再谈“安全运营”之能力升级

董晓琼 平安科技

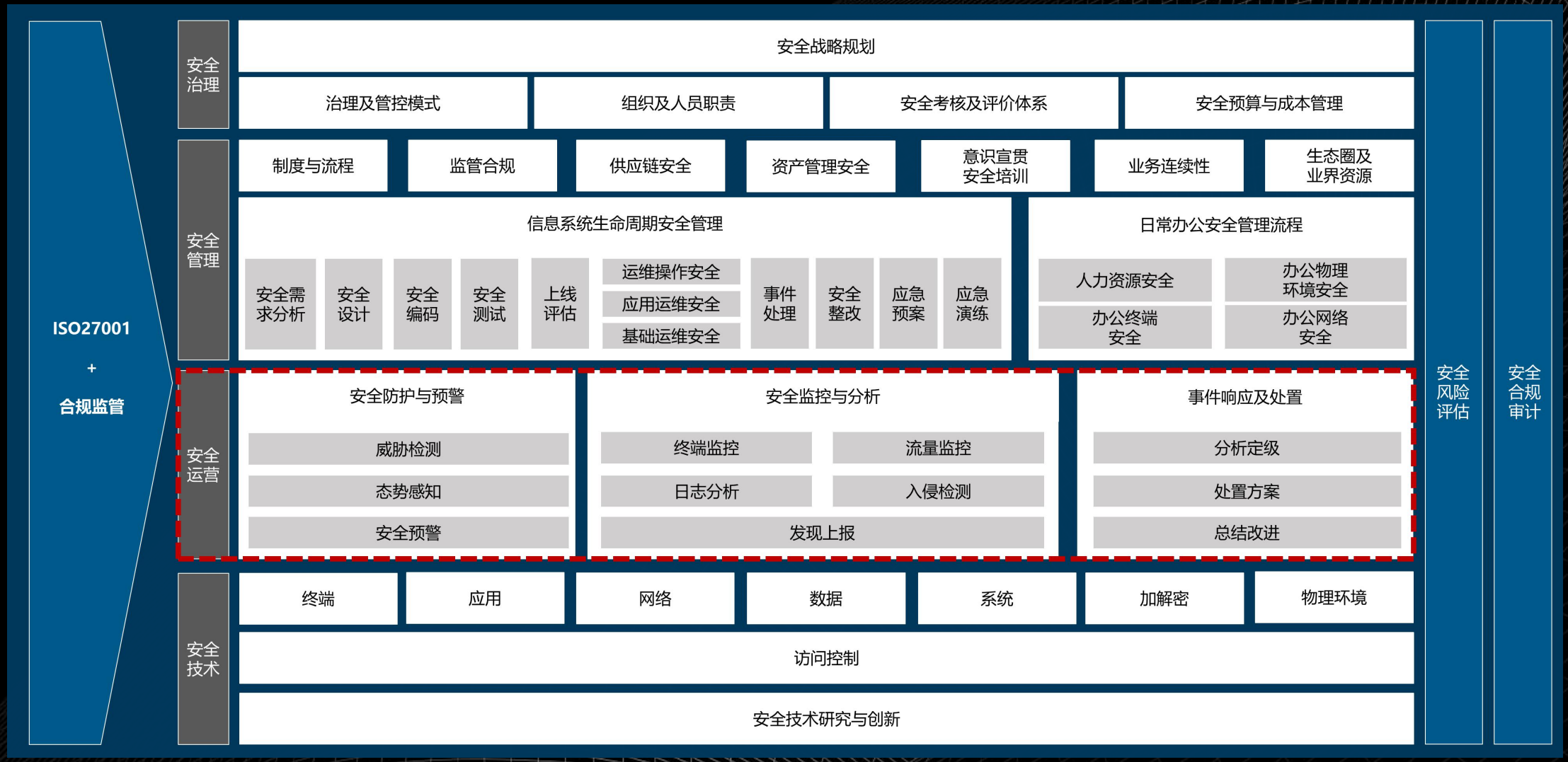
CIS 网络安全创新大会
Cyber Security Innovation Summit

在哪儿：安全运营的今天
去哪儿：安全运营的展望
如何去：安全运营的发展

在企业中，我们所追求的安全“目标”是什么？

再谈“安全运营”

网络安全创新大会
Cyber Security Innovation Summit



安全运营团队的职能

安全运营团队的“日常”

安全产品的运营：
安全措施的推进：
安全措施的改进：
安全预警的处置：

如何评价“安全运营”价值

主动发现的预警占比：
风险资产敞口比例：
资产风险敞口时间：
Mean Time to Response：

“安全运营”效能

自动化处置比率

20%

检测和响应处理时长

1D~/3D-7D

平台效率

Platform 3+

MTTR
-智能化
-可统筹

“安全运营”效能

自动化处置比率

50%

检测和响应处理时长

50%

平台效率

Platform 1+

安全投入成本

Hard to find

Networking
Application Layer Protocols
OS-Unix/Windows
Web Application
APPs (IOS/Android)
Cloud Computing
Data Encryption/Masking
Security Monitoring Tools
Business Fraud
……

Regulatory Compliance
Security Compliance
S-SDLC
Security Investigations
Data Goverance
VRM
……

Communication & Writing
Critical Thinking
Creativity & Curiosity
Motivation
Data Analysis
……

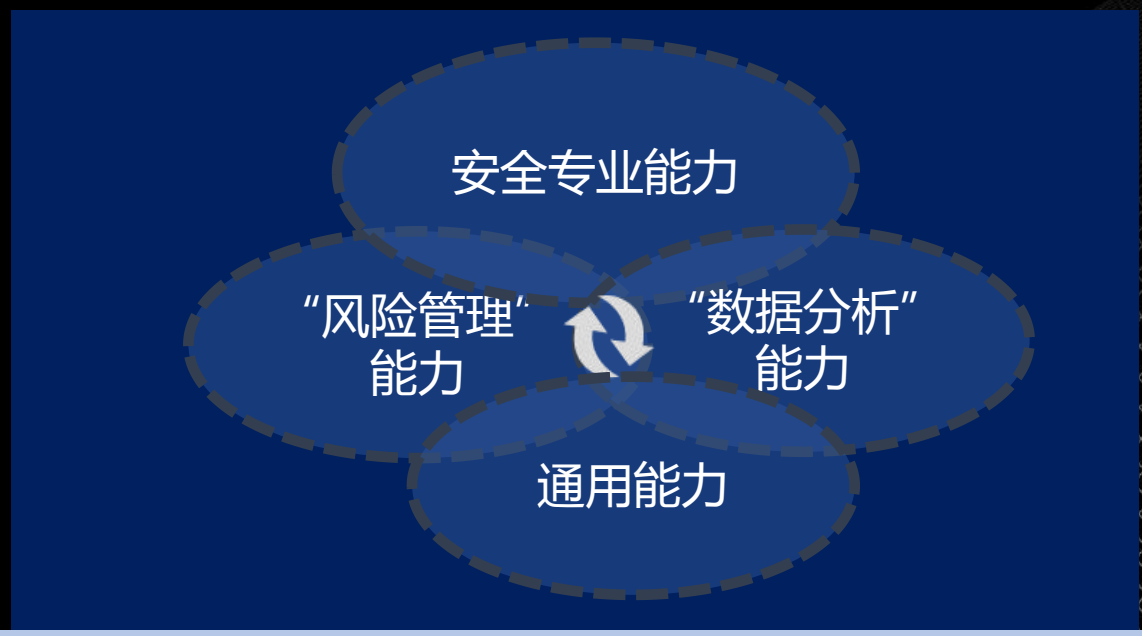
Capabilities Metrix

再谈“安全运营”

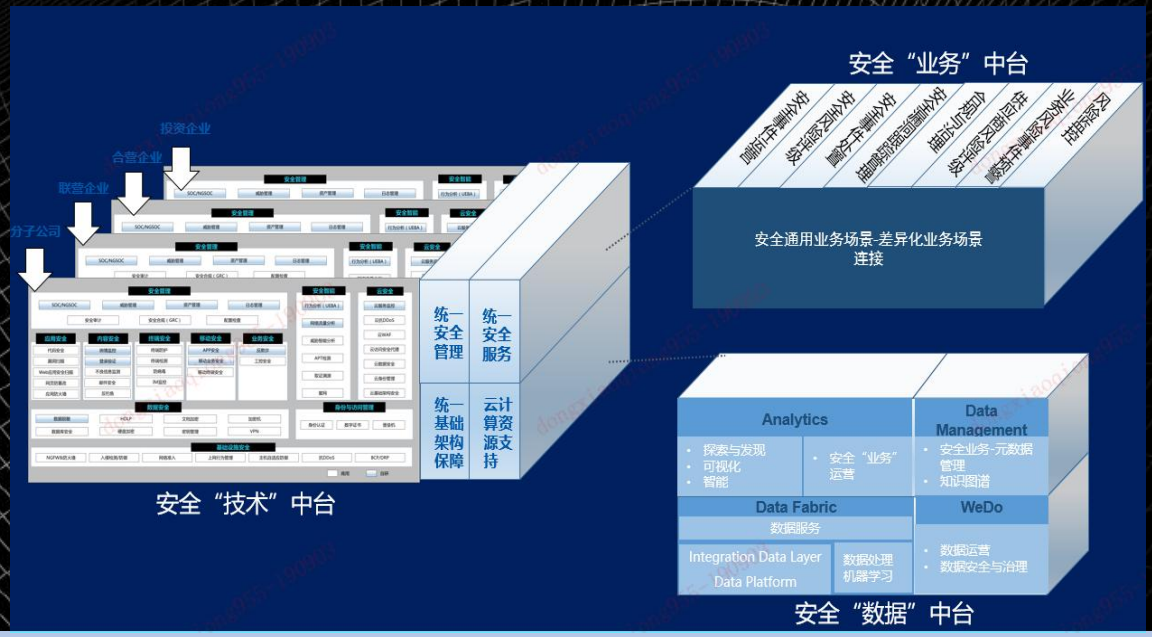
武器很多，检测效果-可靠和可见性？
预警太多，人力/时间不匹配
预警调查，事件优先级，调查路径
预警处置，无法实现响应的运营化

Effectiveness & Efficiency ?

再谈“安全运营”-思维的变革



助力



安全人员能力

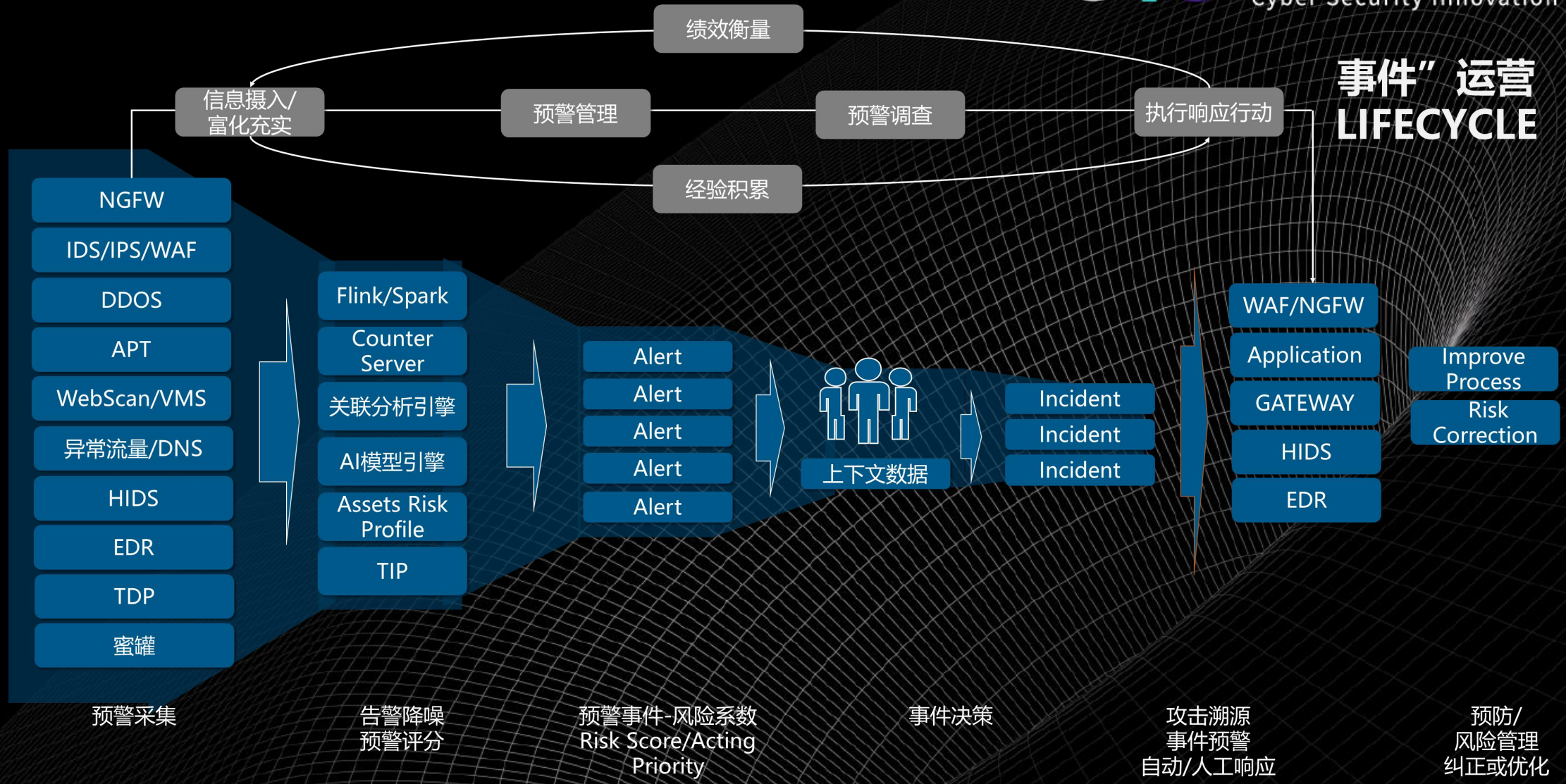
平台能力

自信、快速的识别和响应处置威胁

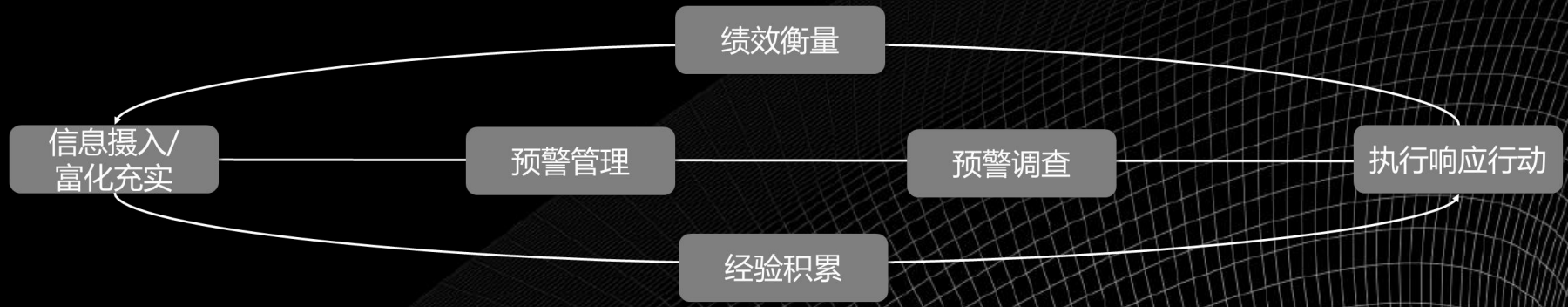
再谈“安全运营”

网络安全创新大会
Cyber Security Innovation Summit

事件”运营 LIFECYCLE



再谈“安全运营”



痛点：
1、检测机制导致的预警准确问题
2、预警量过大，收敛能力不足
3、产品接口自身的能力
4、庞大的业务环境、可你到底有多了解它，资产风险变化的动态性

痛点：
1、不同产品或工具-怎么组合，让支离破碎的信息更有价值
2、预警信息-优先级的定义
3、事件调查-路径长、操作成本高、决策成本高
4、大量的响应处置-无法实现响应的运营化
5、处置标准的固化和优化

数据采集及预警质量
1、预警数据-数量与质量
2、预警数据-跨产品间的场景关联
3、情报数据-不同情报体系的应用

数据富化
1、数据富化（手动-自动化）
2、数据调查能基于多种数据源-上下文
3、高质量/高自动化的预警处理
4、不同情报源的校验和参考

事件调查和处理
1、事件调查的手段和行为积累
2、跨产品搜索的事件回溯和检索的机制
3、事件处理流程可视化，且和编辑
4、重建事件时间线
5、Case管理和积累-每类事件处理流程高效利用

响应与强制执行
1、安全产品的接口丰富度/性能
2、跨平台和跨功能的团队响应
3、剧本可以重复利用、嵌套和共享

优势：

来自不同层面的、丰富的安全数据
数据的计算能力

Log:
Alert Events

Log：
HTTP Access Log
TCP Sessions
DNS Log

TI：
Malware Hash
IP、Domain、Darkweb
CVE

Vulnerability

Assets Profile
Assets Vulnerability
Honey pot

NGSOC
Stream +Rule

Sec Data Center
Stream
ML

Incident

Incident

Investgation

Feedback

挑战：

业务环境复杂、威胁环境特征及变化太快
动机不清：个体、团伙、国家队的威胁，多方遇敌
数据挖掘成本过高，模型结果在不同场景中表现不同

决策大脑智能化
1、“源头”-安全预警萃取
2、场景化的情报数据应用及加工
3、资产及员工行为-风险属性标签化
4、场景化的AI辅助检测
Web应用攻击模型检测
接口异常监控
异常账户行为监控
恶意攻击链识别
WEBSHELL识别等

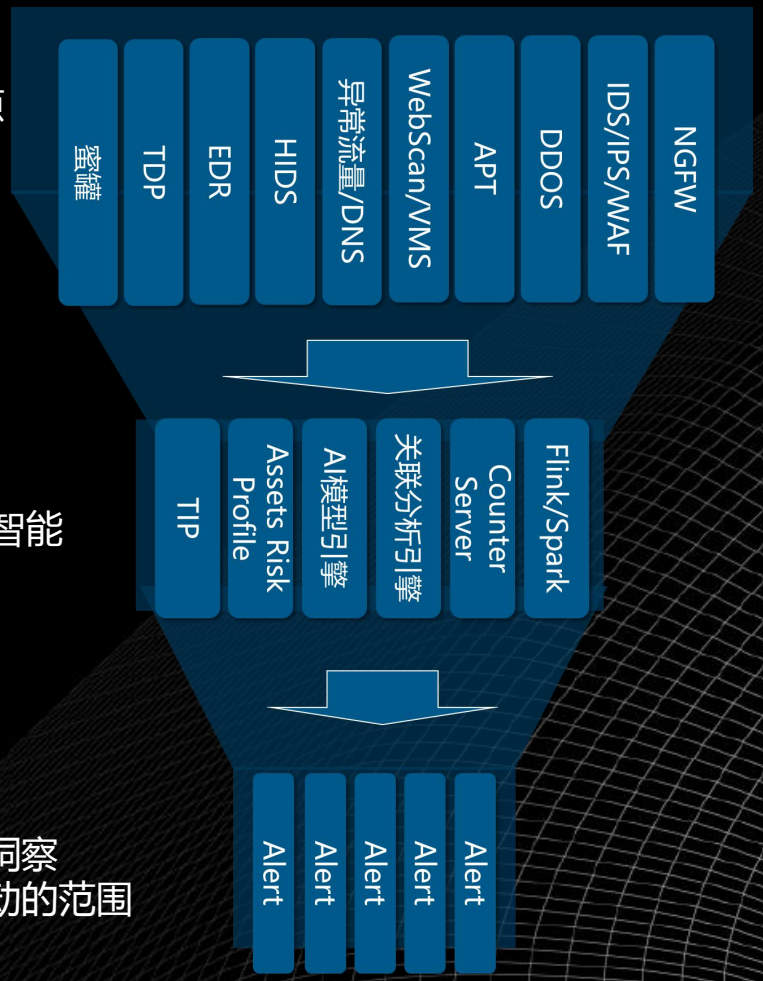
情报及人工智能驱动变革

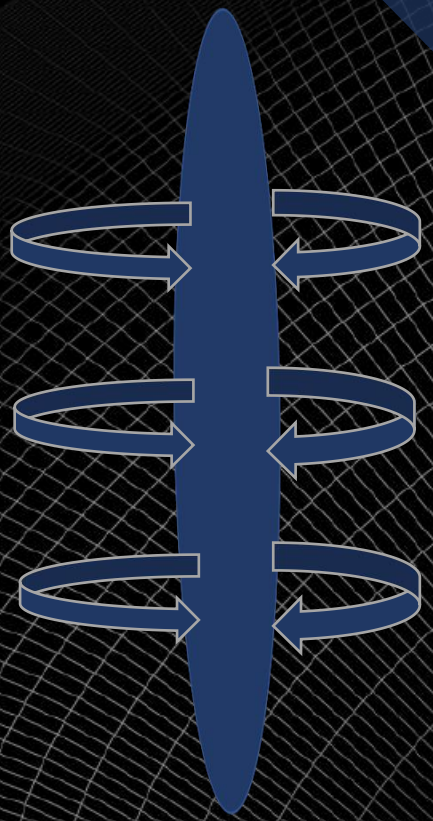
网络安全创新大会
Cyber Security Innovation Summit

广泛的数据源

情报及人工智能

安全可见及洞察
确定优先行动的范围





终端风险预警
7600+

主动安全预警与处置
1300+

主动防御
600万+

业务风险
7000万+

终端违规
98+

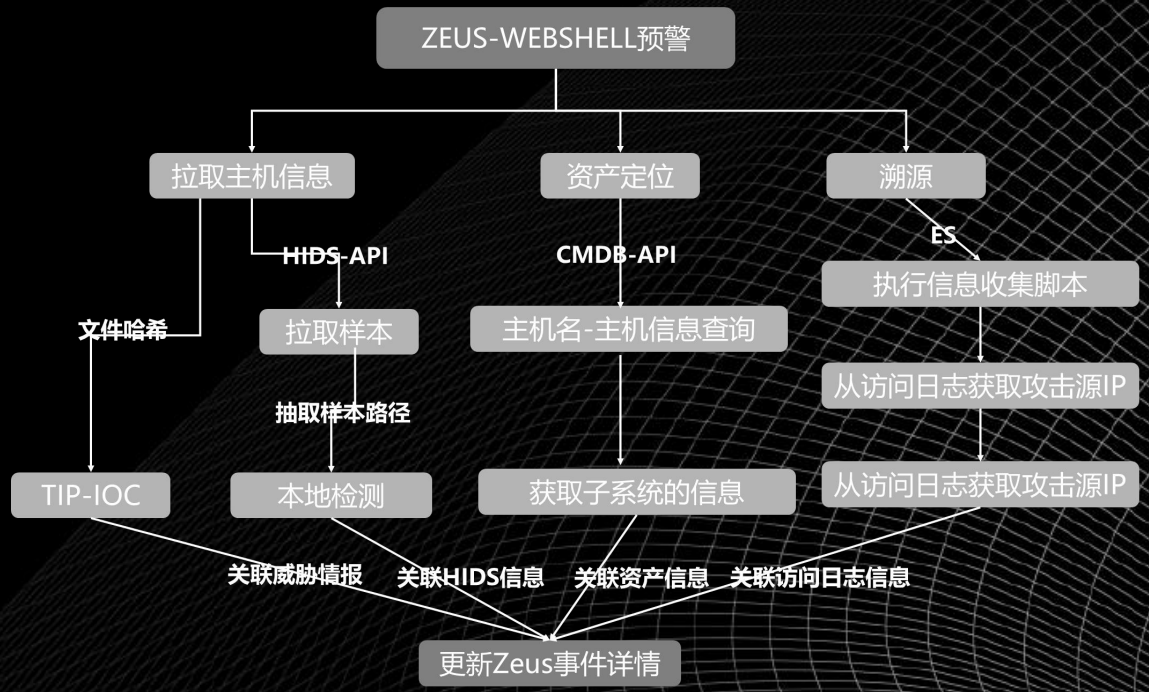
应急响应
1016

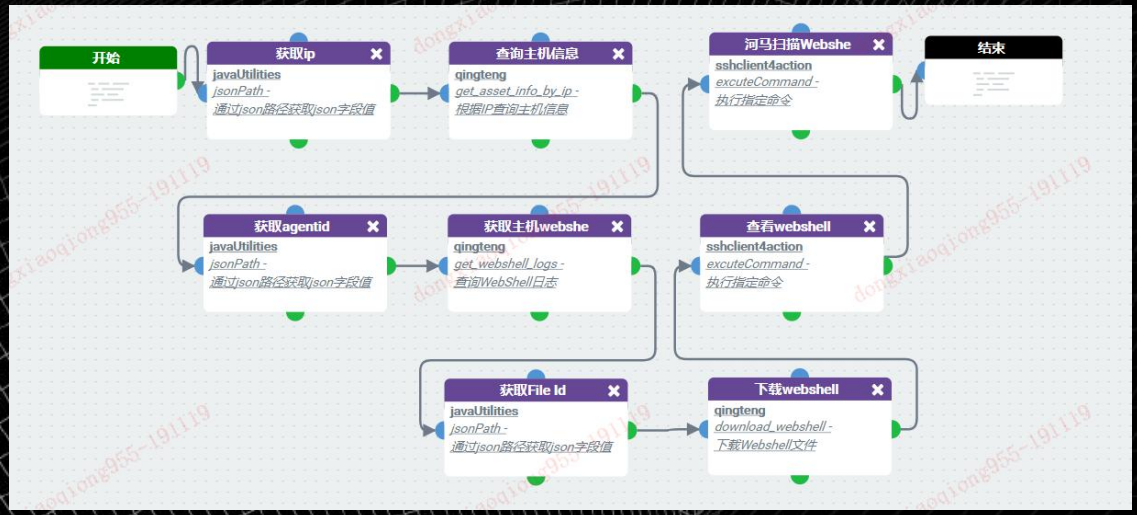
事后安全处置及改进

利用SOAR-“统筹”事件调查和处置

Tools：
HIDS | Zeus-NGSOC| APT| TIP |CMDB| ES|
Token |堡垒机

主机端webshell 预警来源： HIDS/APT
预警处理流程：
HIDS 预警 → 查询主机系统信息→ 查询主机进程 → 主机端口→ 日志详情→ 下载webshell→ 查询和定位主机





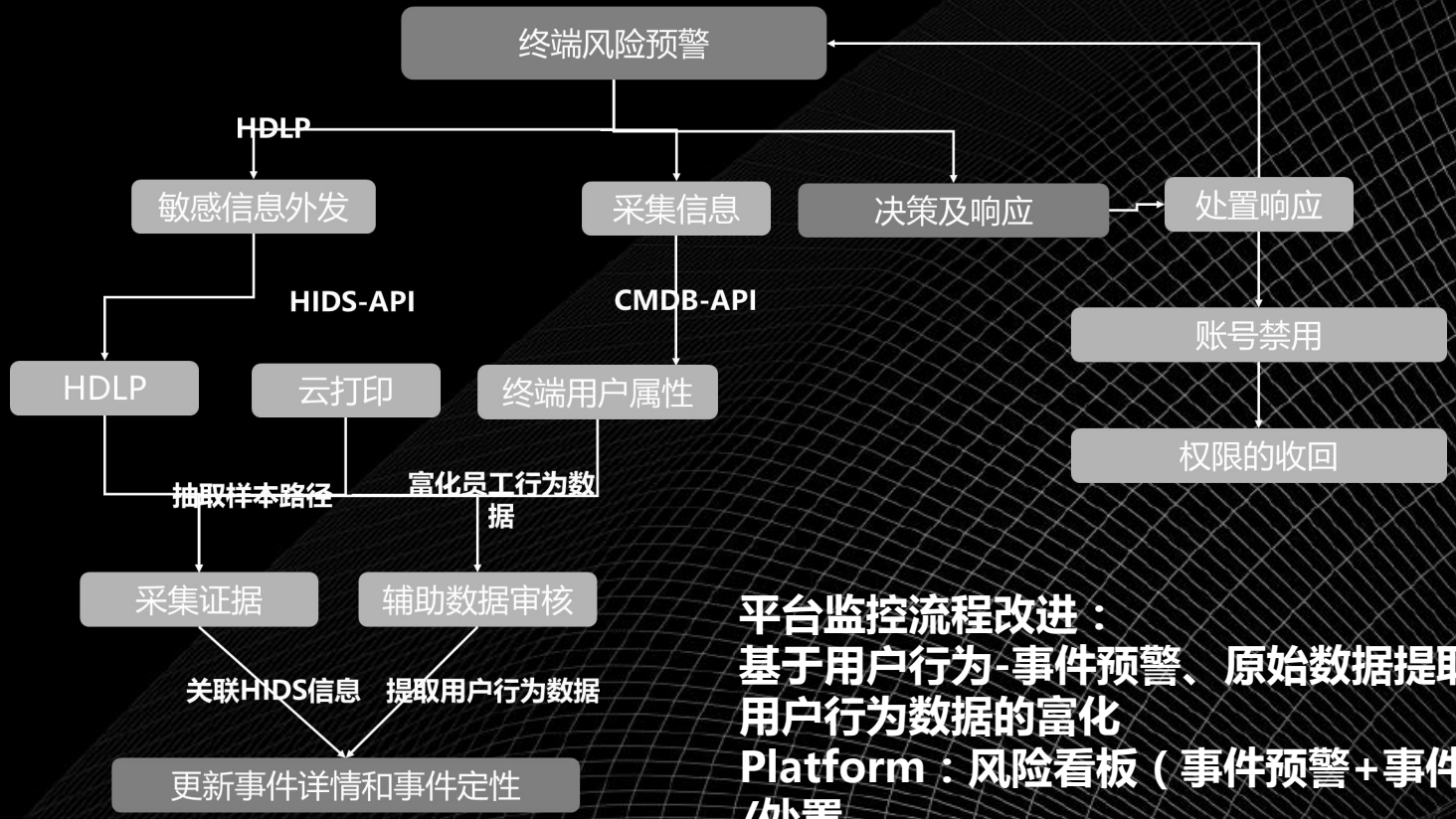
平台改进后处理流程： 信息富化+ 工具化判断
1、TIP预判
2、影响主机定位
3、溯源日志的查询

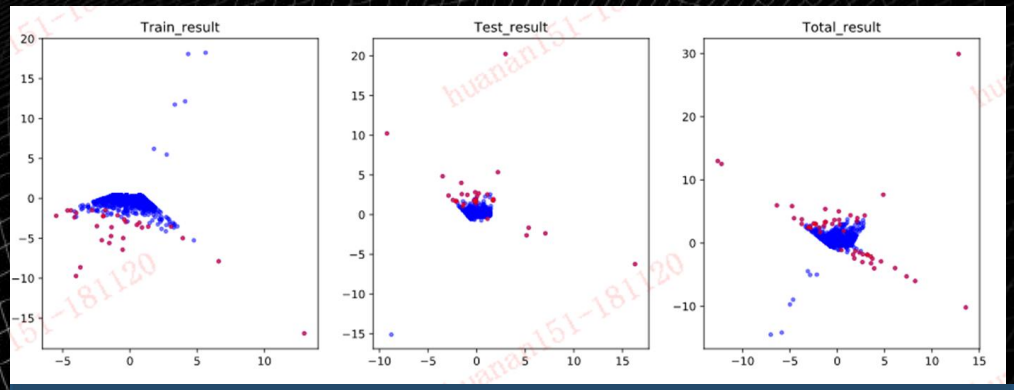
收益：Zeus、人工处理流程简化、15Mins—>19秒

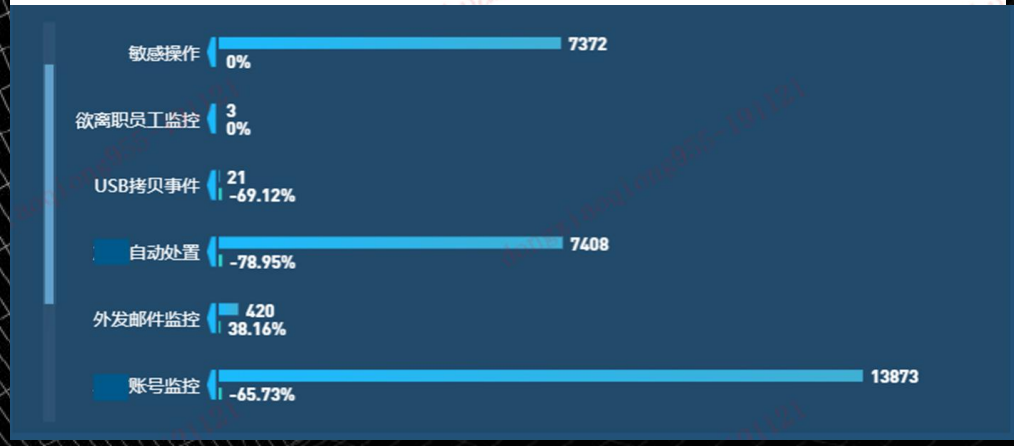
问题：受制于产品接口能力、接口性能

“工具化-”可处置性“响应式运营

风险场景：终端用户信息泄露
预警调查和处置流程：
HDLP终端预警-漏报预警事后发现-定位用户-调取原始数据-定因-事件挽回和定责







平台监控流程改进：
基于用户行为-事件预警、原始数据提取、用户行为数据的富化
Platform：风险看板（事件预警+事件分析/处置

收益：
不同终端测原始预警：
从千万级别-7632+（high Risk），
人工处理：98+
Platform：风险看板（事件预警+事件分析/处置

网络安全创新大会
Cyber Security Innovation Summit

THANKS

安全运营的未来：

平台+数据能力的提升

强化安全“洞察力”、“统筹性”