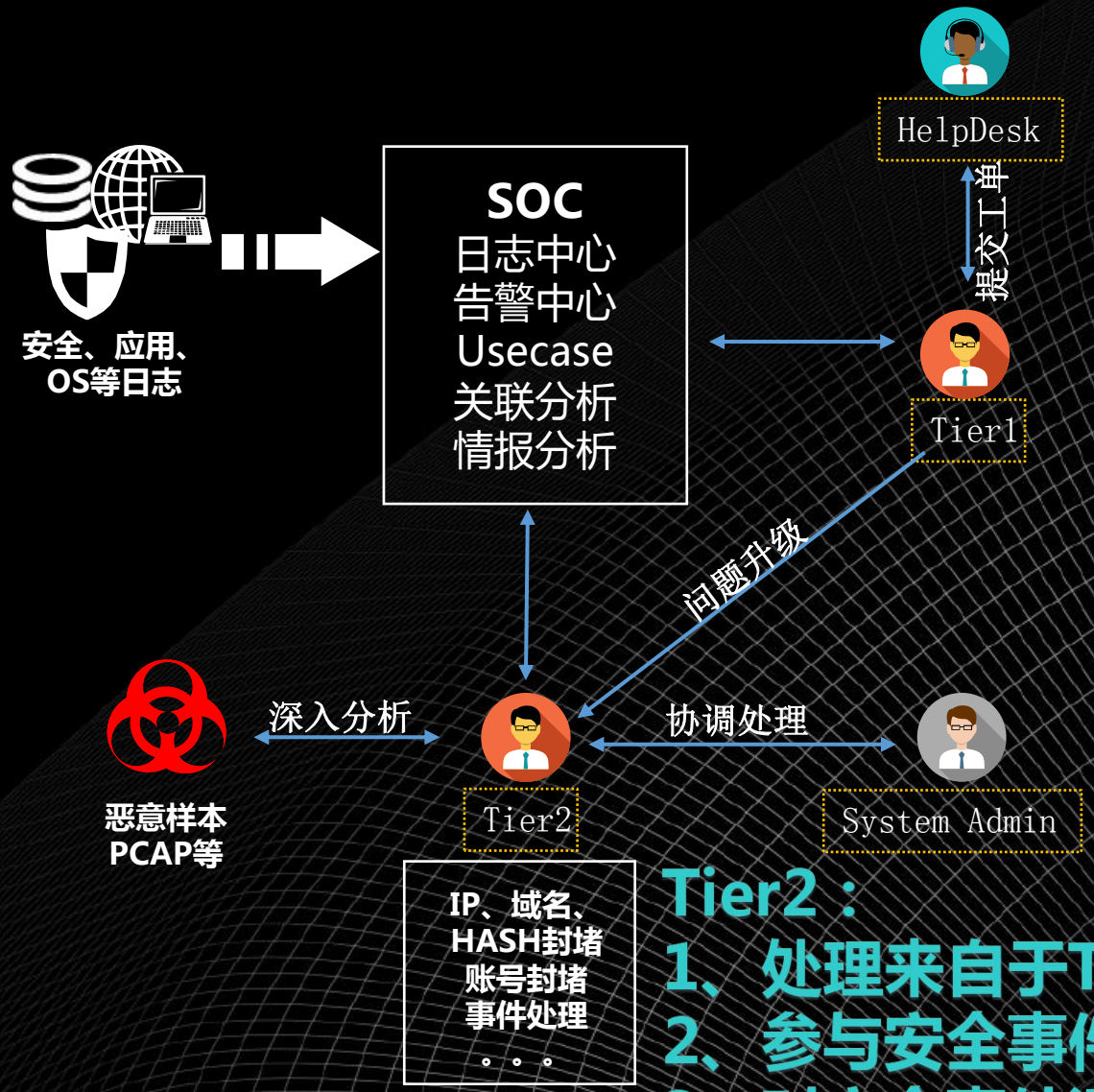
- 依据规范制度，制订检测规则
- 可以包括覆盖面、健康度、正常率

攻防型

- 单个安全设备的检测
- 攻击路径的检测(例如ATT&ACK)
- 奇技淫巧的检测

补充

- 攻防演练、检查审计、事件处理中发现的问题
- 情报监测



Tier1：

1、按照SOP实时监控各类系统告警

2、安全系统、日志发送等各类健康度监测

3、处理简单的告警，提交工单给服务台

4、如遇困难，升级到Tier2

Tier2：

1、处理来自于Tier1升级的告警，进行深入分析

2、参与安全事件调查处理，协调系统负责人处理

3、对安全事件深入分析，完善安全检测与防护策略

4、UseCase的制定、测试及发布

不合规

- 纠正
- 挖掘不合规原因，纳入ITIL“问题管理”

规则不清，或没有规则

- 商定规则
- 审批通过
- 执行改进，或专项任务实施改进

ITIL“问题管理”

- 每周回顾，寻找共性、多发常发的问题
- 组织分析原因和解决方案
- 审批通过
- 专项任务实施改进

- 结果验证

①红蓝对抗（计划中）

②每年2次攻防演练

③每年行业攻防演练

④每年3-4次专项审计（系统、流程、人）

- 度量指标

① 防护覆盖面：安全工具覆盖率、正常率100%

② 运维：系统、流程健康度100%

③ 监测分析：高危风险30分钟发现率100%

④ 响应处置：高危风险及时修复率100%

⑤ 纠正预防：重复问题发生数每年少于5%

3.7 资源和能力

2016年安信证券首届CTF大赛

2017年安信证券第二届CTF大赛

2018年安信证券代表国投集团参加央企首届网络安全攻防大赛

2018年安信证券第三届网络安全技能大赛

70%：在好的平台上实战

\+

20%：以老带新

\+

10%：培训、知识库

复盘对标

- 每日运营开例会、存纪要
- 每周挖掘问题
- 每季度走访学习同行

验证

- 处置人和验证人分开
- 定期有审计、攻防演练来验证

评价

- 基于度量指标，以达成率、提升率进行评价
- 安全团队与系统负责人的安全绩效一致
- 奖励主动改进行为

自动化

- 逐步实现自动化，让干活的人更开心

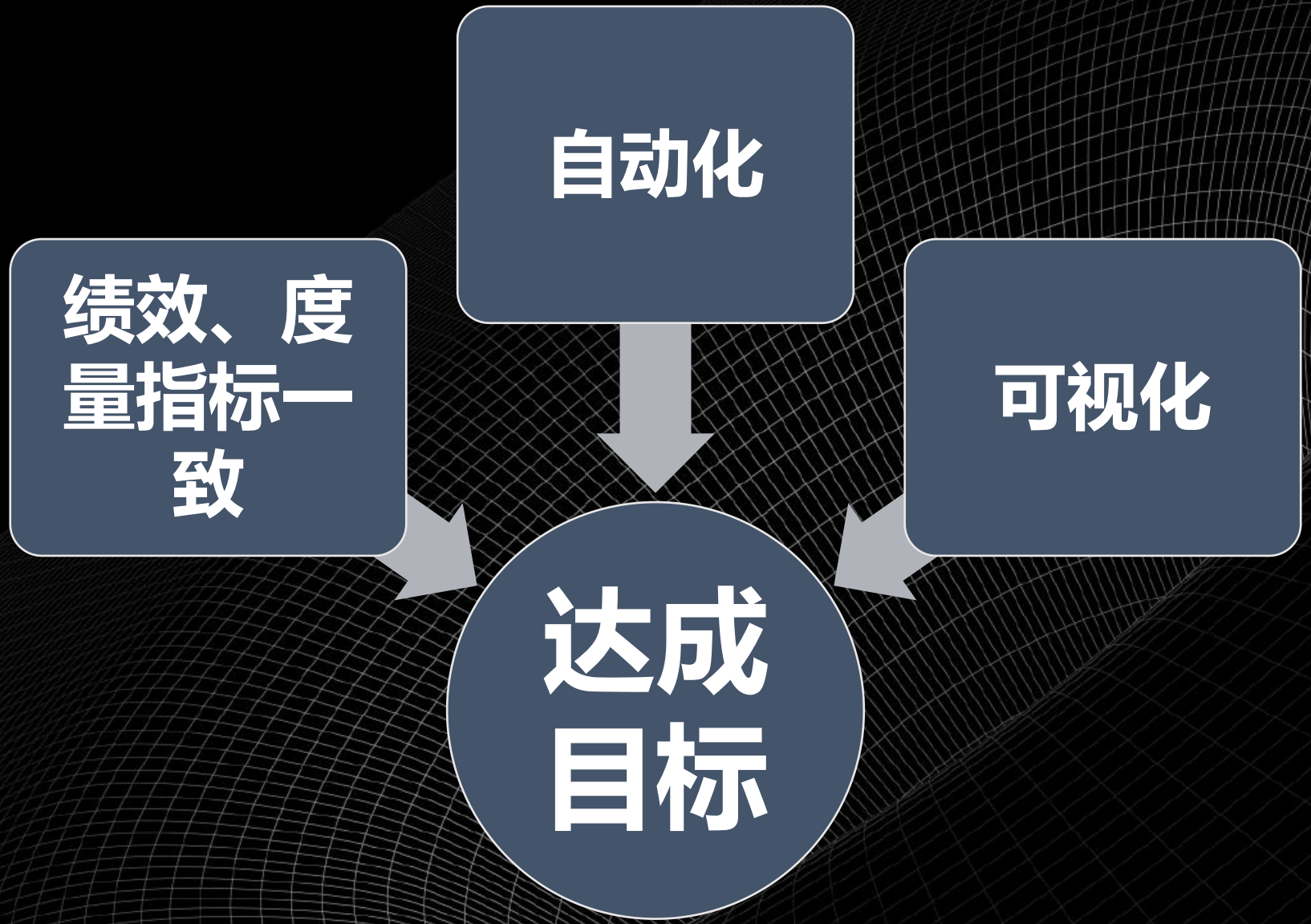
一、以终为始，强调解决问题、可执行，强调解决问题和预防问题两手抓

二、尊重人性。人是最靠不住的，但是安全运营也最离不开人

三、尊重墨菲定律，尽快堵住可能出问题的口子

四、不要被新概念、新工具迷惑

五、以攻促防，让攻防演练成为常态


自动化
绩效、度量指标一致
可视化
达成目标

网络安全创新大会
Cyber Security Innovation Summit

THANKS