



再谈"安全运营"之能力升级

董晓琼 平安科技







在哪儿:安全运营的今天

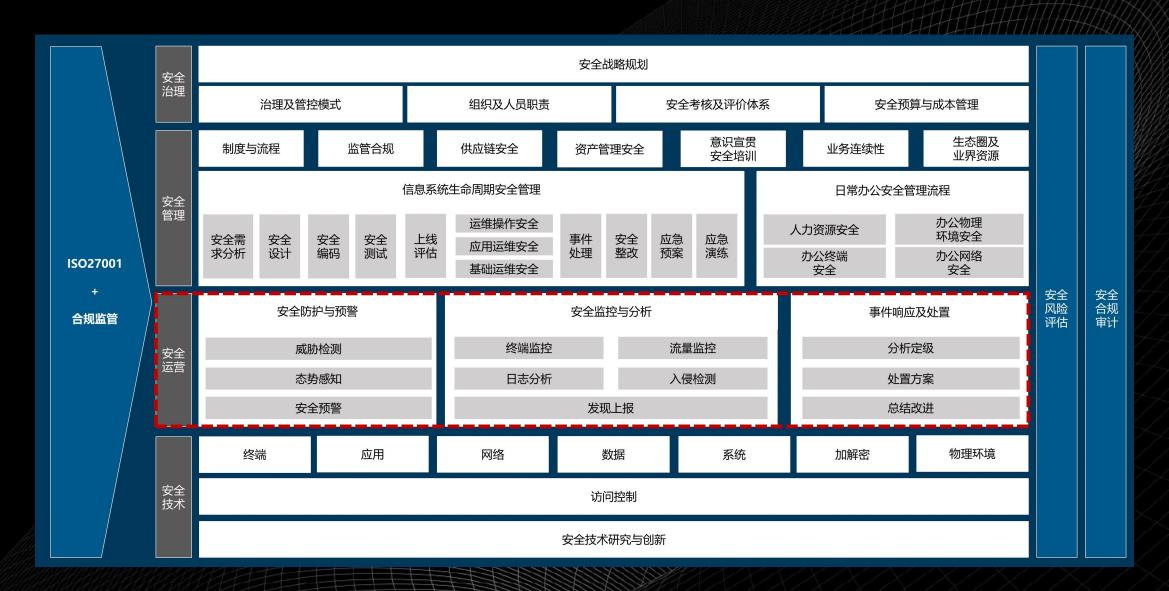
去哪儿:安全运营的展望

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?





安全运营团队的"日常"

如何评价"安全运营"价值

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: 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 检测和响应 比率 处理时长

50% 50%

平台效率

Platform 1+

安全投入成本







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





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?





"风险管理" 能力



"数据分析" 能力

通用能力





		/ 18	
Analytics		Data Management	
探索与发现可视化智能		安全业务-元数据 管理 知识图谱	
Data Fabric 数据服务		WeDo	
Integration Data Layer Data Platform	数据处理机器学习	・ 数据运营 ・ 数据安全与治理	7
並	今"粉坦	" 由公	

安全人员能力

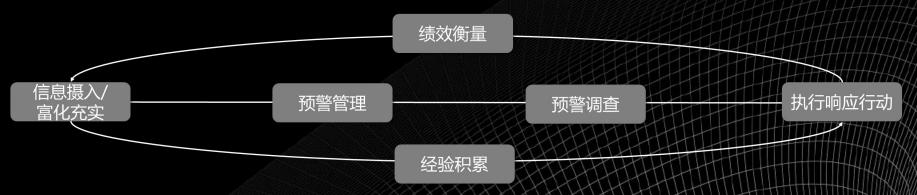
平台能力

自信、快速的识别和响应处置威胁

助

C ≤ 网络安全创新大会 **十 十 -** 再谈 "安全运营" Cyber Security Innovation Summit 绩效衡量 事件"运营 信息摄入 预警管理 执行响应行动 LIFECYCLE 预警调查 富化充实 经验积累 **NGFW** IDS/IPS/WAF Flink/Spark **DDOS** WAF/NGFW Counter **APT** Alert **Application Improve** Server **Process** Alert WebScan/VMS Incident **GATEWAY** 关联分析引擎 Risk Alert Incident Correction 异常流量/DNS HIDS AI模型引擎 Alert Incident 上下文数据 HIDS **EDR** Assets Risk **Alert Profile EDR** TIP **TDP** 蜜罐 告警降噪 预警评分 预警事件-风险系数 预警采集 事件决策 攻击溯源 预防/ Risk Score/Acting 事件预警 风险管理 Priority 自动/人工响应 纠正或优化





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

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

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

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

网络安全创新大会 Cyber Security Innovation Summit

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

Incident

Sec Data Center

Stream

ML

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

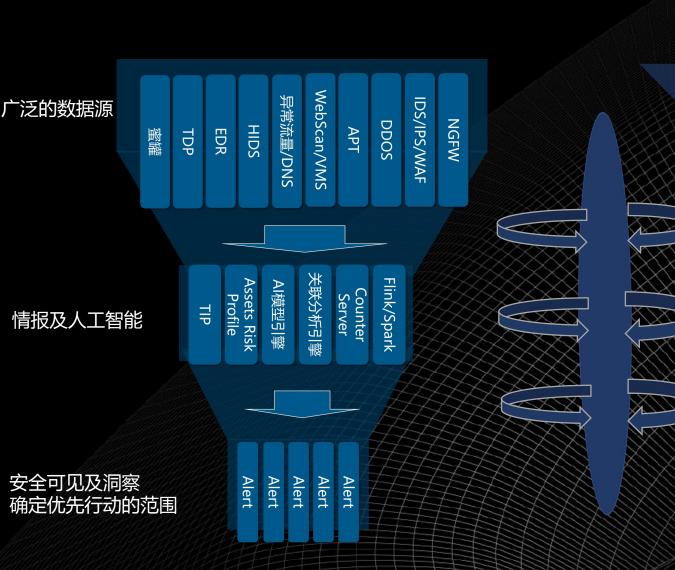
决策大脑智能化

- 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



Investgation





终端风险预警 <u>=</u> 7600+

主动安全预警与 处置 1300+

主动防御 业务风险 终端违规 600万+ 7000万+ 98+

> 应急响应 1016

事后安 全处置 及改进

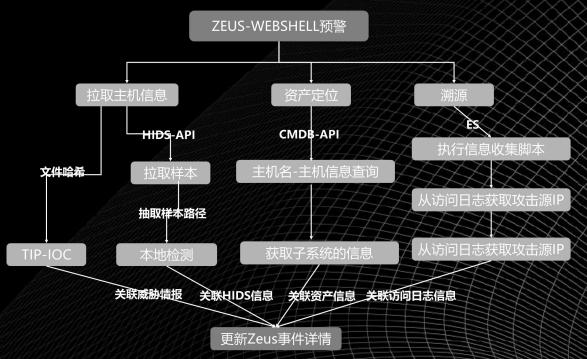


Tools: HIDS | Zeus-NGSOC| APT| TIP |CMDB| ES| Token |堡垒机

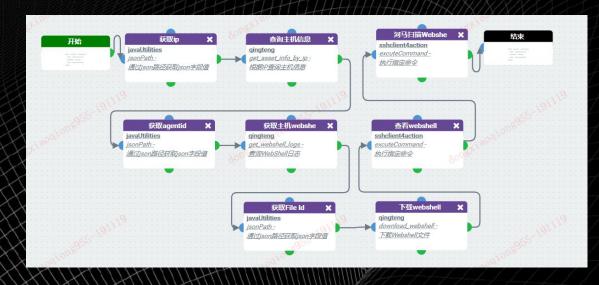
主机端webshell 预警来源: HIDS/APT

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



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



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

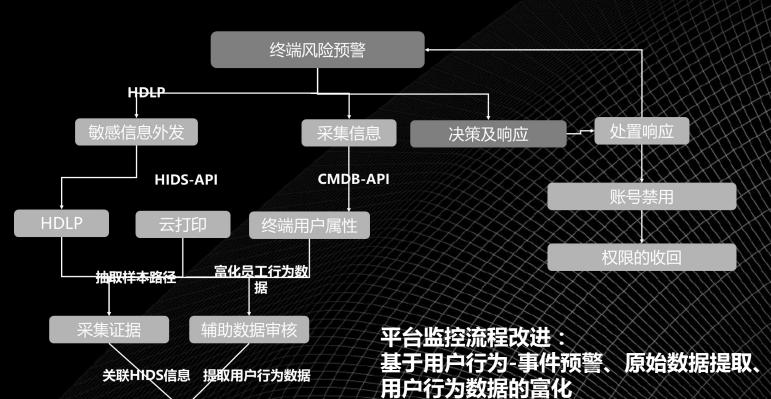
风险场景:终端用户信息泄露

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

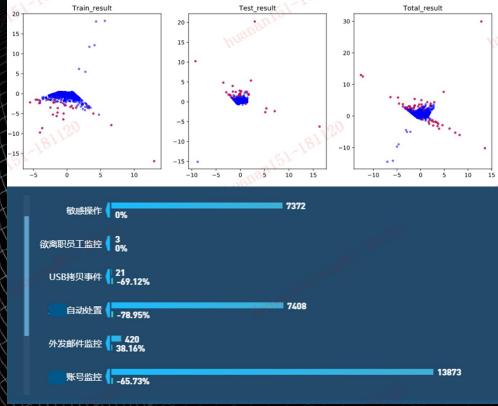
更新事件详情和事件定性



/处置

Platform: 风险看板(事件预警+事件分析

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



收益:

不同终端测原始预警:

从干万级别-7632+ (high Risk),

人工处理:98+

Platform: 风险看板(事件预警+事件分析/

处置





~ 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"