安全运营思考及实践

吴佳伟

兴业证券
INDUSTRIAL SECURITIES

目录

背景

兴业证券 INDUSTRIAL SECURITIES

大环境

- 安全形势日益严峻
- 安全工作备受关注

人

- 专业安全人员稀缺
- 安全规模化管理难

设施

- 基础设施建设普遍完成
- 安全态势感知依然很难

安全运营挑战

在安全形势严峻、安全人员稀缺、安全告警海量的情况下，如何及时、有效、准确发现安全风险并高效响应?

思路上改变：安全运营“四化”

体系化建设

- **系统性设计、整体性协同**

如：安全生命周期管理体系

工程化实施

- **规范化、标准化、自动化**

如：SOAR安全自动化编排技术、“安全分析师”式场景化分析

平台化运营

- **集中整合、综合分析、整体感知、调度协同**

如：安全态势感知平台、SOC

全面化覆盖

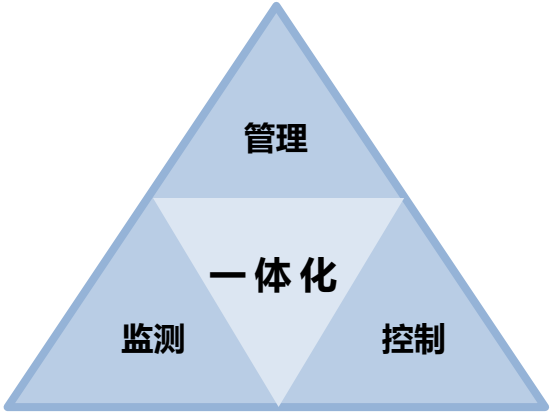
- **全覆盖、无死角**

如：安装率、覆盖面、有效性

安全运营体系

自主可控

灵活整合安全能力、规划安全任务、定义响应流程



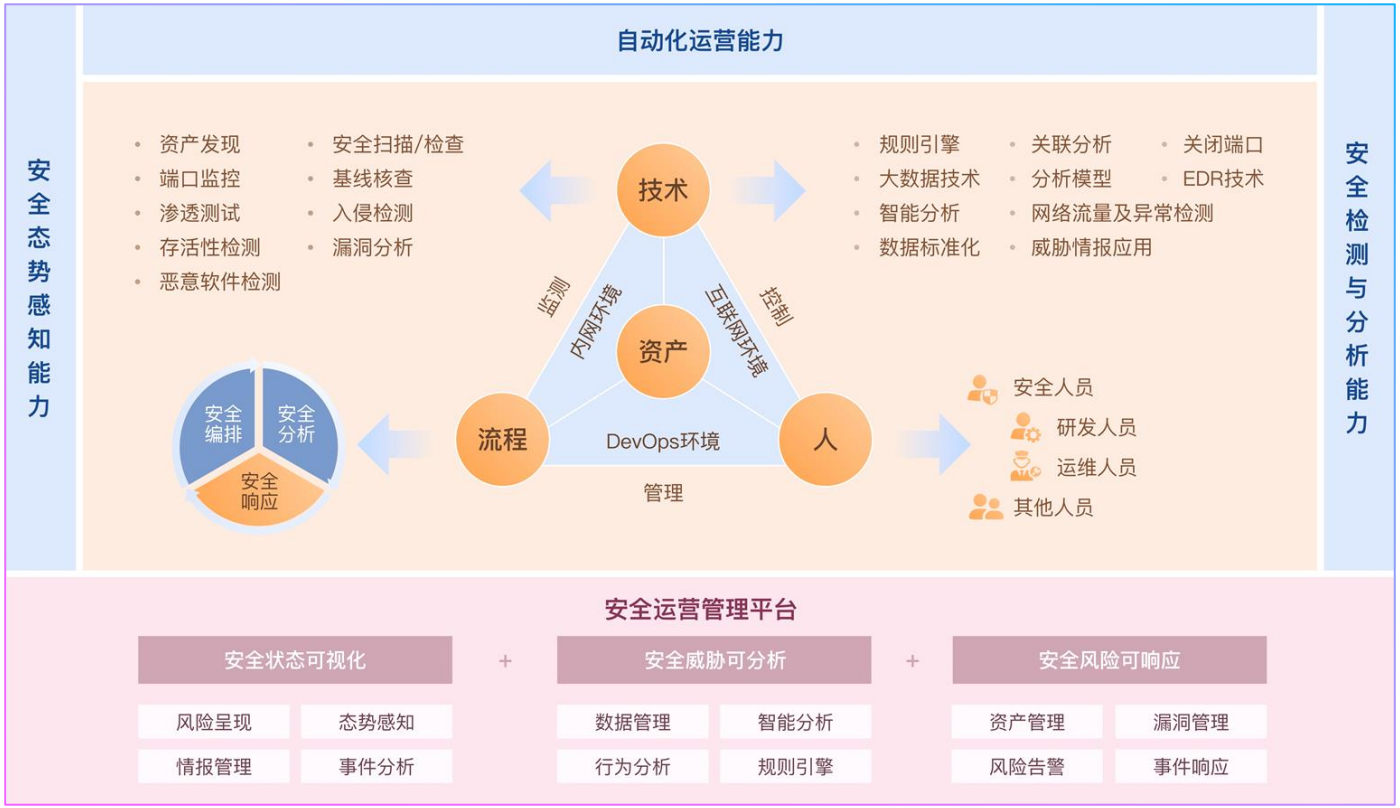
态势感知

整合海量异构数据，设计适用于自身公司的安全场景、模型和指标体系

规模化管理

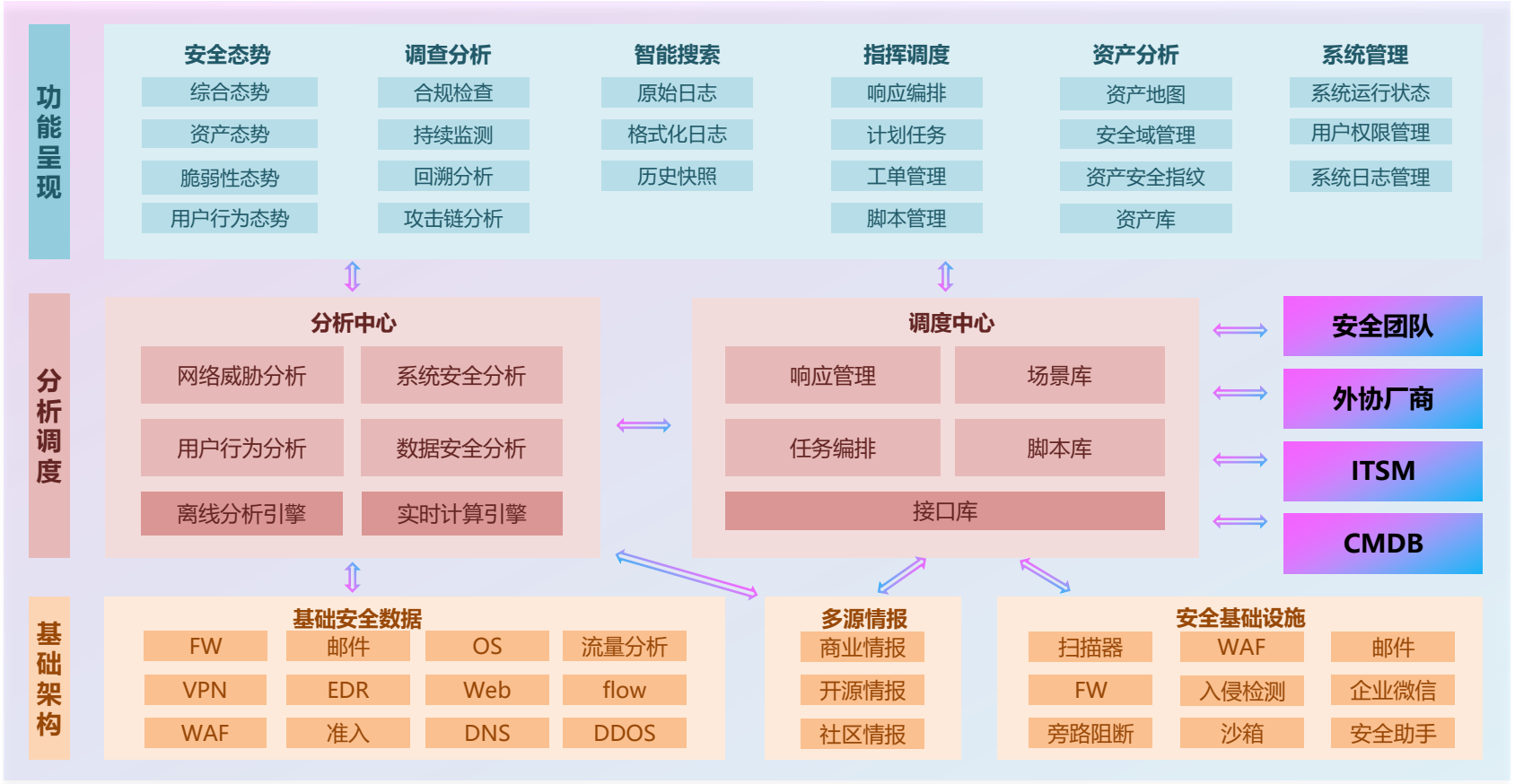
安全运营流程规范化、标准化，自动化驱动关键流程、关键步骤高效运转

安全运营体系：一个平台、三种能力

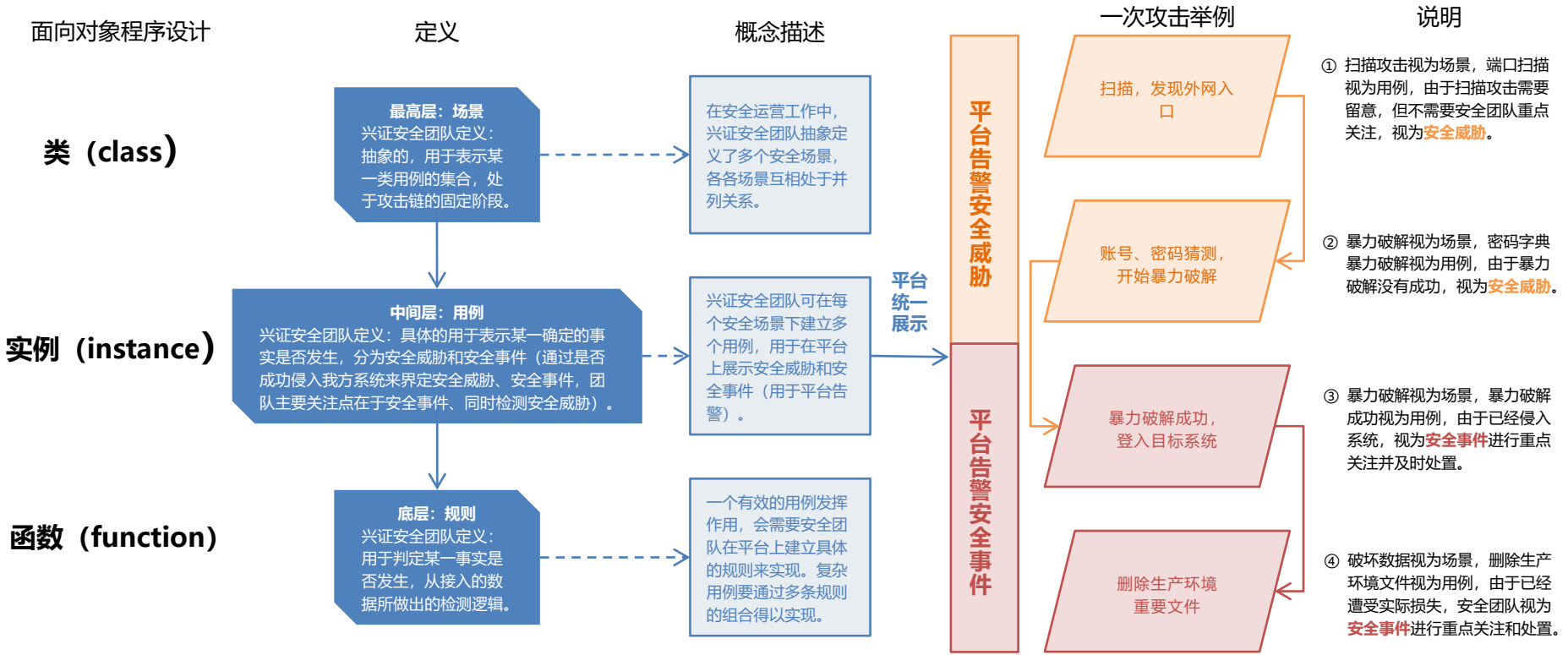


目录

安全运营管理平台逻辑架构



安全运营管理平台安全分析模型



安全运营管理平台视图

兴业证券 INDUSTRIAL SECURITIES

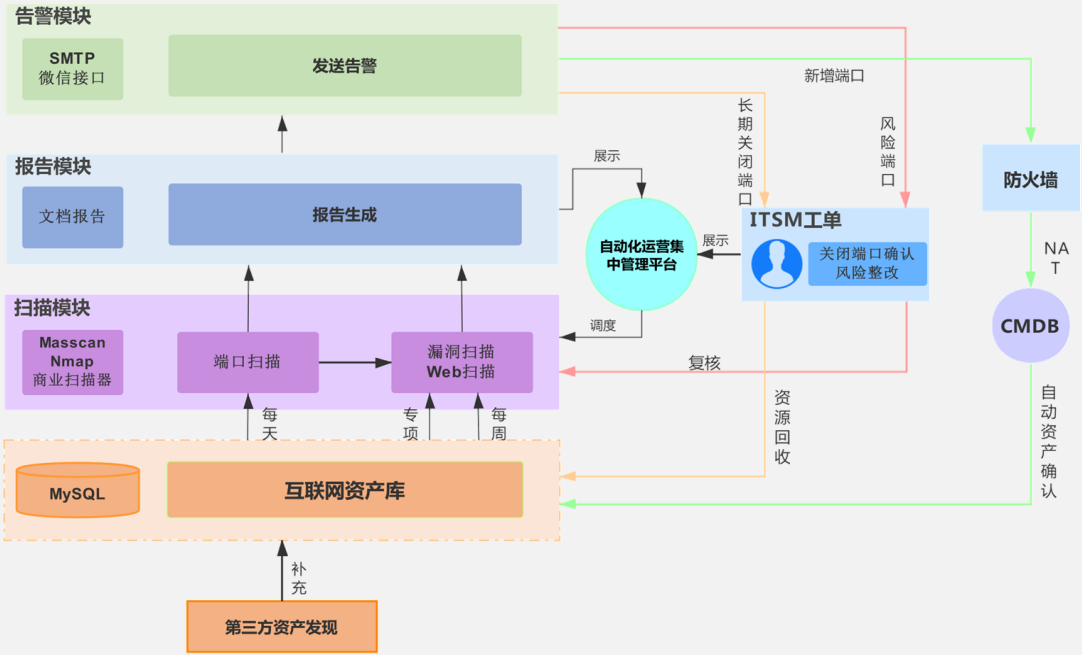
管理者视图

安全人员视图

安全检测与响应矩阵


事前
事中
事后
纵深检测与防御
用户
外包安全管理
身份认证
口令管理
特权帐户监控
堡垒机
终端安全
应用
安全生命周期
防篡改
安全测试
信道加密
蜜罐
应用防护
数据
数据脱敏
水印
DLP
数据库审计
API安全
邮件安全
主机
安全基线
漏洞扫描
补丁管理
防病毒
HIDS
EDR
虚拟
云平台监控
VPC
虚拟流量监控
主机加固
网络
防火墙
网络准入
入侵检测
威胁情报应用
高级威胁
抗DDOS

互联网环境安全自动化运营



自动化闭环管理：资产管理、风险检测、风险处置

互联网信息资产管理

- **基于NAT表自动动态更新互联网资产库**，包含IP、端口、协议、服务、应用、责任人等信息；
- **全端口自动化检测新增、关闭、活动端口**，结果入库。

互联网安全风险检测

- **实时自动监控**重要网站服务异常
- **每天自动监测**新增端口资产漏洞
- **每周自动检测**全量外网资产漏洞
- **每月例行测试**全量外网资产
- **每年深度测试**全量外网资产

互联网安全风险处置

- **自动邮件告警**系统责任人
- **自动创建**漏洞整改**工单任务**
- **处理状态**于安全风险集中管理平台**可视**

互联网环境安全自动化运营

多层次

- 分配周期合理
- 满足安全合规
- 发现风险及时

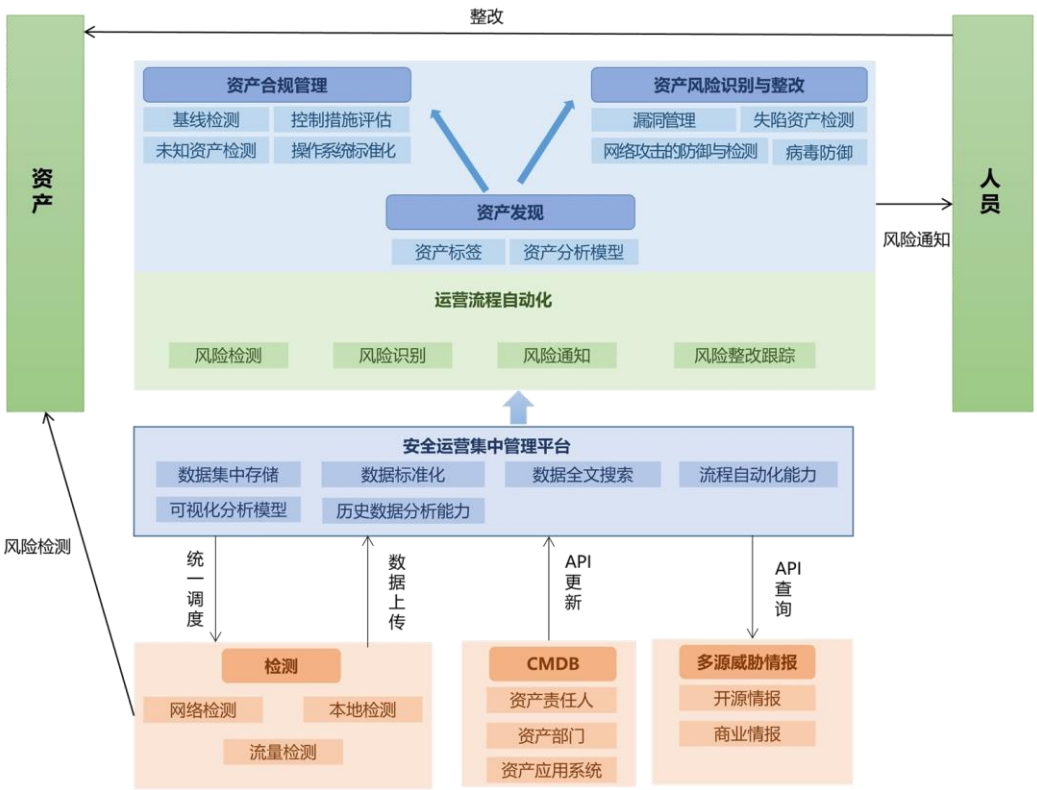
全范围

- 集团面向外网服务器
- 集团外网应用系统
- 集团面向外网APP

高强度

- 检测工具、服务异构
- 检测次数高频

内网环境安全自动化运营



内网信息资产管理

- **本地客户端**自动探测内网资产存活性
- **远程网络**自动检测内网资产存活性
- **网络流量**自动发现内网未知资产

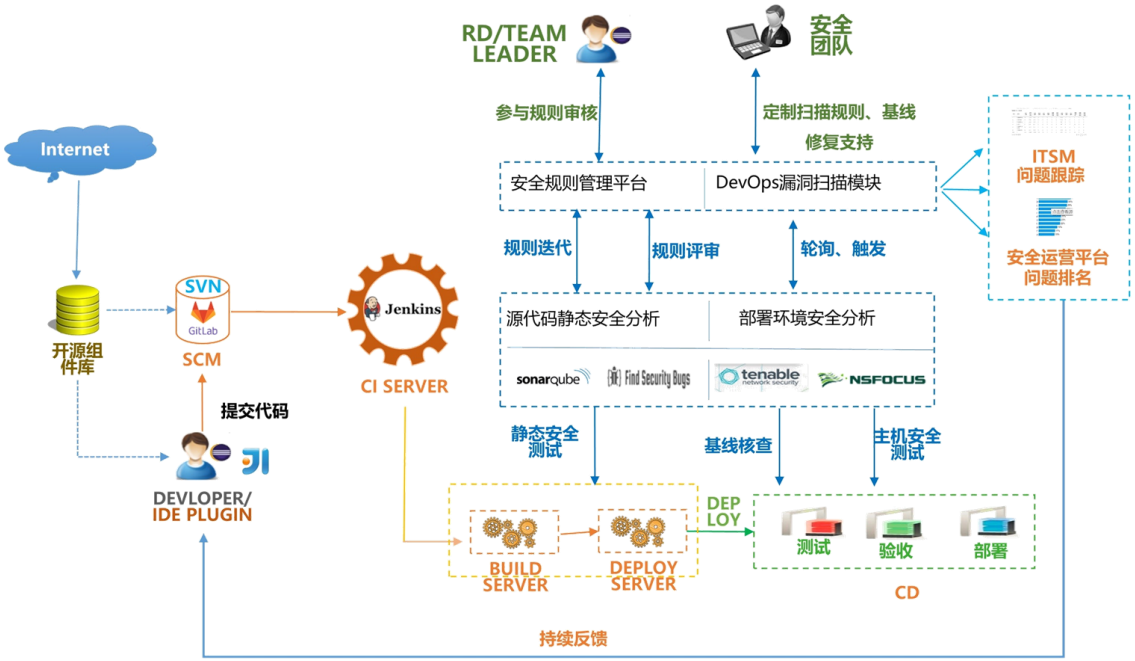
内网安全风险检测

- **每周自动核查**全量内网安全基线
- **每周自动检测**全量内网安全漏洞
- **每半年自动检测**全量内网弱口令

内网安全风险处置

- **自动邮件告警**系统责任人
- **自动创建**漏洞整改**工单任务**
- **处理状态**于安全风险集中管理平台**可视**

DevOps环境安全自动化运营



源代码安全审计

- 开发集成工具调度源代码安全检测引擎**自动静态分析源代码**

部署环境安全检测

- DevOps平台监控系统部署完成情况，**自动调度安全检测引擎实施部署环境安全评估**

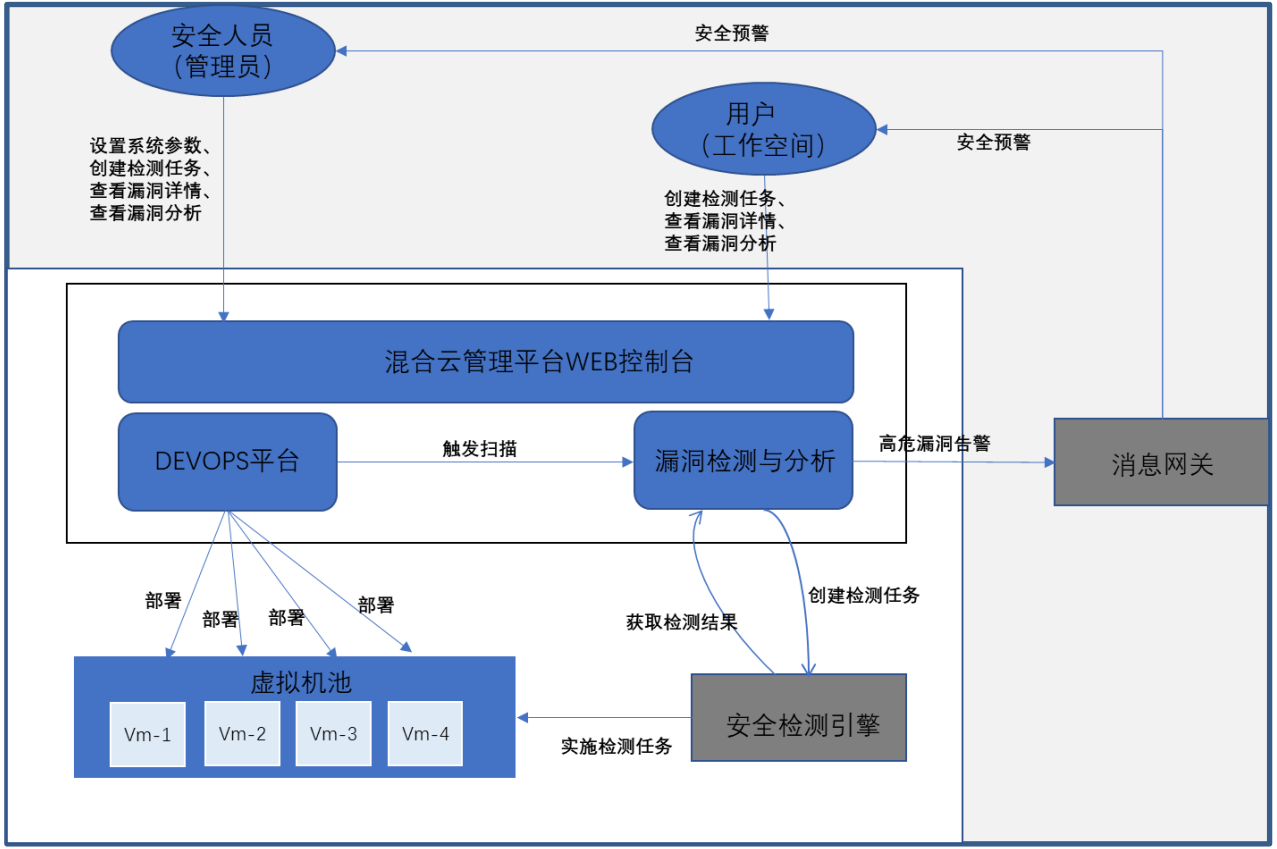
安全风险处置

- **自动邮件告警**系统责任人
- **自动创建**漏洞整改**工单任务**
- **处理状态**于安全风险集中管理平台**可视**

DevOps环境安全自动化运营

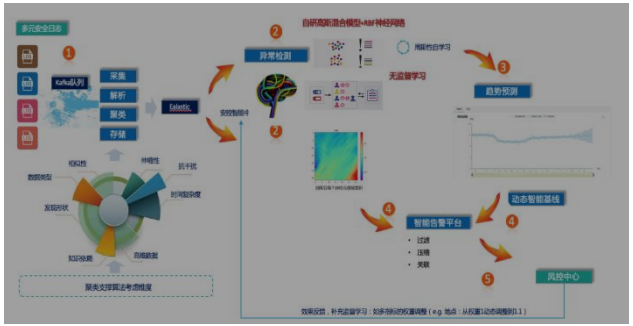
兴业证券 INDUSTRIAL SECURITIES

示例：DevOps部署环境安全检测：人、DevOps平台、安全引擎、虚拟机池有机结合



目录

安全风险感知能力显著提升



安全运营集中可视

安全监测、管理和控制工作统一平台化管理，对安全态势和运营过程进行集中可视化

安全设施集中关联

对异构安全设施进行平台化整合，安全数据集中关联分析，安全告警大幅降噪，精准度大幅提高

安全处置高效协同

自动化对接平台外围系统，实现快速协同响应，安全事件平均处置时间大幅缩短

安全控制精准度进一步提高

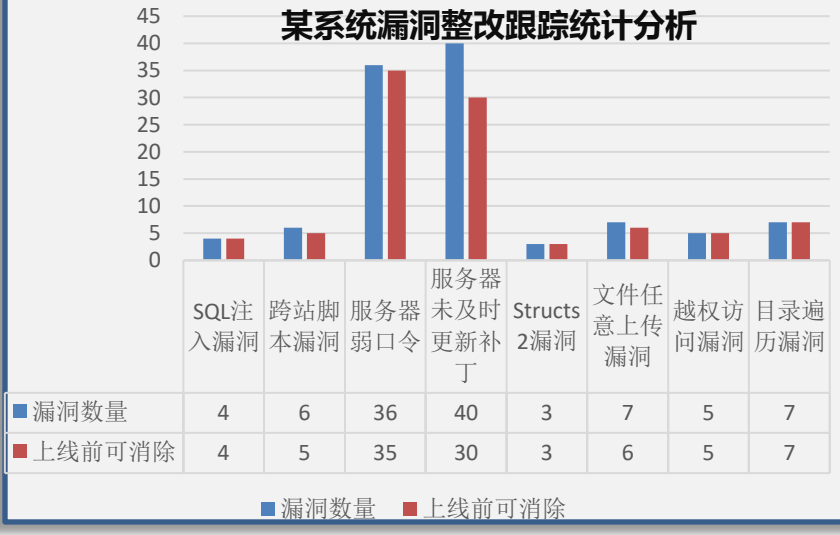
兴业证券 INDUSTRIAL SECURITIES

嵌入系统建设各阶段的安全控制活动高效运转

- 安全需求分析
- 源代码安全审计
- 架构安全评审
- 上线前安全测试
- 安全基线核查

……

安全控制活动更加精准，大幅降低了漏洞暴露时间和整改成本



	对比1	对比2	对比3	对比4
实践前	系统上线或运行前安全漏洞一直暴露在外	仅安全人员单方面实施安全措施，效率低	安全漏洞在系统上线和运行阶段集中暴露，影响系统上线进度	安全漏洞在后期发现，需重新安排人力和时间，整改成本高
实践后	从系统需求分析阶段开始发现和解决安全漏洞，**降低漏洞暴露时间**	驱动业务部门和研发部门人员一起参与安全措施的实施，**提高安全措施的实施效率**	大部分安全漏洞在上线前已解决，**保障系统上线进度**	在系统开发生命周期中同步解决安全问题，**安全漏洞整改成本低**

安全规模化管理能力有效提升

兴业证券 INDUSTRIAL SECURITIES

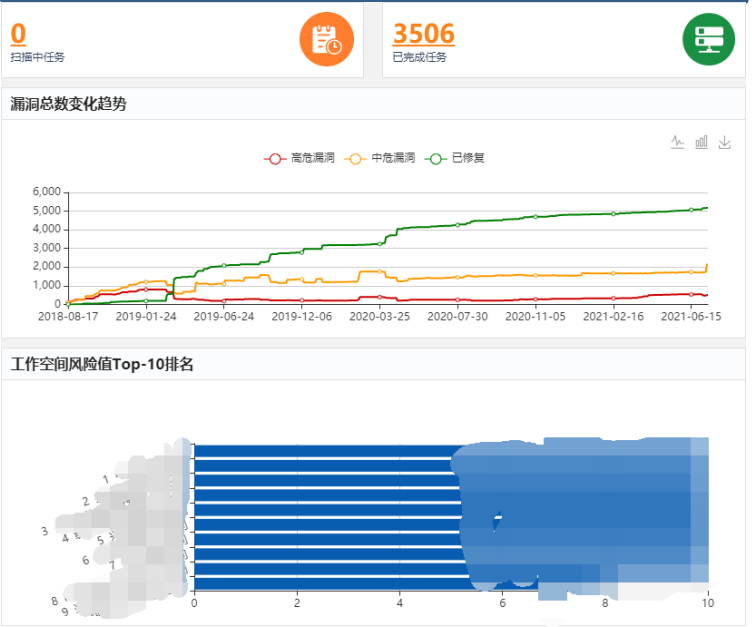
提升了安全标准化水平和安全运营效率，实现了安全规模化管理

覆盖**7000+**个信息资产，建立自动化场景**20+**个，编排任务**100+**个

响应时间：**天降至分钟级别**

覆盖包含**10**个子公司在内的**整个集团互联网信息资产**

基于资产的自动化安全运营体系	建立自动化编排任务数（个）	安全任务执行次数（次）	覆盖资产（个）	处置漏洞数（个）	发现并处置威胁事件数（个）
互联网环境	25	1011	1000+	1000+	10+
内网环境	72	2523	5000+	8000+	90+
DevOps环境	6	918	1000+	1000+	10+
合计	103	4452	7000+	10000+	110+



总结

兴业证券 INDUSTRIAL SECURITIES

安全运营一体化

- 监测、管理、控制一体
- 发现到响应的闭环管理

安全自主可控

- 安全流程灵活定义
- 安全体系自主设计
- 安全平台自主研发

安全运营自动化

- 自动化安全技术应用
- 运营的效率大幅提升
- 实现安全规模化管理

安全态势有效感知

- 安全风险精准识别
- 安全风险运营可视
- 安全管理决策支撑

展望

安全运营对整个技术体系的成熟度要求很高

自动化解决不了所有问题，持续的人工介入是非常必要的

数据整合能力、分析能力、协同能力是三个核心建设方向

谢 谢