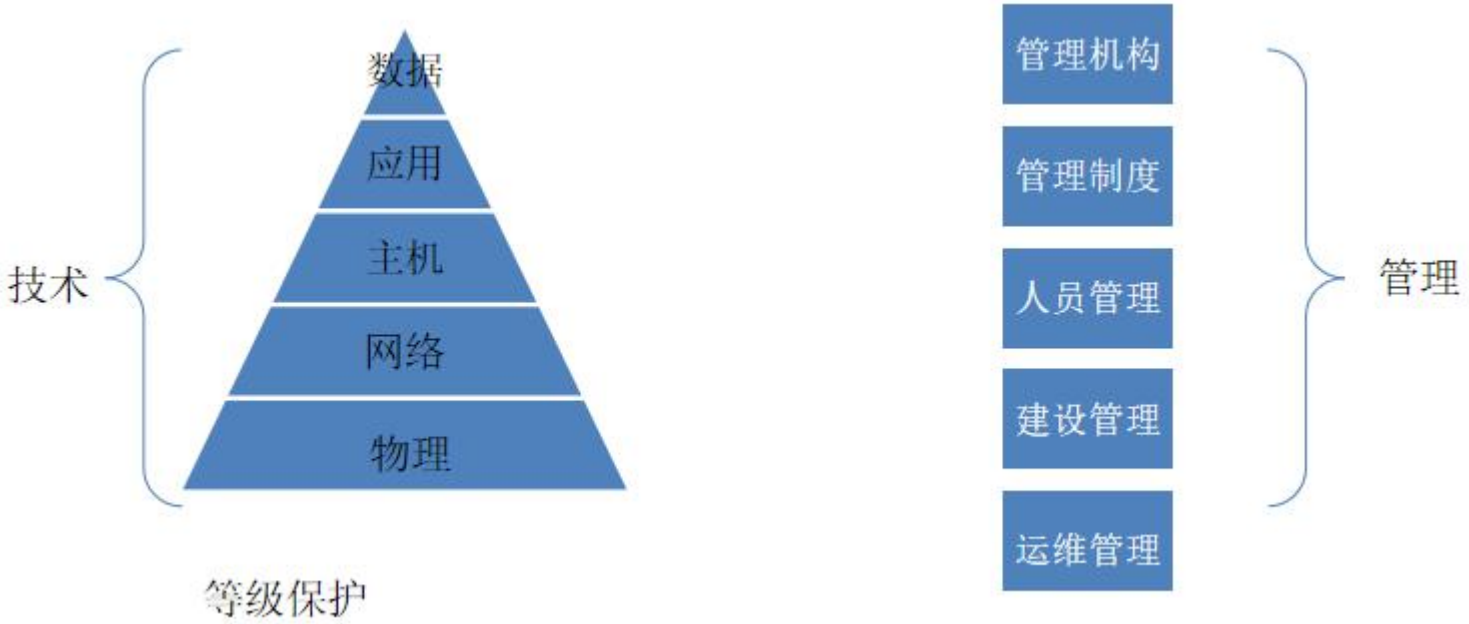
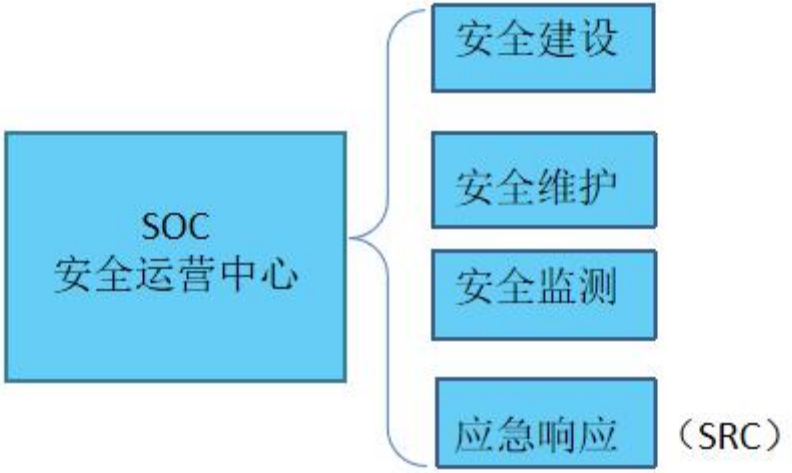
浅谈甲方安全

Leo

攻击点、防御面



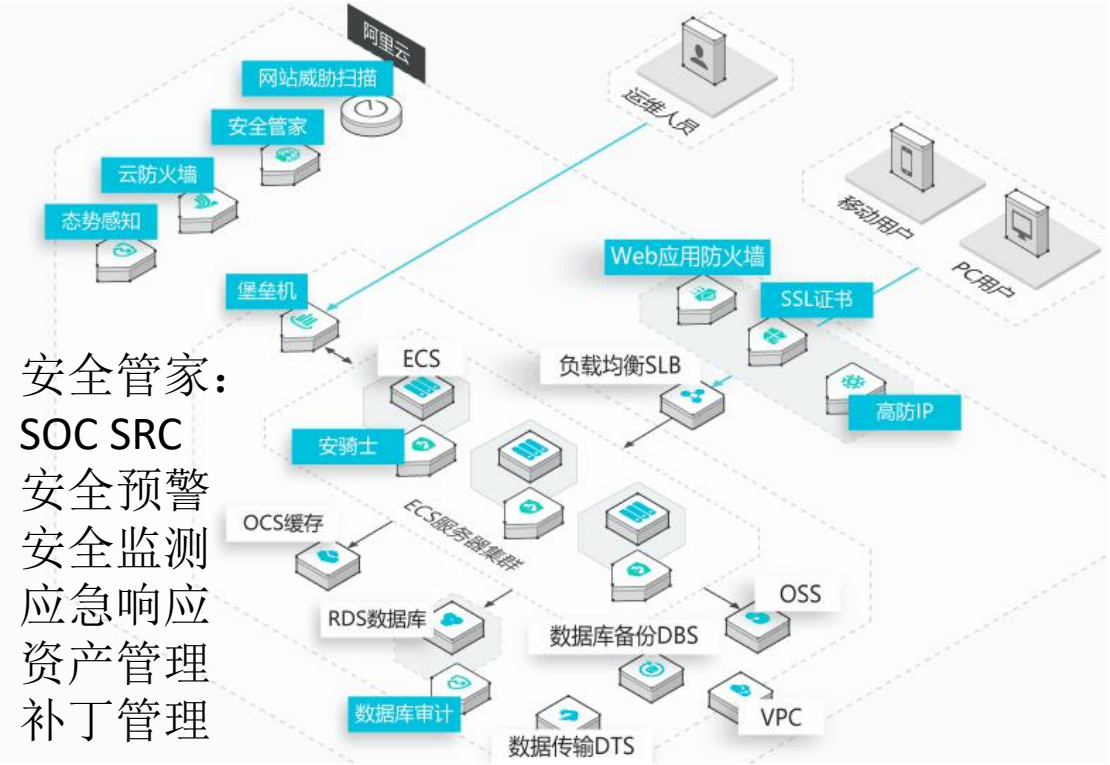

SOC
安全运营中心
安全建设
安全维护
安全监测
应急响应
（SRC）

常规建设


网络安全 Network Security
终端安全 Endpoint Security
应用安全 Application Security
数据安全 Data Security
云 Cloud
大数据 Big Data
物联网 IoT
移动 Mobile
身份与访问管理 Identity & Access management
安全管理 Security Management

常规建设

FW、WAF、SSL、抗D、负载均衡



安全管家：
SOC SRC
安全预警
安全监测
应急响应
资产管理
补丁管理

安骑士：
OS：病毒主动查杀
漏洞检测
主机异常
基线检查
日志检索
Web：网站后门扫描
网页防篡改
Web漏洞扫描
日志检索

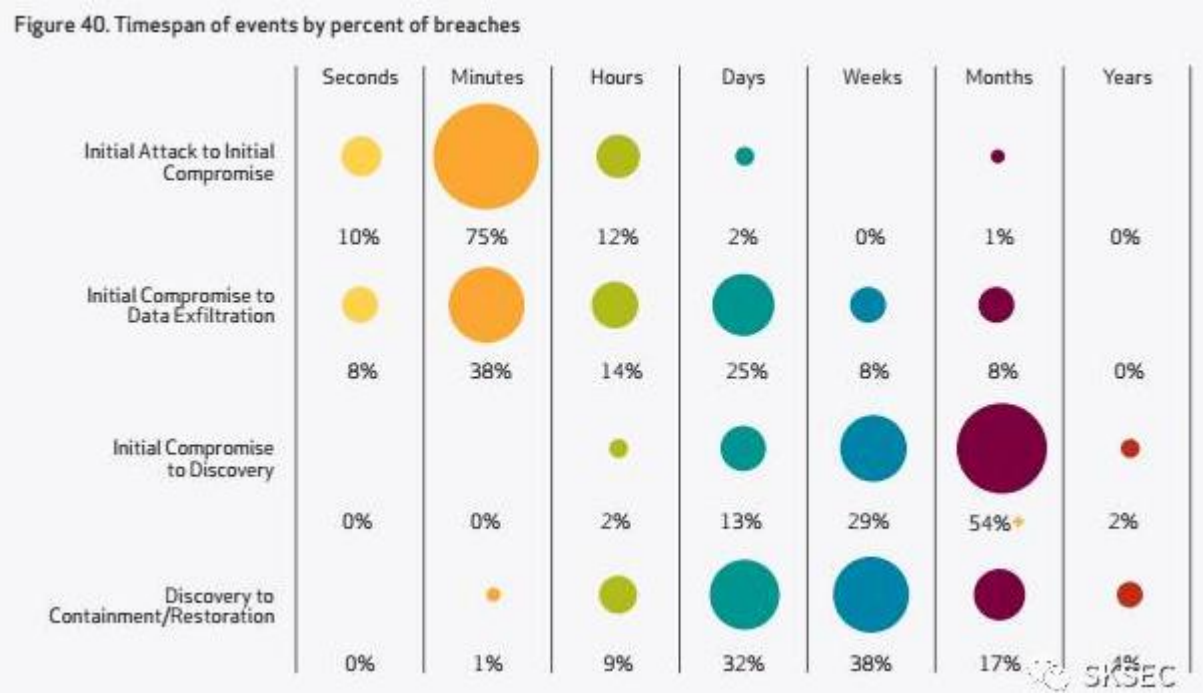
数据库备份、加密、审计与防泄漏

堡垒机、身份认证、访问控制

流量、日志与代码审计、渗透测试

安全规章与人员管理、培训　移动安全、工控安全、无线安全、物联网安全、区块链安全

工程越来越大 处理越来越复杂 防御越来越低效 攻防失衡并未得到扭转（被动挨打）



国外某数据公司发布的攻防时间对比图

化繁为简、智能感知、主动防御

SOC Powered By the BigData & AI

大数据与AI驱动的安全运营中心建设

解决方案

威胁情报

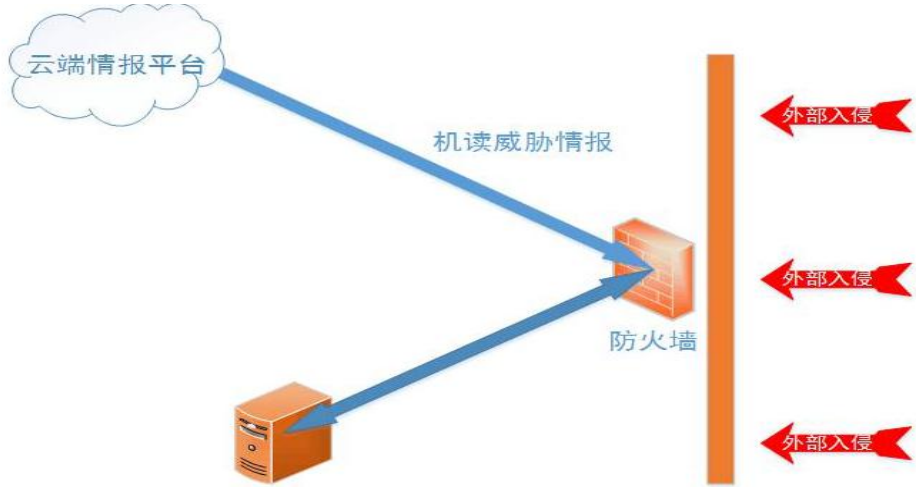
ELK+HDFS 聚合主机、应用日志、网络流量

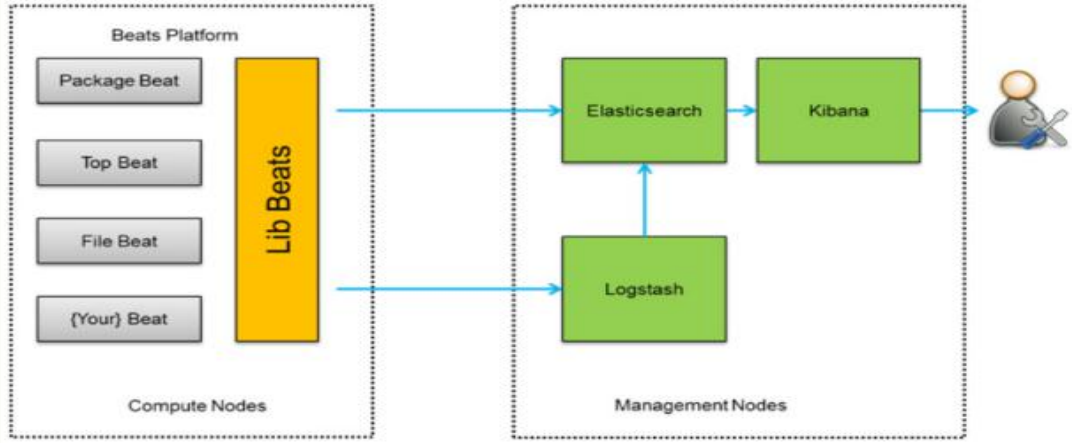
AI自动判断、简化威胁发现、聚合告警、事件合并。

区分自动化随机扫描，锚定针对性攻击，双向全流量交叉验证

内部资产梳理、智能识别非合规应用

全球社区情报驱动 、网络安全命运共同体



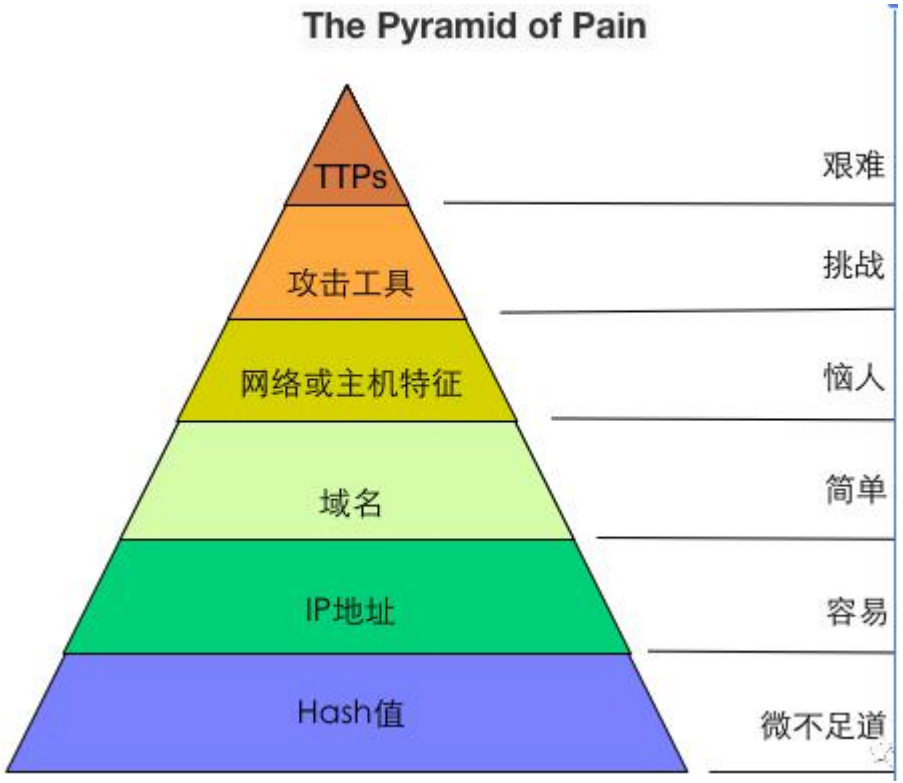


威胁情报

收集分析得到IOC、木马协议分析、DGA等威胁情报并提供可行建议，这些知识可为威胁响应提供决策依据。

主要情报如右图

TTPs：Tactics、Techniques & Procedures



威胁情报

1.攻击监测与防御

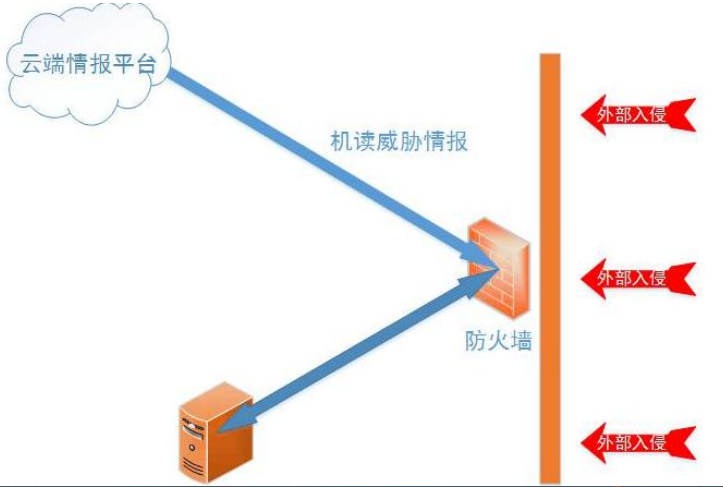
联动IPDS AV SIEM NFT和主动欺骗蜜罐

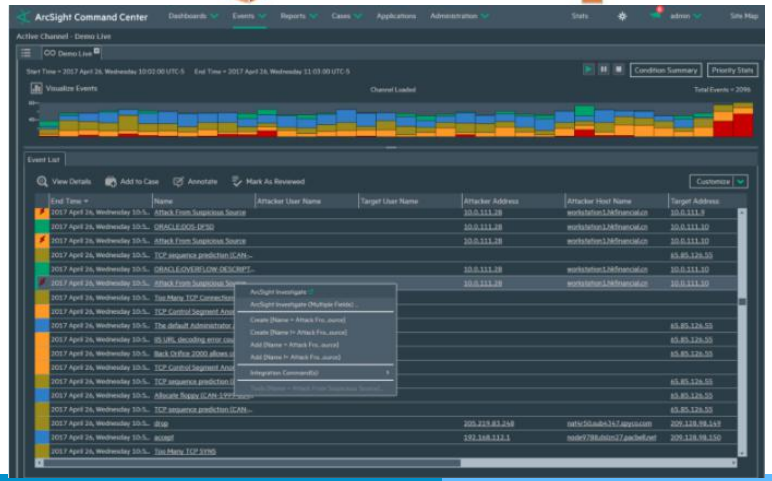
2.攻击溯源

明确攻击范围、SIEM检索

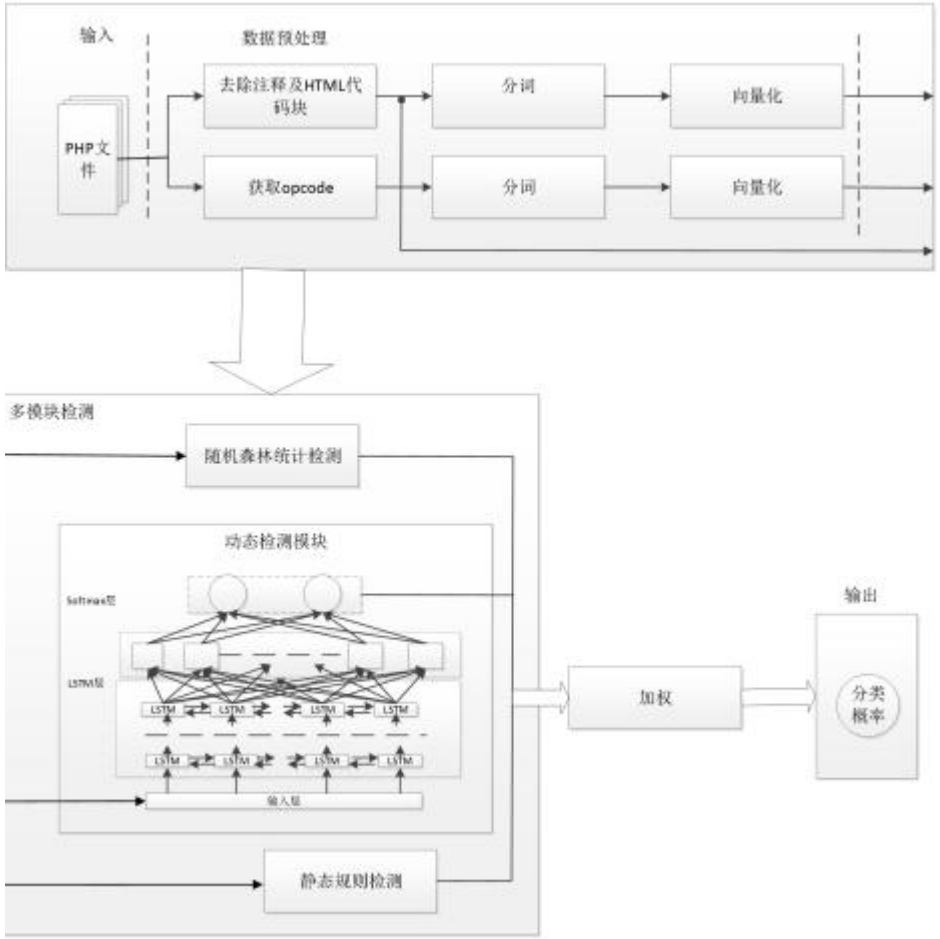
3.态势感知

融合分析、知己知彼





基于集成学习与深度学习的多策略WebShell监测系统



态势感知

以全流量分析为核心，
结合威胁情报、行为分析建模、UEBA、失陷主机检测、图关联分析、机器学习、大数据关联分析、可视化等技术，
对全网流量实现全网业务可视化、威胁可视化、攻击与可疑流量可视化等，
帮助客户在高级威胁入侵之后，
损失发生之前及时发现威胁。

安全事件告警和检索

对安全事件进行实时监控和处理建议说明，并对告警事件进行分析和全文检索

原始日志存储和检索

支持企业版180天内的原始日志检索功能，满足自定义查询日志和分析的需求

安全风险量化和预测

通过机器学习，精量化威胁分析，预测潜在的安全风险

提供安全可视化界面

企业版提供安全可视化界面，全面+实时的感知安全问题

安全演化

安全挑战与机遇并存

THANKS

Name： Leo
Email: leo_infosec@foxmailcom