网络安全创新大会
Cyber Security Innovation Summit

一体化安全架构之路

何艺 2020

个人介绍

何艺

完美世界资深安全总监

- 16年甲方安全经验，9年安全团队管理经历
- 聚焦企业安全建设、安全架构、零信任、安全分析和响应等领域
- freebuf专栏和公众号“小议安全”，有安全招聘、职业相关文章
- 2015年开始研究和实施零信任，零信任产业标准工作组专家、CAS云安全联盟专家、零信任认证CZTP审核专家组、零信任国标专家组
- 蓝星安全联盟成员

个人微信

个人公众号

议题

- 安全思想转变之路
- 一体化安全架构设计
- 运营实例
- 踩坑风险

我理解的一体化安全架构

- 将人、制度、流程、安全系统，结合业务情况通盘考虑和规划，形成一个整体，彼此互为依托，相互支持，相互协作。

思维的转变

- 第一课：甲方安全合规的教育

感受

- 无法落地的制度和流程文档
- 彼此独立的安全系统
- 没法处理的海量报警

安全的价值体现在哪里？

思维的转变

- 第二课：APT教你做检测

From: [redacted]@perfectvworld.com]
Sent: [redacted] 12:57
To: [redacted] <[redacted]@perfectworld.com>
Subject: (URGENT) PWE Account Validation & Security

Hello [redacted],

We would like to inform you regarding our new global policy of secure document handling and account validation.
From now on we require regular validation and renewal of domain accounts to ensure full safety of our networks.

To validate your current account ([redacted]) you have to login at our ADFS page, by clicking the following link:

ADFS: http://[redacted].perfectvworld.com/[redacted]

Once you complete the login you will see a message that your account has been successfully renewed and validated.

IMPORTANT: Please read our latest handling policy for internal documents.

You can download the document at:

Document: http://[redacted].perfectvworld.com/[redacted]/PWE_SecurityValidationPolicy_2016.docm

The document also includes step by step validation instructions for accounts in case you are having troubles.

P.S: If you have any problems validating your account or viewing secure documents, please do not hesitate to reply to this email.

Best Regards,

[redacted]

思维的转变

- 第二课：APT教你做检测

用户

- 账号身份对应问题
- 账号权限回收问题
- 账号权限授权问题

终端设备

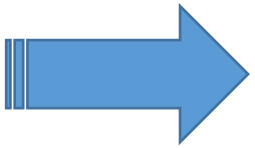
- 终端归属关系问题
- 终端网络位置问题
- 终端安全状态问题
- 终端网络权限控制
- 应急响应问题
- 数据泄露问题

应用

- 应用安全漏洞风险
- 应用权限管控风险
- 应用敏感操作问题

服务器

- 服务器安全漏洞风险
- 服务器安全事件发现能力
- 服务器端口暴露问题



感受

- 分析一定会漏
- 响应一定会慢
- 投入一定不够

安全如何低成本，高回报？

思维的转变

- 第三课：来自业务的爱

什么破软件啊，根本不能用

用户体验极差

感受

- 吐槽必有因
- 影响效率=断人钱财

安全如何推动？

思维的转变

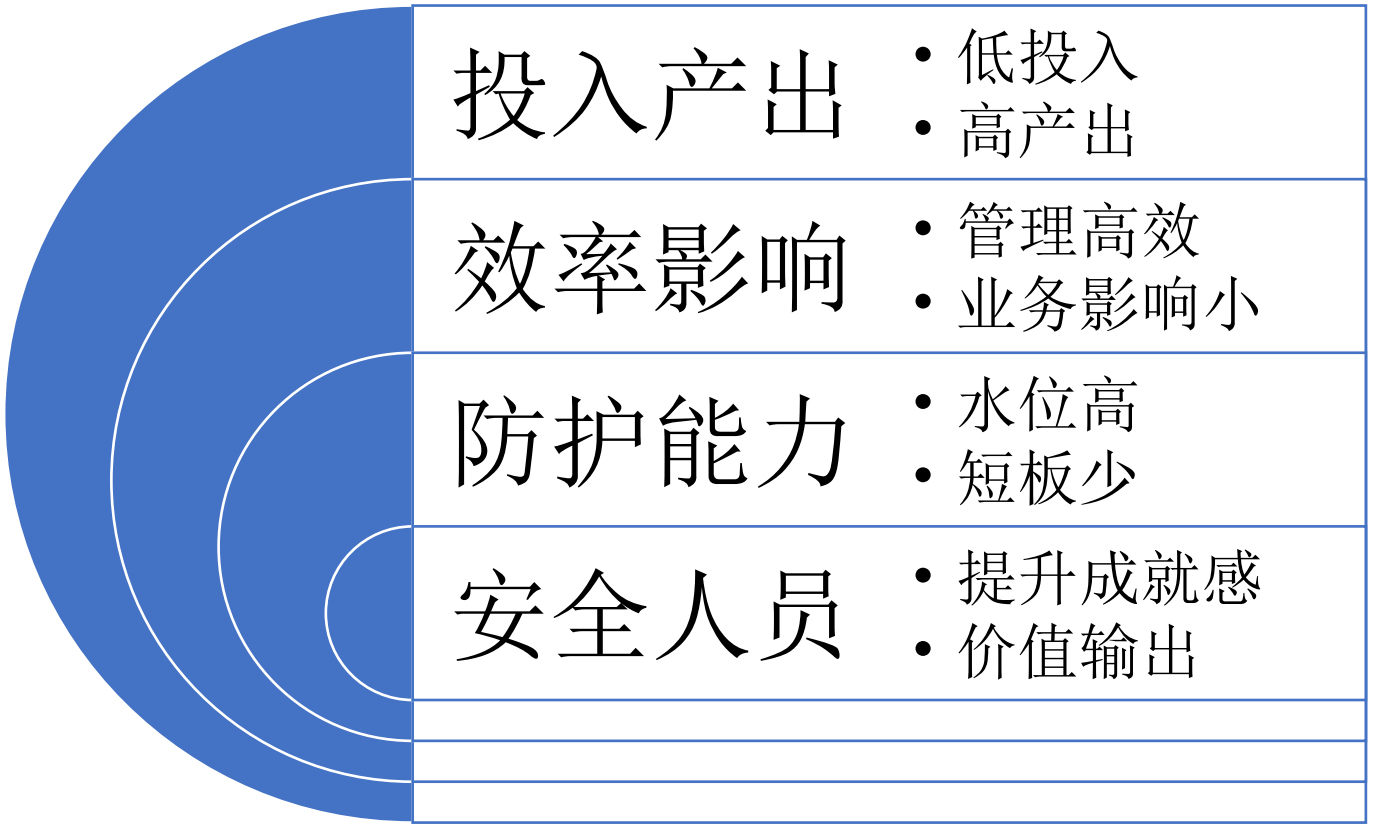
- 第四课：人员流失之痛

感受

- 陷入重复，低价值工作
- 骨干离职=业务瘫痪

如何发挥人的价值？

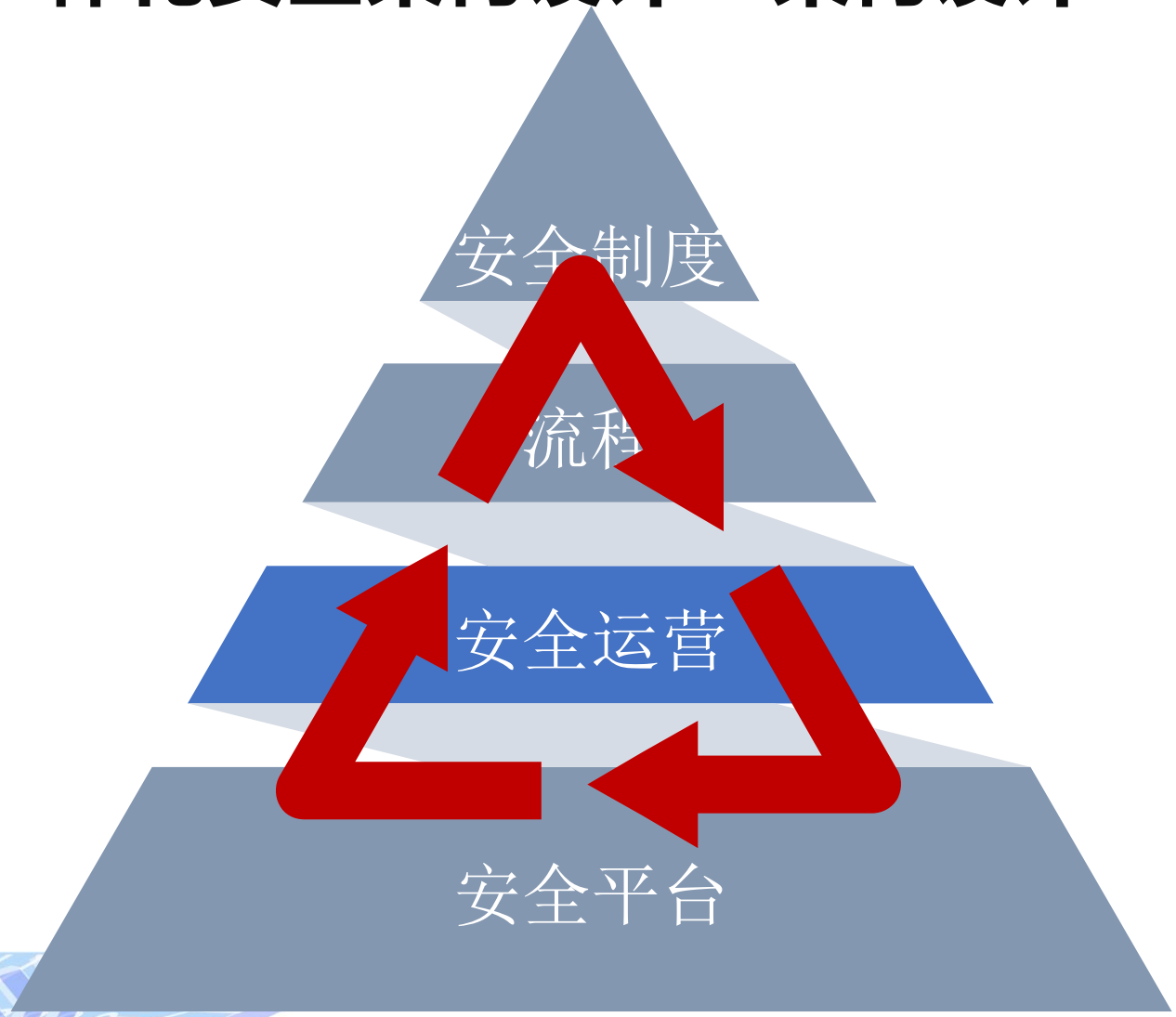
思维的转变 – 追求什么？



议题

- 安全思想转变之路
- 一体化安全架构设计
- 运营实例
- 踩坑风险

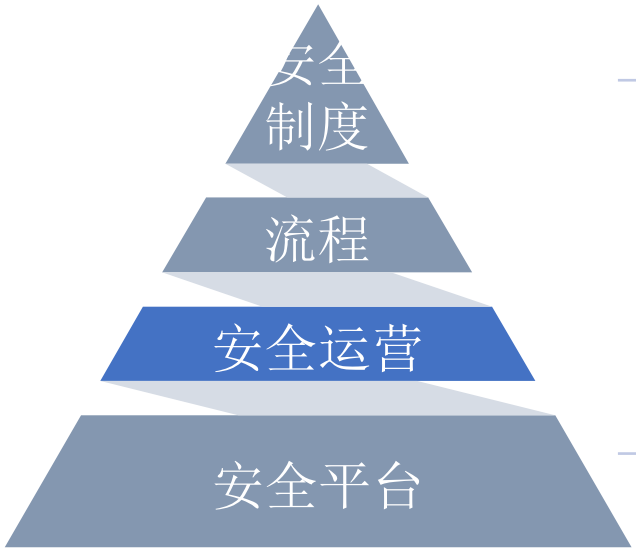
一体化安全架构设计 – 架构设计



1. 减少重复工作
2. 做有价值的事
3. 个人知识转化
4. 共同成长

一体化安全架构设计 – 思想逻辑

内在的逻辑关系

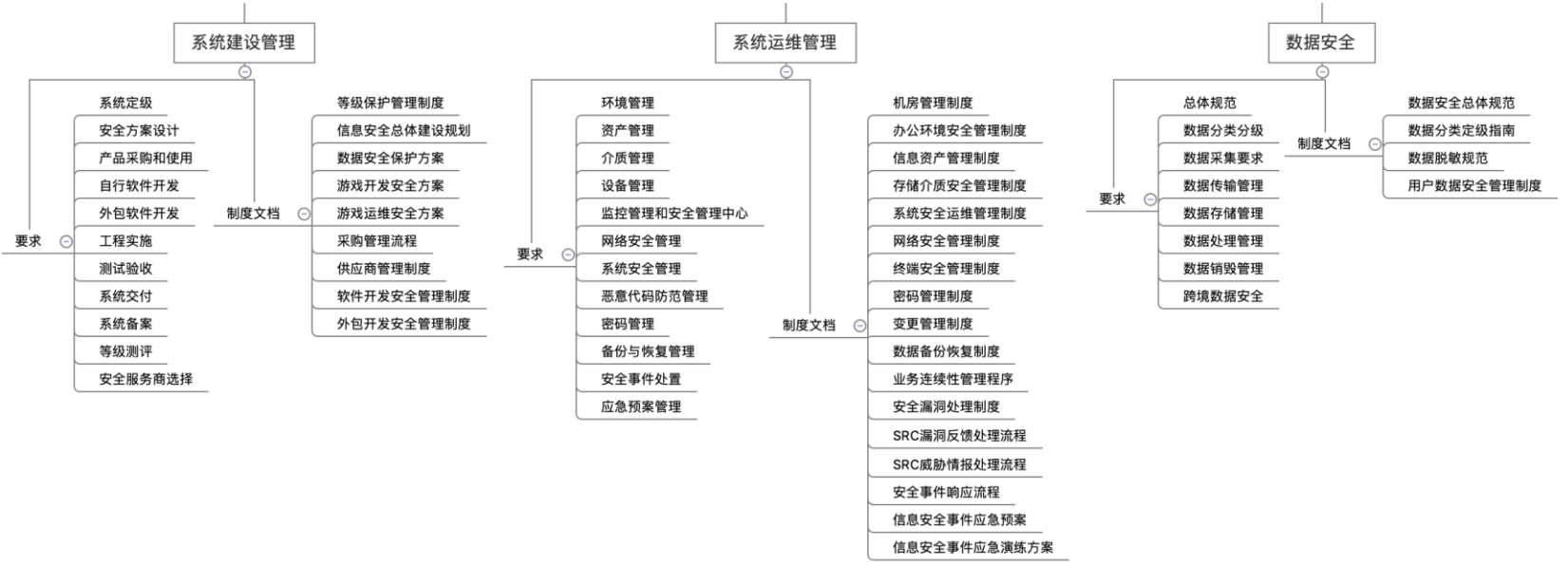


安全制度 -> 靠流程落地

流程 -> 靠安全平台执行、监控、保障

制度、流程、安全平台 -> 靠人运营维护，优化迭代

一体化安全架构设计 – 安全制度

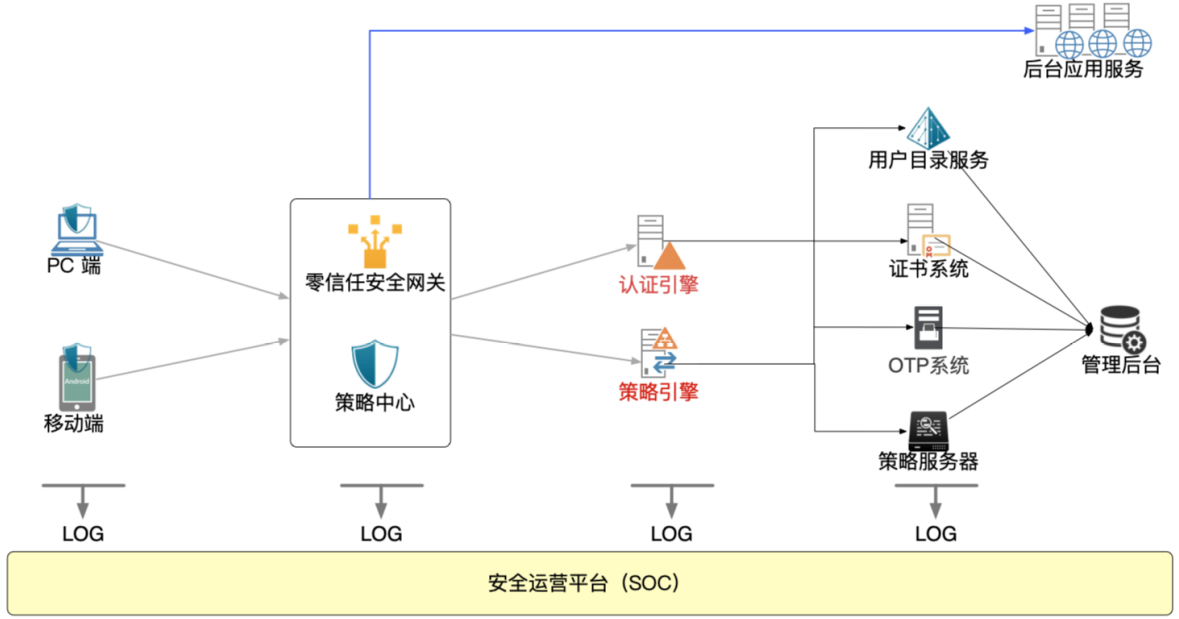


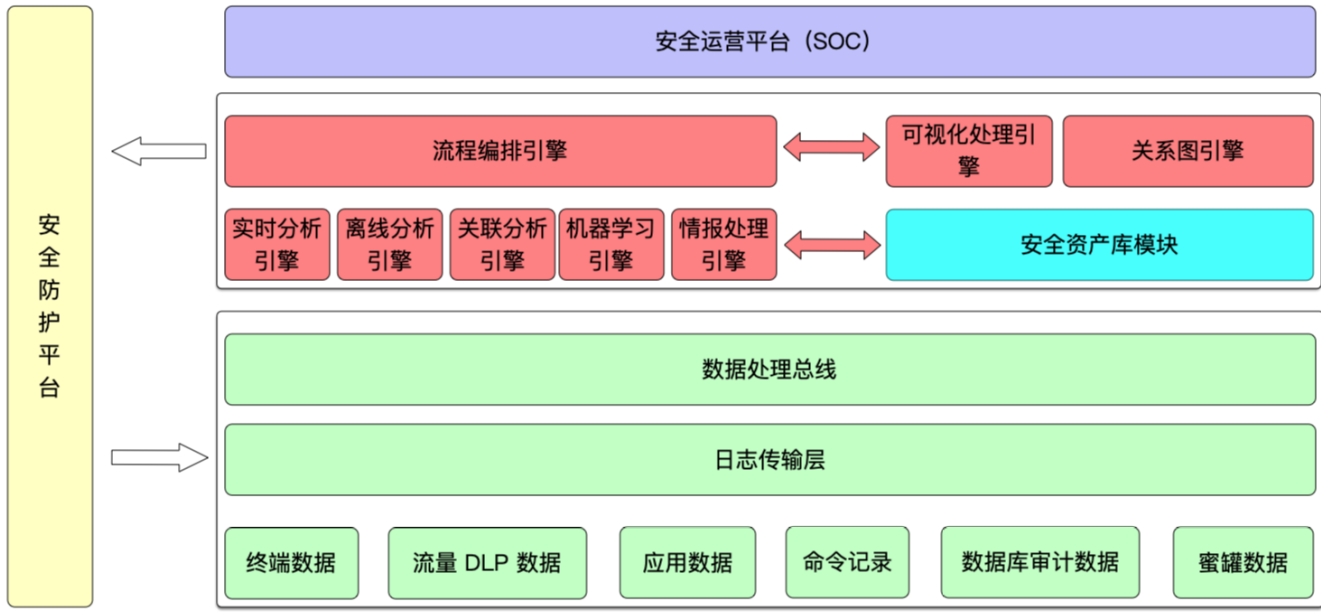
- 监管要求整合，一套制度覆盖多个标准
- 制度包含落地流程，技术平台控制措施
- 覆盖等级保护、个人隐私保护、TIGC审计、上市审计、第三方安全评估、ICP备案

一体化安全架构设计 – 流程控制

- 流程对接安全平台
- 流程要自动化、服务化
- 效率提升，你好，我好，大家好！

一体化安全架构设计 – 安全平台





平台数据集中，接口联动，相互支持

- 零信任防护平台：一体化架构，覆盖全端，全业务，全员工，数据输出运营平台
- 安全运营平台：一体化数据收集、处理、分析、预计、响应，联动防护平台

一体化安全架构设计 – 安全运营

目标

解决什么问题？

- 防入侵？
- 防内鬼？
- 减少漏洞？
- 事件捕获？

方法

采用什么方式？

- 完善制度？
- 优化流程？
- 接入平台？
- 安全服务？

评价

如何评价？

- 覆盖率？
- 检出率？
- 响应时间？

验证

如何证明？

- 穿透性测试
- 有效性验证
- 矩阵式监控

优化

如何优化/固化？

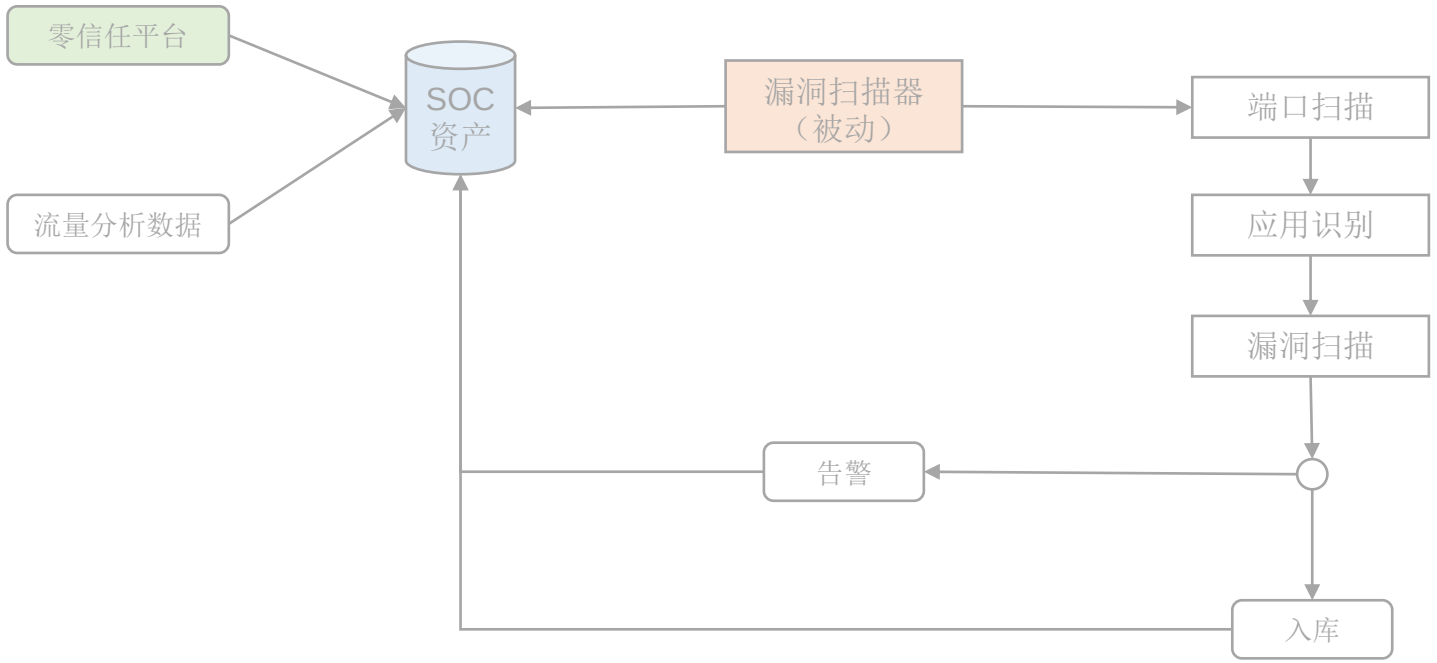
- SOP
- Playbook
- 专家策略

人的运营没有终点！

议题

- 安全思想转变之路
- 一体化安全架构设计
- 运营实例
- 踩坑风险

运营实例 – 扫描联动平台



- 数据集中
- 数据输出
- 数据输入

运营实例 – 权限管控落地

解决什么问题？

- 权限管控

采用什么方式？

- 制度：权限管理制度
- 流程：权限申请流程
- 平台：零信任权限管理对接
- 服务：支持响应

如何评价？

- 覆盖率：流程申请比率
- 检出率：绕过流程
- 响应时间：平均处理时间

如何证明？

- 审计验证

如何优化/固化？

- SOAR自动化审查

议题

- 安全思想转变之路
- 一体化安全架构设计
- 运营实例
- 踩坑风险

踩坑风险

- 不可控的对接
- 半途而费的自研
- 强关联的雪崩效应

让我们在背锅路上结伴而行！

个人微信

个人公众号

网络安全创新大会
Cyber Security Innovation Summit

THANKS